Cisco IOS Quality of Service ソリューション コマンド リファレンス

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/

© 2018 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章

A から C 1

access-list rate-limit 3

account 6

admit cac local 8

atm-address（qos） 9

attribute 11

auto discovery qos 12

auto qos 14

auto qos voip 16

auto qos voip（6500） 19

bandwidth（policy-map クラス） 23

bandwidth qos-reference 35

bandwidth remaining ratio 39

bump 45

bundle 49

bundle svc 51

class（EtherSwitch） 53

class（ポリシー マップ） 56

class-map arp-peruser 64

class-bundle 65

class-map 68

class-map arp-peruser 75

class type tag 76

clear control-plane 78

clear ip nbar 80

clear ip nbar classification auto-learn top-hosts 82

clear ip nbar protocol-discovery 83
clear ip rsvp authentication 84
clear ip rsvp counters 86
clear ip rsvp hello instance counters 87
clear ip rsvp hello instance statistics 89
clear ip rsvp hello statistics 91
clear ip rsvp high-availability counters 93
clear ip rsvp msg-pacing 94
clear ip rsvp reservation 96
clear ip rsvp sender 98
clear ip rsvp signalling fast-local-repair statistics 100
clear ip rsvp signalling rate-limit 101
clear ip rsvp signalling refresh reduction 102
clear mls qos 103
clear service-group traffic-stats 106
compression header ip 107
control-plane 109
copy interface 114
custom-queue-list 116

第 2 章 D から F 119
default ip nbar protocol-pack 121
description（クラスマップ） 122
description（サービス グループ） 124
df 125
disconnect qdm 126
drop 128
dscp 130
dscp（カスタム） 133
estimate bandwidth 135
exponential-weighting-constant 137
fair-queue（class-default） 139
fair-queue（DWFQ） 142

fair-queue（policy-map クラス） 145
fair-queue (WFQ) 147
air-queue aggregate-limit 154
fair-queue individual-limit 156
fair-queue limit 158
fair-queue qos-group 160
fair-queue tos 162
fair-queue weight 164
feedback 166
flow idle-timeout 168
flow rate fixed 169
frame-relay interface-queue priority 170
frame-relay ip rtp compression-connections 173
frame-relay ip rtp header-compression 175
frame-relay ip rtp priority 177
frame-relay ip tcp compression-connections 181
frame-relay ip tcp header-compression 183
frame-relay map ip compress 185
frame-relay map ip nocompress 187
frame-relay map ip rtp header-compression 189
group（サービス グループ） 192
hw-module slot（ESP スケジューリング） 194
hw-module subslot（チャネライズド SPA スケジューリング） 197

第 3 章 **identity policy（ポリシーマップ）から ip rsvp pq-profile** 199
identity policy（policy-map） 201
ingress-class-map 203
ip header-compression disable-feedback 205
ip header-compression max-header 207
ip header-compression max-period 209
ip header-compression max-time 211
ip header-compression recoverable-loss 213
ip header-compression old-iphc-comp 215

ip header-compression old-iphc-decomp 216
ip nbar attribute-map 217
ip nbar attribute-set 219
ip nbar classification auto-learn top-hosts 221
ip nbar classification granularity 222
ip nbar classification tunneled-traffic 224
ip nbar custom 225
ip nbar custom transport 230
ip nbar pdlm 233
ip nbar port-map 235
ip nbar protocol-discovery 237
ip nbar protocol-pack 239
ip nbar resources 241
ip nbar resources protocol 242
ip nbar resources system 244
ip options 246
ip rsvp admission-control compression predict 248
ip rsvp aggregation ip 250
ip rsvp aggregation ip map 252
ip rsvp aggregation ip reservation dscp 254
ip rsvp aggregation ip role interior 256
ip rsvp atm-peak-rate-limit 258
ip rsvp authentication 260
ip rsvp authentication challenge 262
ip rsvp authentication key 264
ip rsvp authentication key-chain 266
ip rsvp authentication lifetime 268
ip rsvp authentication neighbor 270
ip rsvp authentication type 274
ip rsvp authentication window-size 277
ip rsvp bandwidth 279
ip rsvp bandwidth ignore 283
ip rsvp bandwidth percent 284
ip rsvp burst policing 287

ip rsvp data-packet classification none 288
ip rsvp dsbm candidate 290
ip rsvp dsbm non-resv-send-limit 292
ip rsvp flow-assist 294
ip rsvp layer2 overhead 296
ip rsvp listener 300
ip rsvp listener outbound 303
ip rsvp msg-pacing 306
ip rsvp neighbor 308
ip rsvp policy cops minimal 310
ip rsvp policy cops report-all 311
ip rsvp policy cops servers 313
ip rsvp policy cops timeout 315
ip rsvp policy default-reject 316
ip rsvp policy identity 318
ip rsvp policy local 321
ip rsvp policy preempt 331
ip rsvp policy vrf 332
ip rsvp pq-profile 334

第 4 章 **ip rsvp precedence から load protocol** 337
ip rsvp precedence 339
ip rsvp qos 342
ip rsvp reservation 343
ip rsvp reservation-host 347
ip rsvp resource-provider 351
ip rsvp sender 353
ip rsvp sender-host 356
ip rsvp signalling dscp 359
ip rsvp signalling fast-local-repair notifications 360
ip rsvp signalling fast-local-repair rate 362
ip rsvp signalling fast-local-repair wait-time 364
ip rsvp signalling hello（コンフィギュレーション） 365
ip rsvp signalling hello（インターフェイス） 366

ip rsvp signalling hello dscp 368
ip rsvp signalling hello graceful-restart 370
ip rsvp signalling hello graceful-restart dscp 371
ip rsvp signalling hello graceful-restart mode 372
ip rsvp signalling hello graceful-restart mode help-neighbor 374
ip rsvp signalling hello graceful-restart neighbor 376
ip rsvp signalling hello graceful-restart refresh interval 378
ip rsvp signalling hello graceful-restart refresh misses 380
ip rsvp signalling hello graceful-restart send 382
ip rsvp signalling hello refresh interval 384
ip rsvp signalling hello refresh misses 386
ip rsvp signalling hello reroute dscp 388
ip rsvp signalling hello reroute refresh interval 390
ip rsvp signalling hello reroute refresh misses 391
ip rsvp signalling hello statistics 392
ip rsvp signalling initial-retransmit-delay 393
ip rsvp signalling patherr state-removal 394
ip rsvp signalling rate-limit 396
ip rsvp signalling refresh interval 398
ip rsvp signalling refresh misses 400
ip rsvp signalling refresh reduction 402
ip rsvp signalling refresh reduction ack-delay 404
ip rsvp snooping 405
ip rsvp source 407
ip rsvp svc-required 409
ip rsvp tos 411
ip rsvp transport 414
ip rsvp transport sender-host 416
ip rsvp tunnel overhead-percent 418
ip rsvp udp-multicasts 420
ip rsvp udp neighbor 422
ip rtp compression-connections 423
ip rtp header-compression 425
ip rtp priority 429

ip tcp compression-connections 433
ip tcp header-compression 435
iphc-profile 438
lacp max-bundle 442
lane client qos 443
lane qos database 444
load protocol 446

第 5 章 **match access-group から mls ip pbr** 449
mac packet-classify 451
mac packet-classify use vlan 453
map ip 455
map ipv6 458
map mpls 460
match access-group 462
match application（クラスマップ） 466
match any 470
match atm-clp 472
match atm oam 474
match atm-vci 476
match class-map 478
match cos 481
match cos inner 485
match destination-address mac 486
match discard-class 488
match dscp 490
match field 494
match flow pdp 497
match fr-dlci 499
match input vlan 501
match input-interface 505
match ip dscp 508
match ip precedence 509
match ip rtp 510

match mpls experimental 512
match mpls experimental topmost 515
match not 517
match packet length (class-map) 519
match port-type 522
match precedence 523
match protocol 528
match protocol attribute application-group 541
match protocol attribute category 544
match protocol attribute sub-category 546
match protocol attribute encrypted 549
match protocol attribute tunnel 551
match protocol (NBAR) 553
match protocol potentially (NBAR) 625
match protocol citrix 696
match protocol fasttrack 698
match protocol gnutella 700
match protocol http 702
match protocol pppoe-discovery 709
match protocol rtp 711
match qos-group 713
match source-address mac 716
match start 718
match tag (class-map) 721
match vlan (QoS) 722
match vlan inner 724
maximum（ローカル ポリシー） 726
maximum bandwidth ingress 728
maximum bandwidth percent 730
maximum header 732
max-reserved-bandwidth 734
metadata application-params 738
metadata flow 741
metadata flow (troubleshooting) 743

mls ip pbr 746

第 6 章 **mls qos（グローバル コンフィギュレーション モード）から mpls experimental 749**

mls qos（グローバル コンフィギュレーション モード） 751

mls qos（インターフェイス コンフィギュレーション モード） 753

mls qos 10g-only 754

mls qos aggregate-policer 756

mls qos bridged 760

mls qos channel-consistency 761

mls qos cos 762

mls qos cos-mutation 765

mls qos dscp-mutation 766

mls qos exp-mutation 767

mls qos loopback 768

mls qos map 769

mls qos map cos-dscp 772

mls qos map cos-mutation 774

mls qos map dscp-cos 776

mls qos map dscp-exp 778

mls qos map dscp-mutation 780

mls qos map exp-dscp 782

mls qos map exp-mutation 784

mls qos map ip-prec-dscp 786

mls qos map policed-dscp 788

mls qos marking ignore port-trust 790

mls qos marking statistics 791

mls qos mpls trust experimental 792

mls qos police redirected 794

mls qos police serial 795

mls qos protocol 796

mls qos queueing-only 799

mls qos queue-mode mode-dscp 801

mls qos rewrite ip dscp 802

mls qos statistics-export（グローバル コンフィギュレーション） 804

mls qos statistics-export（インターフェイス コンフィギュレーション） 806
mls qos statistics-export aggregate-policer 808
mls qos statistics-export class-map 810
mls qos statistics-export delimiter 813
mls qos statistics-export destination 814
mls qos statistics-export interval 817
mls qos supervisor 10g-only 819
mls qos trust 821
mls qos trust extend 824
mls qos tunnel gre input uniform-mode 826
mls qos vlan-based 827
monitor pids 829
mpls experimental 830

第 7 章 N から P 833
non-tcp 835
non-tcp contexts 836
oam-bundle 838
platform ip features sequential 841
platform ipsec fips-mode 844
platform ipsec llq 845
platform punt-police queue 846
platform qos marker-statistics 849
platform qos match-statistics per-ace 851
platform qos match-statistics per-filter 853
platform qos-port-channel_aggregator 855
platform qos-port-channel_multiple_active 856
platform vfi dot1q-transparency 857
plim qos input 859
plim qos input map 862
plim qos input map cos（VLAN の CoS 値を分類） 868
police 871
police (EtherSwitch) 882
police（percent） 884

police（ポリシー マップ） 892
police（2 つのレート） 900
police rate（コントロールプレーン） 908
police rate pdp 914
policy-map 918
policy-map copp-peruser 926
precedence 927
precedence（WRED グループ） 931
preempt-priority 934
priority 936
priority（10000 シリーズ） 940
priority（SIP400） 943
priority-group 946
priority level 949
priority-list default 952
priority-list interface 954
priority-list protocol 956
priority-list queue-limit 961
priority-queue cos-map 963
priority-queue queue-limit 965
pvc-bundle 967

第 8 章 Q から R 971
qos police order parent-first 973
qos pre-classify 974
qos shape-timer 976
queue-depth 978
queue-limit 980
queue-limit atm clp 987
queue-list default 989
queue-list interface 991
queue-list lowest-custom 993
queue-list protocol 995

queue-list queue byte-count 998
queue-list queue limit 1000
random-detect 1002
random-detect（VC 単位） 1008
random-detect aggregate 1012
random-detect atm-clp-based 1016
random-detect clp 1018
random-detect cos-based 1020
random-detect discard-class 1022
random-detect discard-class-based 1026
random-detect dscp 1027
random-detect dscp（aggregate） 1035
random-detect ecn 1040
random-detect exponential-weighting-constant 1041
random-detect flow 1045
random-detect flow average-depth-factor 1047
random-detect flow count 1049
random-detect prec-based 1051
random-detect precedence 1053
random-detect precedence（aggregate） 1058
random-detect-group 1062
rate 1065
rate-limit 1066
rcv-queue bandwidth 1071
rcv-queue cos-map 1073
rcv-queue queue-limit 1075
rcv-queue random-detect 1077
rcv-queue threshold 1079
recoverable-loss 1082
redirect interface 1084
refresh max-period 1086
refresh max-time 1088
refresh rtp 1090
rtp 1092

第 9 章

send qdm message から show atm bundle svc statistics 1095

sdm prefer enable_portchannel_qos_multiple_active 1097

sdm prefer disable_portchannel_qos_multiple_active 1098

send qdm message 1099

service-group 1101

service-policy 1102

service-policy（クラスマップ） 1114

service-policy（コントロール プレーン） 1116

service-policy（ポリシーマップ クラス） 1119

service-policy（サービス グループ） 1122

service-policy type qos 1123

set atm-clp 1124

set cos 1126

set cos cos-inner（ポリシーマップ コンフィギュレーション） 1131

set cos-inner 1134

set cos-inner cos 1136

set discard-class 1138

set dscp 1139

set fr-de 1143

set ip dscp 1145

set ip dscp（ポリシー マップ コンフィギュレーション） 1146

set ip dscp tunnel 1149

set ip precedence（ポリシー マップ コンフィギュレーション） 1152

set ip precedence（ポリシー マップ） 1155

set ip precedence（ルートマップ） 1156

set ip precedence tunnel 1159

set ip tos（ルートマップ） 1161

set precedence 1164

set qos-group 1168

set vlan inner 1172

shape 1173

shape (percent) 1175

shape（policy-map クラス） 1179
shape adaptive 1186
shape fecn-adapt 1188
shape max-buffers 1190
show access-lists rate-limit 1192
show atm bundle 1194
show atm bundle stat 1196
show atm bundle svc 1198
show atm bundle svc stat 1200

第 10 章 **show auto discovery qos から show ip rsvp hello client lsp detail** 1203
show auto discovery qos 1205
show auto qos 1209
show class-map 1214
show class-map type nat 1217
show class-map type port-filter 1219
show control-plane cef-exception counters 1221
show control-plane cef-exception features 1223
show control-plane counters 1225
show control-plane features 1227
show control-plane host counters 1229
show control-plane host features 1231
show control-plane host open-ports 1233
show control-plane transit counters 1236
show control-plane transit features 1238
show cops servers 1240
show crypto eng qos 1241
show crypto entropy status 1242
show frame-relay ip rtp header-compression 1244
show frame-relay ip tcp header-compression 1249
show interfaces fair-queue 1252
show interfaces random-detect 1255
show interfaces rate-limit 1258
show iphc-profile 1261

show ip nat translations rsvp 1263
show ip nbar attribute 1265
show ip nbar classification auto-learn top-asymmetric-sockets 1268
show ip nbar link-age 1271
show ip nbar classification auto-learn top-hosts 1273
show ip nbar classification granularity 1274
show ip nbar pdlm 1275
show ip nbar port-map 1276
show ip nbar protocol activated 1278
show ip nbar protocol-attribute 1279
show ip nbar protocol-discovery 1281
show ip nbar protocol-id 1285
show ip nbar protocol-pack 1298
show ip nbar resources flow 1300
show ip nbar statistics 1301
show ip nbar trace 1302
show ip nbar unclassified-port-stats 1304
show ip nbar version 1307
show ip rsvp 1310
show ip rsvp aggregation ip 1317
show ip rsvp aggregation ip endpoints 1321
show ip rsvp atm-peak-rate-limit 1325
show ip rsvp authentication 1327
show ip rsvp counters 1333
show ip rsvp counters state teardown 1337
show ip rsvp fast bw-protect 1339
show ip rsvp fast detail 1341
show ip rsvp fast-reroute 1345
show ip rsvp fast-reroute bw-protect 1349
show ip rsvp fast-reroute detail 1353
show ip rsvp hello 1359
show ip rsvp hello client lsp detail 1361

第 11 章 **show ip rsvp hello client lsp summary から show lane qos database** 1363

show ip rsvp hello client lsp summary 1365
show ip rsvp hello client nbr detail 1367
show ip rsvp hello client neighbor detail 1369
show ip rsvp hello client neighbor summary 1371
show ip rsvp hello graceful-restart 1373
show ip rsvp hello instance detail 1375
show ip rsvp hello instance summary 1379
show ip rsvp hello statistics 1382
show ip rsvp high-availability counters 1384
show ip rsvp high-availability database 1390
show ip rsvp high-availability summary 1409
show ip rsvp host 1414
show ip rsvp host vrf 1418
show ip rsvp ingress 1420
show ip rsvp installed 1422
show ip rsvp interface 1432
show ip rsvp interface detail 1450
show ip rsvp listeners 1452
show ip rsvp neighbor 1455
show ip rsvp p2mp counters 1459
show ip rsvp policy 1461
show ip rsvp policy cops 1463
show ip rsvp policy identity 1464
show ip rsvp policy local 1467
show ip rsvp policy vrf 1475
show ip rsvp precedence 1478
show ip rsvp request 1480
show ip rsvp reservation 1489
show ip rsvp sbm 1501
show ip rsvp sender 1504
show ip rsvp signalling 1539
show ip rsvp signalling blockade 1542
show ip rsvp signalling fast-local-repair 1545
show ip rsvp signalling rate-limit 1551

show ip rsvp signalling refresh 1553
show ip rsvp snooping 1555
show ip rsvp tos 1556
show ip rsvp transport 1558
show ip rsvp transport sender 1560
show ip rtp header-compression 1563
show ip tcp header-compression 1566
show ip vrf 1569
show lane qos database 1574

第 12 章 **show mls qos から wrr-queue threshold** 1577
show metadata application table 1580
show metadata flow 1582
show mls qos 1589
show mls qos aggregate policer 1594
show mls qos free-agram 1596
show mls qos interface 1597
show mls qos maps 1599
show mls qos mpls 1603
show mls qos protocol 1605
show mls qos queuing interface 1606
show mls qos statistics-export info 1610
show platform hardware acl entry global-qos 1612
show platform hardware pp active infrastructure pi npd rx policer 1614
show platform hardware qfp active feature qos config global 1616
show platform lowq 1618
show platform qos policy-map 1619
show platform software infrastructure punt statistics 1622
show policy-manager events 1624
show policy-manager policy 1626
show policy-map 1628
show policy-map class 1645
show policy-map control-plane 1647
show policy-map interface 1651

show policy-map interface brief 1704
show policy-map interface port-channel 1716
show policy-map interface service group 1718
show policy-map interface service instance 1721
show policy-map mgre 1726
show policy-map multipoint 1729
show policy-map session 1731
show policy-map target service-group 1739
show policy-map type access-control 1741
show policy-map type nat 1744
show policy-map type port-filter 1746
show protocol phdf 1748
show qbm client 1751
show qbm pool 1753
show qdm status 1756
show queue 1758
show queueing 1764
show queueing interface 1772
show random-detect-group 1777
show running-config service-group 1780
show sdm prefer current 1782
show service-group 1783
show service-group interface 1786
show service-group state 1788
show service-group stats 1789
show service-group traffic-stats 1792
show subscriber policy ppm-shim-db 1794
show table-map 1795
show tech-support nbar platform 1797
show tech-support rsvp 1813
show traffic-shape 1814
show traffic-shape queue 1817
show traffic-shape statistics 1822
show vrf 1825

show wrr-queue 1829
subscriber accounting accuracy 1830
svc-bundle 1831
table-map（値マッピング） 1832
tcp 1835
tcp contexts 1836
traffic-shape adaptive 1838
traffic-shape fecn-adapt 1840
traffic-shape group 1842
traffic-shape rate 1845
trust 1848
tx-ring-limit 1850
vbr-nrt 1852
vc-hold-queue 1857
wrr-queue bandwidth 1858
wrr-queue cos-map 1860
awrr-queue dscp-map 1862
wrr-queue queue-limit 1864
wrr-queue random-detect 1866
wrr-queue threshold 1868

A から C

- access-list rate-limit （3 ページ）
- account （6 ページ）
- admit cac local （8 ページ）
- atm-address（qos） （9 ページ）
- attribute （11 ページ）
- auto discovery qos （12 ページ）
- auto qos （14 ページ）
- auto qos voip （16 ページ）
- auto qos voip（6500） （19 ページ）
- bandwidth（policy-map クラス） （23 ページ）
- bandwidth qos-reference （35 ページ）
- bandwidth remaining ratio （39 ページ）
- bump （45 ページ）
- bundle （49 ページ）
- bundle svc （51 ページ）
- class（EtherSwitch） （53 ページ）
- class（ポリシー マップ） （56 ページ）
- class-map arp-peruser （64 ページ）
- class-bundle （65 ページ）
- class-map （68 ページ）
- class-map arp-peruser （75 ページ）
- class type tag （76 ページ）
- clear control-plane （78 ページ）
- clear ip nbar （80 ページ）
- clear ip nbar classification auto-learn top-hosts （82 ページ）
- clear ip nbar protocol-discovery （83 ページ）
- clear ip rsvp authentication （84 ページ）
- clear ip rsvp counters （86 ページ）
- clear ip rsvp hello instance counters （87 ページ）

- clear ip rsvp hello instance statistics （89 ページ）
- clear ip rsvp hello statistics （91 ページ）
- clear ip rsvp high-availability counters （93 ページ）
- clear ip rsvp msg-pacing （94 ページ）
- clear ip rsvp reservation （96 ページ）
- clear ip rsvp sender （98 ページ）
- clear ip rsvp signalling fast-local-repair statistics （100 ページ）
- clear ip rsvp signalling rate-limit （101 ページ）
- clear ip rsvp signalling refresh reduction （102 ページ）
- clear mls qos （103 ページ）
- clear service-group traffic-stats （106 ページ）
- compression header ip （107 ページ）
- control-plane （109 ページ）
- copy interface （114 ページ）
- custom-queue-list （116 ページ）

access-list rate-limit

専用アクセス レート（CAR）ポリシーで使用するアクセス リ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 **access-listrate-limit** コマンドを使用します。このコンフィギュレーションからアクセス 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。

access-list rate-limit *acl-index* {*precedencemac-addressexp*|**mask** *mask*}
no access-list rate-limit *acl-index* {*precedencemac-addressexp*|**mask** *mask*}

構文の説明

acl-index	アクセス リスト番号。次のものでパケットを分類します • IP プレシデンス。1 ～ 99 の任意の数値を使用 • MAC アドレス。100 ～ 199 の任意の数値を使用 • マルチプロトコル ラベル スイッチング（MPLS）実験フィールド。200 ～ 299 の任意の数値を使用
precedence	IP プレシデンス。有効値の範囲は 0 ～ 7 です。
mac-address	MAC アドレス。
exp	MPLS 実験フィールド。有効値の範囲は 0 ～ 7 です。
mask *mask*	マスク。同じレート制限アクセス リストに複数の IP プレシデンスまたは MPLS 実験フィールドの値を割り当てる場合は、このオプションを使用します。

コマンド デフォルト

CAR アクセス リストは設定されていません。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
12.1(5)T	このコマンドに MPLS 実験フィールドに基づくアクセス リストが含められました。
12.2(2)T	このコマンドが Cisco IOS Release 12.2(2)T に統合されました。
12.2(4)T	このコマンドが Cisco MGX RPM-PR カードを持つ Cisco MGX 8850 スイッチおよび MGX 8950 スイッチに実装されました。
12.2(4)T2	このコマンドは、Cisco 7500 シリーズに実装されました。
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。

リリース	変更箇所
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

このコマンドを使用して、特定の CAR アクセス リストに対して指定した IP プレシデンス、MACアドレス、またはMPLS実験フィールド値によってパケットを分類します。次に、**rate-limit** コマンドを使用して、個々のレート制限アクセス リストに CAR ポリシーを適用できます。この方法によってアクセス リスト内のパケットが分類される場合は、異なる IP プレシデンス、MAC アドレス、または MPLS 実験フィールド値を持つパケットに、CAR プロセスで異なる処理が行われます。

レート制限アクセス リストごとに、1 つだけのコマンドを指定できます。同じアクセス リスト番号を使用してこのコマンドを複数回入力すると、新しいコマンドが前のコマンドを上書きします。

複数の IP プレシデンスまたは MPLS 実験フィールドの値を同一のレート制限リストに割り当てるには、**mask** キーワードを使用します。**mask** 値を確認するには、次の手順を実行します。

1. このレート制限アクセス リストに割り当てるプレシデンスを決定します。
2. 各ビットを 1 つの値に対応させて、8 ビットの数値をプレシデンスまたはMPLS実験フィールド値に変換します。たとえば、MPLS 実験フィールド値 0 は 00000001 に対応し、1 は 00000010 に対応し、6 は 01000000 に対応し、7 は 10000000 に対応します。
3. 選択した MPLS 実験フィールド値の 8 ビットの数値を加えます。たとえば、MPLS 実験フィールドの値 1 と 6 のマスクは、01000010 です。
4. **access-listrate-limit** コマンドは、16 進形式を予期します。バイナリ マスクを、対応する 16 進数に変換します。たとえば、01000010 は 42 としてコマンドで使用します。1 または 6 の MPLS 実験フィールド値を持つすべてのパケットは、このアクセス リストに一致します。

マスク FF は、すべてのプレシデンスに一致します。また、00 はどのプレシデンスにも一致しません。

例

次の例では、値が 7 の MPLS 実験フィールドがレート制限アクセス リスト 200 に割り当てられます。

```
Router(config)# access-list rate-limit 200 7
```

次に、レート制限がレート制限アクセス リストに一致するパケットのみに適用されるように、そのレート制限アクセス リストを、**rate-limit** コマンドで使用できます。

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# rate-limit input access-group rate-limit 200 8000 8000 8000
conform-action set-mpls-exp-transmit 4 exceed-action set-mpls-exp-transmit 0
```

関連コマンド

コマンド	説明
rate-limit	CAR および DCAR ポリシーを設定します。
showaccess-listsrate-limit	レート制限アクセス リストに関する情報を表示します。

account

このコマンドを設定したトラフィック クラスに対して一致するパケットの統計収集を有効にするには、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、**account** コマンドを使用します。統計収集を無効にするには、このコマンドの **no** 形式を使用します。

account [drop]
no account

構文の説明

drop	（オプション）コマンドを設定するトラフィック クラスに対して破棄されるパケットの統計収集を有効にします。これはデフォルトの動作です。

コマンド デフォルト

account コマンドを設定すると、デフォルトの動作では、破棄される統計を収集します。**account** コマンドが設定されていない場合、統計は収集されません。

コマンド モード

ポリシーマップ クラス（config-pmap-c）

コマンド履歴

リリース	変更箇所
Cisco IOS XE Release 2.6	このコマンドが導入されました。

使用上のガイドライン

account コマンド QoS の一部（Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでサブスクライバごとの統計の収集をサポートする Cisco IOS XE リリース 2.6 のポリシー集約の拡張機能）として実装されました。

設定時のデフォルトでは、このコマンドは、設定したクラスのトラフィックに対して破棄される統計の収集を有効にします。したがって、オプションの **drop** キーワードは、破棄される統計の収集を有効にするために必須ではありません。

showpolicy-mapinterface コマンドを使用すると、特定のトラフィック クラスに対して収集されたサブスクライバの統計を表示できます。

例

サブスクライバのポリシーマップの EF トラフィック クラスに対して、破棄される統計収集（デフォルト）を有効にする例を次に示します。

```
Router(config)# policy-map subscriber
Router(config-pmap)# class EF
Router(config-pmap-c)# account
```

関連コマンド

コマンド	説明
class(policy-map)	作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルト クラス（一般に class-default クラスといいます）を指定します。
policy-map	ポリシーマップ コンフィギュレーション モードを開始し、サービス ポリシーを指定するため 1 つ以上のインターフェイスに適用できるポリシー マップを作成または修正します。
showpolicy-mapinterface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

admit cac local

クラスに対する Per-Flow Admission ポリシーを有効にするには、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 **admitcac local** コマンドを使用します。クラスに対する Per-Flow Admission 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。

admit cac local
no admit cac local

構文の説明

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

Per-Flow Admission は、クラスに対して有効になっていません。

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 モード（config-pmap-c）

コマンド履歴

リリース	変更箇所
15.4(2)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

クラスで Per-Flow Admission を有効にしてフローを検出するには、このコマンドを使用します。Per-Flow Admission ポリシーは、フローを制限し、すでに流入したフローを保護します。

例

```
Device(config-pmap-c)# admit cac local
```

関連コマンド

コマンド	説明
rate	帯域幅プールのサイズを kbps 単位で設定するか、出力クラスの帯域幅のパーセンテージとして設定します。
flow rate fixed	各フローに割り当てる帯域幅の量を指定します。
flow idle-timeout	フローのタイムアウト期間を指定します。

atm-address（qos）

特定の ATM アドレスに関連付けられる QoS パラメータを指定するには、LANE QoS データベース設定モードで **atm-address** 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。

atm-address *atm-address* [**ubr+** **pcr** *value* **mcr** *value*]
no atm-address *atm-address* [**ubr+** **pcr** *value* **mcr** *value*]

構文の説明

atm-address	ATM アドレスを制御します。
ubr+	（オプション）未指定ビット レート プラス（UBR+）仮想チャネル接続（VCC）。
pcr	（オプション）ピーク セル レート（PCR）。
value	（オプション）UBR+ の PCR 値（kbps）。
mcr *value*	（オプション）最小セル レート（MCR）値（kbps）

コマンド デフォルト

デフォルトの ATM アドレスはありません。

コマンド モード

LANE QoS データベース設定

コマンド履歴

リリース	変更箇所
12.1(2)E	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
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。

例

特定の ATM アドレスに関する PCR および MCR の値を使用し、必要な QoS パラメータを入力する方法を、次の例に示します。このコマンドは、LANE QoS データベース設定モードから入力します。

```
Router(lane-qos)# atm-address 47.009181000000061705B0C01.00E0B0951A40.0A ubr+ pcr 500000
 mcr 100000
```

関連コマンド

コマンド	説明
laneclientqos	QoS over LANE データベースをインターフェイスに適用します。
laneqosdatabase	QoS over LANE データベースを構築する処理を開始します。
showlaneqosdatabase	特定の QoS over LANE データベースの内容を表示します。
ubr+cos	CoS 値を UBR+ VCC にマップします。

attribute

属性プロファイルに属性を追加するには、属性マップ コンフィギュレーション モードで **attribute** コマンドを使用します。

attribute *attribute-name attribute-value*

構文の説明

attribute-name	プロファイルに設定する属性の名前。
attribute-value	属性値。

コマンド モード

属性マップ コンフィギュレーション（config-attribute-map）

コマンド履歴

リリース	変更箇所
15.2(4)M2	このコマンドが導入されました。
Cisco IOS XE Release 3.8S	このコマンドが、Cisco IOS XE リリース 3.8S に統合されました。

使用上のガイドライン

このコマンドには **no** 形式はありません。

例

次の例は、application-group 属性をプロファイルに追加する方法を示しています。

```
Device# configure terminal
Device(config)# ip nbar attribute-map nntp-attrib
Device(config-attribute-map)# attribute application-group aol-group
Device(config-attribute-map)# end
```

関連コマンド

コマンド	説明
ip nbar attribute-map	プロトコルの属性を設定します。
ipnbarattribute-set	プロトコルに新しい属性プロファイルをアタッチします。

auto discovery qos

エンタープライズ機能の AutoQoS を設定するためにデータの検出および収集を開始するには、インターフェイス コンフィギュレーション モードで **autodiscoveryqos** コマンドを使用します。データの検出および収集を停止するには、このコマンドの **no** 形式を使用します。

auto discovery qos [trust]
no auto discovery qos

構文の説明

trust	（オプション）パケットの Differentiated Services Code Point（DSCP; DiffServ コード ポイント）のマーキングが音声、ビデオ、およびデータ トラフィックの分類に対する trust（つまり、信頼されていること）を示します。 オプションの **trust** キーワードが指定されない場合、音声、ビデオ、およびデータ トラフィックは、Network-Based Application Recognition（NBAR）を使用して分類されます。また、パケットは適切な DSCP 値でマークされます。

コマンド デフォルト

データ収集は実行されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.3(7)T	このコマンドが導入されました。
12.3(11)T	信頼モードが、プロトコル タイプではなく DSCP 値でパケットが分類されるように変更されました。

使用上のガイドライン

autodiscoveryqos コマンドは、エンタープライズ機能の AutoQoS の自動検出（データ収集）フェーズを開始します。このコマンドは、NBAR Protocol Discovery を呼び出してデータを収集し、インターフェイスの出力方向のトラフィックを分析します。

noautodiscoveryqos コマンドは、自動検出フェーズを終了し、生成されたすべてのデータ収集レポートを削除します。

指定された DSCP マーキングに基づいて、信頼されたモデルに **trust** キーワードを使用します。詳細については、Cisco IOS リリース 12.3(7)T の *AutoQoS for the Enterprise* 機能モジュールの「Trusted Boundary」セクションを参照してください。

例

serial2/1/1 サブインターフェイスでエンタープライズ機能の AutoQoS の自動検出（データ収集）フェーズを有効にした設定例を、次に示します。

```
Router> enable
Router# configure terminal
```

```
Router(config)# interface serial2/1.1
Router(config-if)# frame-relay interface-dlci 58
Router(config-if)# auto discovery qos
Router(config-if)# end
```

関連コマンド

コマンド	説明
autoqos	エンタープライズ機能の AutoQoS によって作成された QoS クラス マップおよびポリシー マップをインストールします。
servicepolicy	入力インターフェイスまたはVC、あるいは出力インターフェイスまたはVCに、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showautoqos	特定のインターフェイスまたはすべてのインターフェイスで AutoQoS によって作成されたインターフェイス コンフィギュレーション、ポリシー マップ、およびクラス マップを表示します。

auto qos

エンタープライズ機能の AutoQoS によって作成された Quality of Service（QoS）クラス マップおよびポリシー マップをインストールするには、インターフェイス コンフィギュレーション モードで **autoqos** コマンドを使用します。QoS 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。

auto qos
no 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

QoS ポリシーはインストールされません。

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	変更箇所
12.3(7)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

エンタープライズ機能の AutoQoS によって自動的に生成されたテンプレートから、クラスマップおよびポリシーマップが作成されます。これらのテンプレート（および結果として作成されるクラス マップとポリシー マップ）は、エンタープライズ機能の AutoQoS の自動検出フェーズで収集したデータに基づいて生成されます。自動検出フェーズの詳細については、Cisco IOS リリース 12.3(7)T の *AutoQoS for the Enterprise* 機能モジュールの「Configuration Phases」セクションを参照してください。

noautoqos コマンドは、インターフェイスにインストールされている、AutoQoS によって生成されたすべてのクラス マップおよびポリシー マップを削除します。

autoqos コマンドは、ギガビット インターフェイスでサポートされていません。

例

serial2/1/1 サブインターフェイスでエンタープライズ機能の AutoQoS を有効にした設定例を、次に示します。この設定では、AutoQoS のクラスマップおよびポリシーマップは、serial2/1 インターフェイスにインストールされます。

```
Router> enable
Router# configure terminal
Router(config)# interface serial2/1
Router(config-if)# frame-relay interface-dlci 58
Router(config-if)# auto qos
Router(config-if)# end
```

関連コマンド

コマンド	説明
servicepolicy	入力インターフェイスまたはVC、あるいは出力インターフェイスまたはVCに、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showautoqos	特定のインターフェイスまたはすべてのインターフェイスで AutoQoS によって作成されたインターフェイス コンフィギュレーション、ポリシー マップ、およびクラス マップを表示します。

auto qos voip

インターフェイスで AutoQoS--VoIP 機能を設定するには、インターフェイス コンフィギュレーション モードまたはフレーム リレー DLCI コンフィギュレーション モードで **autoqosvoip** コマンドを使用します。インターフェイスから AutoQoS--VoIP 機能を削除するには、このコマンドの **no** 形式を使用します。

auto qos voip [trust] [fr-atm]
no auto qos voip [trust] [fr-atm]

構文の説明

trust	（オプション）パケットの Differentiated Services Code Point（DSCP; DiffServ コード ポイント）のマーキングが音声トラフィックの分類に対する trust（つまり、信頼されていること）を示します。オプションの **trust** キーワードが指定されない場合、音声トラフィックは、Network-Based Application Recognition（NBAR）を使用して分類されます。また、パケットは適切な DSCP 値でマークされます。
fr-atm	（オプション）フレーム リレー/ATM 間リンクに対して AutoQoS--VoIP 機能を有効にします。このオプションは、フレーム リレー/ATM 間インターワーキングのみに対するフレーム リレー データ リンク接続識別子（DLCI）で使用可能です。

コマンド デフォルト

デフォルト モードでは無効です。

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）
フレーム リレー DLCI コンフィギュレーション（フレーム リレー DLCI で使用）（config-fr-dlci）

コマンド履歴

リリース	変更箇所
12.2(15)T	このコマンドが導入されました。
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

AutoQoS--VoIP 機能を、フレーム リレー/ATM 間インターワーキングに対して有効にするには、**fr-atm** キーワードを明示的に設定する必要があります。ただし、**fr-atm** キーワードは、低速 DLCI のみに影響します。高速 DLCI には影響しません。

（注） 768 kbps 以下のリンク速度の DLCI は 低速 DLCI と見なされ、768 kbps を超えるリンク速度の DLCI は 高速 DLCI と見なされます。

このコマンドに **trust** キーワードが設定されているかどうかに応じて、AutoQoS--VoIP 機能は自動的に次の 2 つのポリシー マップの 1 つを作成します。

- 「AutoQoS-Policy-Trust」（**trust** キーワードが設定されている場合に作成される）
- 「AutoQoS-Policy-UnTrust」（**trust** キーワードが設定されていない場合に作成される）

これらポリシー マップの両方は、インターフェイスまたは相手先固定接続（PVC）上の Voice over IP（VoIP）トラフィックを処理するように設計されています。また、ネットワークの Quality of Service（QoS）の要件に合わせて変更できます。これらのポリシー マップを変更するには、適切な Cisco IOS コマンドを使用します。

これらのポリシー マップは、**service-policy** コマンドを使用してインターフェイスまたは PVC にアタッチしないでください。この方法でポリシー マップをアタッチすると、AutoQoS--VoIP 機能（つまり、ポリシーマップ、クラスマップ、およびアクセス コントロール リスト [ACL]）は、**noautoqosvoip** コマンドの設定時に適切に削除されません。

同一のネットワーク内で ATM PVC と相互接続されている低速フレーム リレー DLCI の場合は、**autoqosvoip** コマンドで **fr-atm** キーワードを明示的に設定し、AutoQoS--VoIP 機能を適切に設定する必要があります。つまり、コマンドを **autoqosvoipfr-atm** として設定する必要があります。

フレーム リレー/ATM 間によって設定される低速フレーム リレー DLCI では、マルチリンク PPP（MLP）over Frame Relay（MLPoFR）が自動的に設定されます。サブインターフェイスには IP アドレスが必要です。MLPoFR の設定時、この IP アドレスは削除され、MLP バンドルに置かれます。**autoqosvoip** コマンドを使用し、ATM 側で AutoQoS--VoIP 機能を設定する必要もあります。

autoqosvoip コマンドは、サブインターフェイスまたはギガビット インターフェイスでサポートされていません。

autoqosvoip コマンドは、フレーム リレー DLCI に対して使用可能です。

AutoQoS--VoIP の無効化

noautoqosvoip コマンドは、AutoQoS--VoIP 機能を無効にし、この機能に関連付けられた設定を削除します。

noautoqosvoip コマンドを使用すると、AutoQoS--VoIP 機能によって最初に生成された個々のコマンドの **no** 形式が設定されます。個々のコマンドの **no** 形式を使用すると、システムのデフォルトが復元されます。コマンドの **no** 形式は、ユーザがコマンドを個別に入力するのと同様に適用されます。デフォルト設定を復元する設定が適用されるにしたがって、コマンドの処理によって生じるメッセージが表示されます。

（注） **noautoqosvoip** コマンドを設定することなくサブインターフェイスまたは PVC を削除した場合（ATM の場合もフレーム リレー PVC の場合も）、AutoQoS--VoIP 機能は適切に削除されません。

例

シリアルのポイントツーポイント サブインターフェイス 4/1.2 で AutoQoS--VoIP 機能を設定した例を、次に示します。この例では、**trust** と **fr-atm** の両方のキーワードが設定されています。

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/1.2 point-to-point
Router(config-if)# bandwidth 100
Router(config-if)# ip address 192.168.0.0 255.255.255.0
Router(config-if)# frame-relay interface-dlci 102
Router(config-fr-dlci)# auto qos voip trust fr-atm
Router(config-fr-dlci)# end
Router(config-if#

exit
```

関連コマンド

コマンド	説明
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showautoqos	特定のインターフェイスまたはすべてのインターフェイスで、AutoQoS--VoIP 機能によって作成された設定を表示します。

auto qos voip（6500）

Voice over IP（VoIP）ポート インターフェイスで AutoQoS 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 **autoqosvoip** コマンドを使用します。このコンフィギュレーションから AutoQos を削除するには、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 に対して Quality of Service（QoS）入力マクロを有効にします。
cisco-softphone	Cisco IP SoftPhone に対して QoS 入力マクロを有効にします。
trust	Differentiated Services Code Point（DSCP; DiffServ コード ポイント）およびサービス クラス（CoS）トラフィック マーキングを信頼しているポートに対して AutoQoS を指定します。

コマンド デフォルト

AutoQos は、DSCP および CoS トラフィック マーキングを信頼します。

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	変更箇所
12.2(33)SXH	このコマンドが導入されました。

使用上のガイドライン

autoqosvoip コマンドは、ギガビット インターフェイスでサポートされていません。

QoS（AutoQoS）の自動化を使用すると、特定のポートに必要な QoS パラメータのタイプを指定できます。たとえば、**autoqosvoipcisco-softphone** コマンドを入力すると、Cisco IP SoftPhone に対して QoS 入力マクロを有効にすることができます。

Smartports 機能は、特定のアプリケーションに関連するすべてのスイッチ設定を、単一のコマンドで設定するためのツール セットを提供します。たとえば、**autoqosvoipcisco-phone** コマンドを入力すると、IP フォンをスイッチに接続するために必要なすべての設定が構成されます。

showautoqos コマンドを入力すると、設定済みの AutoQoS マクロを表示できます。

AutoQoS と Smartports は、次のモジュールでサポートされています。

- WS-X6548-RJ45
- WS-X6548-RJ21
- WS-X6148-GE_TX
- WS-X6548-GE-TX-CR
- WS-X6148-RJ45V

- WS-X6148-RJ21V
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6248-TEL

（注） **noautoqosvoip** インターフェイス コンフィギュレーション コマンドは、QoS をグローバルに無効にすることはありません。また、AutoQoS によって作成された受信済みの CoS/内部 DSCP マップを削除することもありません。

autoqosvoipcisco-phone および **autoqosvoipcisco-softphone** コマンドを使用すると、インターフェイスの AutoQoS に対して、受信 QoS 設定マクロを有効にすることができます。場合によっては、インターフェイスに固有の **autoqosvoip** コマンドを使用して、グローバルに適用される設定コマンドを生成することもできます。

autoqosvoipcisco-phone コマンドを入力した場合は、**switchport** コマンドを使用してインターフェイスを設定する必要があります。**autoqosvoipcisco-softphone** コマンドを入力した場合、**switchport** コマンドを入力してインターフェイスを設定することはできません。

switchport コマンドを使用してインターフェイスを設定する場合は、AutoQoS によってインターフェイスが CoS を信頼するように設定されます。**switchport** コマンドを使用してインターフェイスを設定しない場合は、AutoQoS によってインターフェイスが DSCP を信頼するように設定されます。

AutoQoS は、デフォルト以外の CoS/DSCP マップを使用します。このため、ポート ASIC ベースでポートの信頼を設定する必要があります。

autoqosvoipcisco-phone コマンドを入力すると、次の動作が発生します。

- QoS が無効になっている場合は、有効になります。
- ポートは、ポートベースの QoS に変更されます。
- 適切な CoS マップが設定されます。
- （該当する場合）すべてのポートは、ポートベースのモードに変更されます。
- trust-CoS QoS ポリシーが作成され、trust-CoS QoS ポリシーが必要なポート（COIL2 と COIL1）に適用されます。
- ポート上で信頼境界を有効にします。
- 信頼境界の CoS 値が 0 に設定されます。
- ポートの信頼は、trust-cos に設定されます。
- 10/100 ポートと 10/100/1000 ポートのみがサポートされています。
- CDP バージョンがバージョン 2 でない場合、警告メッセージが表示されます。

autoqosvoipcisco-softphone コマンドを入力すると、次の動作が発生します。

- **cisco-softphone** マクロは、**cisco-phone** マクロのスーパーセットであり、Cisco IP Phone が Catalyst 6500 シリーズ スイッチで適切に動作するために必要なすべての機能を設定します。
- VoIP パケットを分類し、プライオリティ キューまたは別の低遅延キューに登録するため、AutoQoS ポリシー マップ、クラス マップ、およびアクセス リストのグローバル設定が作成されます。インターフェイスの設定は、インターフェイスのタイプとリンク速度に応じて作成されます。
- cisco-softphone ポートベースの AutoQoS マクロが実行されるインターフェイスには、2 つのレートリミッタが関連付けられています。2つのレートリミッタによって、cisco-softphone ポートのすべての着信トラフィックに次の特性が確保されます。
  - DSCP 46 のレートは、予期されたソフトフォン レート以下。
  - DSCP 26 のレートは、予期されたシグナリング レート以下。
  - その他すべてのトラフィックは DSCP 0（デフォルト トラフィック）に再マークされる。
- DSCP-46 は、バーストが 2 KB の 320 Kbps のレートでポリシングされます。DSCP 26 は、バーストが 8 KB の 32 Kbps でポリシングされます。
- ポートは、すべてのポートタイプに対して信頼できないものとして設定されます。ポリシング済み DSCP マップでは、DSCP 46 が DSCP 0 にマークダウンされ、DSCP 26 が DSCP 0 にマークダウンされるように設定されます。デフォルトの QoS IP ACL は、他のすべてのトラフィックを DSCP 0 に再マークします。

autoqosvoipsoft-phone コマンドを入力すると、次の動作が発生します。

- QoS が無効な場合、QoS を有効にします。
- ポートベースの QoS にポートを変更します。
- 適切なポリシング済み DSCP マップを設定します。
- 適切な CoS/DSCP マップを設定します。
- （該当する場合）すべてのポートをポートベースのモードに変更します。
- 必要なポートに、trust-dscp QoS ポリシーを作成します（COIL2 と COIL1）。
- trust-dscp QoS ポリシーをポート（COIL2 と COIL1）に適用します。
- ポート上で信頼境界を無効にします。
- 信頼を untrusted に変更します。
- 10/100 ポートと 10/100/1000 ポートのみを許可します。
- 2 つのレートリミッタを適用します。1 つは DSCP 46、もう 1 つは DSCP 26 着信トラフィック用です。着信の DSCP 46 および DSCP 26 トラフィックに限り信頼します。

- トラフィックのレート制限結果のいずれかの違反を DSCP 0 にマークダウンします。
- その他すべて（DSCP 26 および 46 以外）の着信トラフィックを DSCP 0 に再マークします。

autoqosvoiptrust コマンドを入力すると、次のようになります。

- DSCP および CoS マーキングは、音声トラフィックの分類に対して信頼されます。
- QoS が無効な場合、QoS を有効にします。
- ポートベースの QoS にポートを変更します。
- （該当する場合）すべてのポートをポートベースのモードに変更します。
- 必要なポートに、trust-dscp および trust-cos QoS ポリシーを作成します（COIL2 と COIL1）。
- trust-dscp および trust-cos QoS ポリシーをポート（COIL2 と COIL1）に適用します。
- ポート上で信頼境界を無効にします。
- ポートの信頼を trust-cos に設定します。
- すべてのポートがサポートされます。
- dscp-to-q マッピングを許可するすべてのポートに対して、キューイングを DSCP に基づいて実行します。許可されていない場合は、キューイングを CoS に基づいて実行します。

例

Cisco IP Phone に対して QoS 入力マクロを有効にする方法を、次の例に示します。

```
Router(config-if)# auto qos voip cisco-phone
```

関連コマンド

コマンド	説明
showautoqos	AutoQoS 情報を表示します。
showrunning-configinterface	インターフェイスのステータスと設定を表示します。
switchport	LAN インターフェイスをレイヤ 2 スイッチド インターフェイスとして設定します。

bandwidth（policy-map クラス）

ポリシーマップに属するクラスに割り当てられる帯域幅を指定または変更するには、あるいは ATM オーバーヘッド アカウンティングを有効にするには、QoS 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 **bandwidth** コマンドを使用します。クラスに指定されている帯域幅を削除するか、または ATM オーバーヘッド 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。

bandwidth {*kbps*|[**remaining**] **percent** *percentage*} [**account** {**qinq**|**dot1q**} **aal5** *subscriber-encapsulation*]
no bandwidth

Cisco 10000 シリーズ ルータ（PRE3）
bandwidth {*kbps*|[**remaining**] **percent** *percentage*} **account** {**qinq**|**dot1q**} {**aal5**|**aal3**} *subscriber-encapsulation***user-defined** *offset* **[atm]**
no bandwidth

構文の説明

kbps	クラスに割り当てる帯域幅の量（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応じて変わります。値は 1 ～ 2,000,000 kbps である必要があります。
remaining	（オプション）保証帯域幅の割合は、使用可能な帯域幅の相対パーセントに基づくように指定します。
percent *percentage*	プライオリティ クラスのために確保される利用可能な帯域幅の絶対パーセントまたは使用可能な帯域幅の相対パーセントに基づいて、保証帯域幅のパーセンテージを指定します。有効な指定範囲は 1 ～ 100 です。
account	（任意）ATMオーバーヘッド アカウンティングをイネーブルにします。
qinq	（任意）ATM オーバーヘッド アカウンティングのデジタル加入者線アクセス マルチプレクサ（DSLAM）のカプセル化タイプに対して、キューインキューのカプセル化をブロードバンド アグリゲーション システム（BRAS）として指定します。
dot1q	（任意）ATM オーバーヘッド アカウンティングの BRAS-DSLAM カプセル化タイプとして IEEE 802.1Q VLAN カプセル化を指定します。
aal5	（オプション）ATM オーバーヘッド アカウンティングの加入者線で ATM アダプテーション層とカプセル化タイプを指定します。AAL5 は、コネクション型の可変ビット レート（VBR）サービスをサポートします。有効なカプセル化タイプについては、「使用上のガイドライン」を参照してください。

subscriber-encapsulation	加入者線のカプセル化のタイプ。有効なカプセル化タイプについては、「使用上のガイドライン」を参照してください。
aal3	コネクションレス型リンクとコネクション型リンクの両方をサポートする ATM アダプテーション層 5 を指定します。**aal3** または **aal5** のいずれかを指定する必要があります。
user-defined *offset*	ルータでの ATM オーバーヘッド計算に使用するオフセット サイズを指定します。 有効な値は、–127 ～ 127 バイトです。0 は有効な値ではありません。 （注） **user-defined** *offset* オプションを指定していない場合、ルータはオフセット サイズを設定します。
atm	ATM オーバーヘッドの計算に ATM セル タックスを適用します。 （注） *offset* オプションと **atm** オプションの両方を設定すると、オフセット サイズに合わせてパケット サイズが調整されてから、ATM セル タックスが追加されます。

コマンド デフォルト

帯域幅は指定されていません。

ATM オーバーヘッド アカウンティングはディセーブルです。

コマンド モード

QoS ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合され、Versatile Interface Processor（VIP）対応型 Cisco 7500 シリーズ ルータに実装されました。
12.0(7)T	このコマンドが変更されました。**percent** キーワードが追加されました。
12.0(17)SL	このコマンドは、Cisco IOS Release 12.0(17)SL に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.0(22)S	このコマンドが変更されました。**percent** キーワードのサポートが Cisco 10000 シリーズ ルータに追加されました。
12.0(23)SX	このコマンドが変更されました。**remaining percent** キーワードのサポートが Cisco 10000 シリーズ ルータに追加されました。
12.1(5)T	このコマンドが Cisco IOS Release 12.1(5)T に統合され、VIP 対応型 Cisco 7500 シリーズ ルータに実装されました。

リリース	変更箇所
12.2(2)T	このコマンドが変更されました。**remaining percent** キーワードが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(31)SB	このコマンドは、Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.2(31)SB2	このコマンドが、Cisco IOS Release 12.0(17)SL に統合され、Cisco 10000 シリーズ ルータの PRE3 に実装され、PRE3 向け Cisco 10000 シリーズ ルータでの ATM オーバーヘッド アカウンティング用に機能拡張されました。
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。
12.2(31)SB6	このコマンドが ATM オーバーヘッドを計算する際のオフセット サイズを指定するように変更され、PRE3 向け Cisco 10000 シリーズ ルータに実装されました。
12.2(33)SRC	このコマンドは、Cisco IOS Release 12.2(33)SRC に統合され、Cisco 7600 シリーズ ルータに実装されました。
12.2(33)SB	このコマンドは、Cisco IOS Release 12.2(33)SB に統合され、Cisco 7300 シリーズ ルータに実装されました。
12.4(20)T	このコマンドが変更されました。モジュラ Quality of Service （QoS）CLI（MQC）を使用する階層型キューイング フレームワーク（HQF）に対するサポートが追加されました。
15.1(1)T	このコマンドが変更されました。*kbps* 引数の許容値が変更されました。8 ～ 2000000 の範囲で値を入力する必要があります。
15.2(1)T	このコマンドが変更されました。offset 引数と kbps 引数の許容値が変更されました。

ポリシー マップ コンフィギュレーション

class-map コマンドで定義されたクラスのポリシー マップを設定する場合は、**bandwidth** コマンドを使用します。**bandwidth** コマンドは、そのクラス内のトラフィックの帯域幅を指定します。クラス ベース均等化キューイング（CBWFQ）は、クラスに属するパケットのウェイトを、クラスに割り当てられた帯域幅から導出します。次に、CBWFQ はこのウェイトを使用して、このクラスのキューを適正に処理します。

帯域幅を持つ完全プライオリティの設定

完全プライオリティで設定できるクラスは1つだけです。その他のクラスは、プライオリティの設定も帯域幅の設定も持てません。他のクラスに最小帯域幅を設定するには、**bandwidthremainingpercent** コマンドを使用します。

Cisco10000シリーズルータ以外のサポートされるすべてのプラットフォームに対するパーセンテージとしての帯域幅の指定

kbps単位で帯域幅の量を指定する以外に、使用可能な帯域幅または総帯域幅に対するパーセント比率で帯域幅を指定することもできます。輻輳の発生中には、そのクラスは、設定されている帯域幅比率に比例した帯域幅で処理されます。帯域幅のパーセンテージは、インターフェイスの帯域幅に基づきます。使用可能な帯域幅とは、インターフェイスの帯域幅からリソース予約プロトコル（RSVP）機能、IP RTP プライオリティ機能、低遅延キューイング（LLQ）機能に予約されているすべての帯域幅の合計を差し引いた帯域幅です。

（注） **bandwidthremainingpercent** コマンドが設定されていると、確実な保証帯域幅が提供されない場合があり、相対的な帯域幅しか確保されないことを念頭に置いておいてください。つまり、クラスの帯域幅は、常にインターフェイスの帯域幅に対する指定されたパーセント比率に比例します。リンク帯域幅が固定されている場合、クラス帯域幅の保証は、設定されているパーセンテージに比例します。リンク帯域幅がわからないか変動する場合、ルータは、kbpsでのクラス保証帯域幅を計算することができません。

Cisco 10000 シリーズ ルータに対するパーセンテージとしての帯域幅の指定

kbps単位で帯域幅の量を指定する以外に、使用可能な帯域幅または総帯域幅に対するパーセント比率で帯域幅を指定することもできます。輻輳の発生中には、そのクラスは、設定されている帯域幅比率に比例した帯域幅で処理されます。最小帯域幅のパーセンテージは、至近の親 シェーピング レートに基づきます。

（注） **bandwidthremainingpercent** コマンドが設定されていると、確実な保証帯域幅が提供されない場合があり、相対的な帯域幅しか確保されないことを念頭に置いておいてください。つまり、クラスの帯域幅は、常にインターフェイスの帯域幅に対する指定されたパーセント比率に比例します。リンク帯域幅が固定されている場合、クラス帯域幅の保証は、設定されているパーセンテージに比例します。リンク帯域幅がわからないか変動する場合、ルータは、kbpsでのクラス保証帯域幅を計算することができません。

ルータは、指定された帯域幅をインターフェイス速度の 1/255（ESR–PRE1）または 1/65535（ESR–PRE2）の至近の倍数に変換します。実際の帯域幅を表示するには、**showpolicy-mapinterface** コマンドを使用します。

サポートされているすべてのプラットフォームの制限

bandwidth コマンドには、次の制限事項があります。

- 設定する帯域幅の量は、レイヤ2オーバーヘッドも十分処理できる量にする必要があります。
- ポリシー マップには、同一クラス内で kbps または割合のいずれか（両方ではない）で指定されたすべてのクラスの帯域幅が含まれる場合があります。ただし、プライオリティ クラス内での **priority** コマンドの単位は、非プライオリティ クラスの帯域幅単位と異なっていてもかまいません。
- **bandwidthpercent** コマンドが設定され、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。この制限事項は、**bandwidthremainingpercent** には適用されません。

（注） CSCsy73939 で **bandwidthpercent** コマンドから有効な範囲よりも低い帯域幅値が得られた場合、この値を指定するポリシーマップをインターフェイスに付加することはできません。ルータから「サービス ポリシー出力の親として設定されているパーセンテージは、範囲外の kbps です。許可された範囲は min-value–max-value で、現在の CIR 値は n です。（service-policy output parent Configured Percent results in out of range kbps. Allowed range is *min-value–max-value*. The present CIR value is *n*.）」というエラー メッセージが表示されます。

帯域割り当ての詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Congestion Management Overview」モジュールを参照してください。

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アタッチされて、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ることに注意してください。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。

モジュラ QoS CLI キューの制限

bandwidth コマンドを MQC で使用すると、特定のクラスの帯域幅を指定できます。MQC で使用される場合、**bandwidth** コマンドには、クラスにデフォルトのキュー制限があります。このキュー制限は、**queue-limit** コマンドを使用して変更でき、**bandwidth** コマンドによって設定されたデフォルトが上書きされます。

（注） インターフェイスで必要な最低帯域保証を満たすには、**queue-limit** コマンドを使用して高速インターフェイスのデフォルトのキュー制限を変更します。

Cisco 10000 シリーズ ルータ

Cisco 10000 シリーズ ルータでは、発信インターフェイスのみで**bandwidth** コマンドがサポートされます。着信インターフェイスでは、このコマンドはサポートされません。

PRE2 で、帯域幅値と帯域幅値の単位を指定します。帯域幅の有効な値は 1 ～ 2488320000 です。単位は bps、kbps、mbps、および gbps です。デフォルトの単位は kbps です。たとえば、次のコマンドは 10000 bps と 10000 kbps の帯域幅を PRE2 に設定します。

```
bandwidth 10000 bps
bandwidth 10000
```

PRE3 で指定するのは、帯域幅値のみです。単位は常に kbps であるため、PRE3 は unit 引数をサポートしません。有効な値は 1 ～ 2000000 です。たとえば、次のコマンドは、PRE3 に 128,000 kbps の帯域幅を設定します。

```
bandwidth 128000
```

PRE3 は、PRE2 **bandwidth** コマンドが unit 引数なしで使用される場合に限り、このコマンドを受け入れます。PRE3 は、PRE3 の有効な帯域幅値の範囲外の帯域幅が指定された場合（1 ～ 2000000）、PRE2 **bandwidth** コマンドを拒否します。

kbps 単位で帯域幅の量を指定する以外に、使用可能な帯域幅または総帯域幅に対するパーセント比率で帯域幅を指定することもできます。輻輳の発生中には、そのクラスは、設定されている帯域幅比率に比例した帯域幅で処理されます。帯域幅のパーセンテージは、インターフェイスの帯域幅に基づきます。ただし、階層型ポリシーでは、最小帯域幅のパーセンテージは至近の親シェーピング レートに基づきます。

（注） **bandwidthremainingpercent** コマンドが設定されていると、確実な保証帯域幅が提供されない場合があり、相対的な帯域幅しか確保されない可能性があります。クラスの帯域幅は、常にインターフェイスの帯域幅に対する指定されたパーセンテージに比例します。リンク帯域幅が固定されている場合、クラス帯域幅の保証は、設定されているパーセンテージに比例します。リンク帯域幅がわからないか変動する場合、ルータは、kbps でのクラス保証帯域幅を計算することができません。

ルータは、指定された帯域幅をインターフェイス速度の 1/255（PRE1）または 1/65535（PRE2、PRE3）の至近の倍数に変換します。実際の帯域幅を表示するには、**showpolicy-mapinterface** コマンドを使用します。

ATM のオーバーヘッド アカウンティング（Cisco 10000 シリーズ ルータ）

ATM オーバーヘッド アカウンティングを設定する場合は、BRAS-DSLAM、DSLAM-CPE、および加入者線カプセル化タイプを指定する必要があります。ルータは、次の加入者線カプセル化タイプをサポートします。

- mux-1483routed
- mux-dot1q-rbe

- snap-pppoa
- mux-rbe
- snap-1483routed
- snap-dot1q-rbe
- mux-pppoa
- snap-rbe

user-defined *offset* オプションを指定していない場合、ルータはオフセット サイズを計算します。

階層型ポリシーでは、次の方法で ATM オーバーヘッド アカウンティングを設定します。

- 親で有効：親ポリシー上の ATM オーバーヘッド アカウンティングを有効にした場合は、子ポリシー上のアカウンティングを有効にする必要はありません。
- 子および親で有効：子ポリシー上の ATM オーバーヘッド アカウンティングを有効にした場合は、親ポリシー上の ATM オーバーヘッド アカウンティングも有効にする必要があります。

カプセル化タイプは、子および親ポリシーと一致する必要があります。

ユーザ定義のオフセット値は、子および親ポリシーと一致する必要があります。

例

Cisco 10000 シリーズ ルータ：例

次の例では、ポリシー マップ VLAN がクラス Customer1 に帯域幅の 30 % を、クラス Customer2 に帯域幅の 60 % を保証します。VLAN ポリシー マップを 1-Mbps リンクに適用すると、クラス Customer1 に 300 kbps（1 Mbps の 30 %）が保証され、クラス Customer2 に 600 kbps（1 Mbps の 60 %）が保証されて、class-default クラス用に 100 kbps が残ります。class-default クラスが追加の帯域幅を必要としない場合、未使用の 100 kbps はクラス Customer1 とクラス Customer2 が使用できます。両方のクラスが帯域幅を必要としている場合、設定レートに比例して共有します。次の例では、共有比率は 30:60 または 1:2 です。

```
router(config)# policy-map VLAN
router(config-pmap)# class Customer1
router(config-pmap-c)# bandwidth percent 30
router(config-pmap-c)# exit
router(config-pmap)# class Customer2
router(config-pmap-c)# bandwidth percent 60
```

CBWFQ 帯域幅の保証：例

2 つのクラスを持つポリシー マップを作成する方法、CBWFQ のみが設定されている場合に帯域幅を保証する方法、およびポリシーをシリアル インターフェイス 3/2/1 にアタッチする方法を、次の例で示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth percent 25
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/2/1
Router(config-if)# service output policy1
Router(config-if)# end
```

show policy-map コマンドからの次の出力は、ポリシー マップ policy1 の設定を示します。

```
Router# show policy-map policy1

Policy Map policy1
 Class class1
  Weighted Fair Queuing
   Bandwidth 50 (%) Max Threshold 64 (packets)
 Class class2
  Weighted Fair Queuing
   Bandwidth 25 (%) Max Threshold 64 (packets)
```

show policy-map interface コマンドからの出力は、インターフェイス帯域幅の 50% がクラス class1 に対して保証され、25% がクラス class2 に対して保証されることを示しています。この出力には、帯域幅の量がパーセンテージと kbps の両方で示されています。

```
Router# show policy-map interface serial3/2

Serial3/2
Service-policy output:policy1
Class-map:class1 (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match:none
 Weighted Fair Queuing
  Output Queue:Conversation 265
  Bandwidth 50 (%)
  Bandwidth 772 (kbps) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
Class-map:class2 (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match:none
 Weighted Fair Queuing
  Output Queue:Conversation 266
  Bandwidth 25 (%)
```

```
  Bandwidth 386 (kbps) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
Class-map:class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match:any
```

この例では、シリアル インターフェイス 3/2 に合計 1544 kbps の帯域幅があります。輻輳時には、帯域幅の 50%（772 kbps）がクラス class1 に保証され、リンク帯域幅の 25%（386 kbps）がクラス class2 に保証されます。

CBWFQ と LLQ の帯域幅割り当て：例

次の例では、インターフェイスには合計で 1544 kbps の帯域幅があります。輻輳時には、帯域幅の 50%（772 kbps）がクラス class1 に保証され、リンク帯域幅の 25%（386 kbps）がクラス class2 に保証されます。

show policy-map コマンドからの次の出力例は、ポリシー マップ p1 の設定を示します。

```
Router# show policy-map p1
Policy Map p1
 Class voice
  Weighted Fair Queuing
   Strict Priority
   Bandwidth 500 (kbps) Burst 12500 (Bytes)
 Class class1
  Weighted Fair Queuing
   Bandwidth remaining 50 (%) Max Threshold 64 (packets)
 Class class2
  Weighted Fair Queuing
   Bandwidth remaining 25 (%) Max Threshold 64 (packets)
```

シリアル インターフェイス 3/2 での **show policy-map interface** コマンドからの次の出力は、500 kbps の帯域幅がクラス voice1 に対して保証されることを示します。クラス class1 とクラス class2 はそれぞれ、残りの帯域幅の 50 % と 25 % を得ることができます。未割り当ての帯域幅は、class1、class2、およびベストエフォート トラフィック クラス間に比例して分配されます。

（注） 次の出力例では（この項で前出の多くの出力例とは異なり）、class1 と class2 に対する帯域幅の表示はパーセンテージのみです。kbps の数で表現される帯域幅は、**percent** キーワードが **bandwidth remaining** コマンドで使用されたため、表示されていません。**bandwidth remaining percent** コマンドでは、インターフェイスで使用可能な全帯域幅の相対パーセンテージとして帯域幅を割り当てることができます。

```
Router# show policy-map interface serial3/2

Serial3/2
Service-policy output:p1
 Class-map:voice (match-all)
```

```
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:ip precedence 5
  Weighted Fair Queuing
   Strict Priority
   Output Queue:Conversation 264
   Bandwidth 500 (kbps) Burst 12500 (Bytes)
    (pkts matched/bytes matched) 0/0
    (total drops/bytes drops) 0/0
 Class-map:class1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:none
  Weighted Fair Queuing
   Output Queue:Conversation 265
   Bandwidth remaining 50 (%) Max Threshold 64 (packets)
    (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0
 Class-map:class2 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:none
  Weighted Fair Queuing
   Output Queue:Conversation 266
   Bandwidth remaining 25 (%) Max Threshold 64 (packets)
    (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0
 Class-map:class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:any
```

ATM のトラフィック シェーピング オーバーヘッド アカウンティング：例

親ポリシーで ATM オーバーヘッド アカウンティングが有効になっている場合は、**bandwidth** コマンドまたは **shape** コマンドを含まない子トラフィック クラス上で ATM オーバーヘッド アカウンティングを有効にする必要はありません。次に、subscriber_classes という名前の子ポリシー マップの gaming クラスと class-default クラス、および、subscriber_line という名前の親ポリシー マップの class-default クラスで ATM オーバーヘッド アカウンティングが帯域幅に対してイネーブルである設定例を示します。voip クラスおよび video クラスでは、ATM オーバーヘッド アカウンティングが明示的に有効になっていません。これらのプライオリティ キューは、親ポリシーで ATM オーバーヘッド アカウンティングが有効になっているため、オーバーヘッド アカウンティングは暗黙的に有効になります。親ポリシーと子ポリシーの機能で同じカプセル化タイプが使用されていることに注意してください。

```
Router(config)# policy-map subscriber_classes
Router(config-pmap)# class voip
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 8000
Router(config-pmap-c)# exit
Router(config-pmap)# class video
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# police 20
Router(config-pmap-c)# exit
Router(config-pmap)# class gaming
Router(config-pmap-c)# bandwidth remaining percent 80 account aal5 snap-rbe-dot1q
```

```
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining percent 20 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# policy-map subscriber_line
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining ratio 10 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# shape average 512 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# service policy subscriber_classes
```

次の例では、ルータは ATM オーバーヘッドの計算に 20 のオーバーヘッド バイトと ATM セル タックスを使用します。子ポリシーと親ポリシーには必須の一致オフセット値が含まれています。親ポリシーが virtual template 1 に適用されます。

```
Router(config)# policy-map child
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 500 account user-defined 20 atm
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# shape average 30000 account user-defined 20 atm
Router(config-pmap)# exit
Router(config)# exit
Router(config)#
```

関連コマンド

コマンド	説明
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
max-reserved-bandwidth	CBWFQ、LLQ、および IP RTP プライオリティに割り当てるインターフェイス帯域幅のパーセント比率を変更します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
priority	ポリシーマップに属するトラフィックのクラスのプライオリティを指定します。
queue-limit	キューが保持できる、ポリシーマップ内に設定されるクラスポリシーのパケットの最大数を指定または変更します。
random-detect(interface)	WRED または DWRED をイネーブルにします。

コマンド	説明
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detectprecedence	特定の IP precedence に対する WRED パラメータと DWRED パラメータを設定します。
showpolicy-map	指定されたサービスポリシーマップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービスポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

bandwidth qos-reference

物理インターフェイスまたは論理インターフェイスに関する Quality of Service（QoS）のパーセント設定の割合を計算するための参照として使用される帯域幅を設定するには、インターフェイス コンフィギュレーションまたはサブインターフェイス コンフィギュレーション モードで **bandwidthqos-reference** コマンドを使用します。この明示的に指定された参照帯域幅を削除するには、このコマンドの **no** 形式を使用します。

bandwidth qos-reference *bandwidth-amount*
no bandwidth qos-reference *bandwidth-amount*

構文の説明

bandwidth-amount	キロビット/秒（kb/秒）の帯域幅の量。有効な値は 1 ～ 10000000 です。

コマンド デフォルト

このコマンドはディセーブルです。論理インターフェイスの参照帯域幅は、メイン インターフェイスまたはメイン インターフェイスの QoS ポリシーから取得されます。

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）
サブインターフェイス コンフィギュレーション（config-subif）

コマンド履歴

リリース	変更箇所
12.2(33)XNE	このコマンドが導入されました。
15.1(3)T	論理インターフェイスのサポートが、メインインターフェイス、サブインターフェイス、フレーム リレーを含むように拡張されます。
Cisco IOS XE リリース 3.17S	このコマンドが変更されました。論理インターフェイスのサポートが、メインインターフェイスと、サブインターフェイスに拡張されました。このコマンドが、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。

使用上のガイドライン

bandwidthqos-reference コマンドは、論理インターフェイスの QoS パーセント設定の割合を計算するための参照としてのみ使用されます。このコマンドは、論理インターフェイスに対して指定した量の帯域幅を実際に割り当てるわけではありません。

（注） Cisco IOS Release 12.2(33)XNE では、**bandwidthqos-reference** コマンドは、トンネル論理インターフェイスでのみサポートされます。Cisco IOS Release 15.1(3)T では、メイン インターフェイス、サブインターフェイス、フレーム リレー、およびトンネル論理インターフェイスを含むようにサポートが拡張されています。

shape（パーセント）コマンドと police（パーセント）コマンドの互換性

bandwidthqos-reference コマンドは、**shape**（パーセント）コマンドおよび **police**（パーセント）コマンドとの互換性があり、これらのコマンドに関連します。**shape**（パーセント）コマンドを使用すると、インターフェイスで利用可能な帯域幅のパーセンテージに基づいて、平均レートまたはピーク レートのトラフィック シェーピングを設定できます。**police**（パーセント）コマンドを使用すると、インターフェイスで利用可能な帯域幅の割合に基づいて、トラフィック ポリシングを設定できます。

bandwidthqos-reference コマンドは、**shape**（パーセント）コマンドおよび **police**（パーセント）コマンドと、次のようにやりとりします。

- **bandwidthqos-reference** コマンドを使用して帯域幅が指定された場合、**shape**（パーセント）コマンドおよび **police**（パーセント）コマンドは、この指定された量を使用して、それぞれの帯域幅比率を計算します。
- 帯域幅の指定に **bandwidthqos-reference** コマンドが使用されない場合、**shape**（パーセント）コマンドと**police**（パーセント）コマンドは、インターフェイスで利用可能な帯域幅の量を使用して、それぞれの帯域幅比率を計算します。

bandwidth（インターフェイス）コマンドとの互換性

bandwidth（インターフェイス）コマンドを使用すると、インターフェイスに対して継承され、受け取った帯域幅値を設定できます。

bandwidth（インターフェイス）コマンドと **bandwidthqos-reference** コマンドの両方が任意のインターフェイスで有効になっている場合、**bandwidthqos-reference** コマンドによって指定された値は、その特定の物理インターフェイスまたは論理インターフェイスの QoS パーセント設定の割合を計算するための参照として使用されます。**bandwidth**（インターフェイス）コマンドによって指定された値は、無視されます。

以下のサンプル設定で、**bandwidthqos-reference** コマンドの値は 8000 kb/秒、**bandwidth**（インターフェイス）コマンドの値は 900 kb/秒として入力されています。**shapeaveragepercent** コマンドの値は、50 に設定されています。4000000 ビット/秒（8000 kb/秒の 50 パーセント）に設定されている **targetshaperate** コマンドの出力で、その効果は次のように確認できます。

```
Router(config)# interface e0/1
Router(config-if)# bandwidth qos-reference 8000
Router(config-if)# bandwidth 900

Router(config)# interface e0/1
Router(config-if)# bandwidth 900
Router(config-if)# end
Router# show running-config interface e0/1
interface Ethernet0/1
 bandwidth 900
 bandwidth qos-reference 8000
 no ip address
 load-interval 30
end
Router(config-if)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# interface e0/1
Router(config-if)# service-policy out test
Router# show policy-map interface
```

```
 Ethernet0/1
Service-policy output: test
 Class-map: class-default (match-any)
  79 packets, 7837 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 79/7837
  shape (average) cir 4000000, bc 40000, be 40000
  target shape rate 4000000
```

例

bandwidthqos-reference コマンドを設定し、トンネル インターフェイス 1 に対して参照の割合として 2000 kb/秒の帯域幅を割り当てる方法を、次の例に示します。

```
Router> enable
Router# configure terminal
Router(config)# interface tunnel1
Router#(config-if)# bandwidth qos-reference 2000
```

bandwidthqos-reference コマンドを設定し、メイン インターフェイス e0/1 に対して参照の割合として 700 kb/秒の帯域幅を使用する方法を、次の例に示します。

```
Router(config)# interface e0/1
Router(config-if)# bandwidth qos-ref 700
Router(config-if)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# interface e0/1
Router(config-if)# service-policy out test
```

bandwidthqos-reference コマンドを設定し、サブインターフェイス e0/1.1 に対して参照の割合として 500 kb/秒の帯域幅を使用する方法を、次の例に示します。

```
Router(config-subif)# interface e0/1
Router(config-if)# no service-policy out test
Router(config-if)# interface e0/1.1
Router(config-subif)# bandwidth qos-ref 500
Router(config-subif)# service-policy ou test
```

bandwidthqos-reference コマンドを設定し、フレーム リレー インターフェイス s6/0.1 に対して参照の割合として 400 kb/秒の帯域幅を使用する方法を、次の例に示します。

```
Router(config)# no policy-map test
Router(config)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# map-class frame-relay fr1
Router(config-map-class)# service-policy out test
Router(config-map-class)# end
Router# configure terminal
Router(config)# interface s6/0.1
Router(config-subif)# bandwidth qos-ref 400
Router(config-subif)# end
```

関連コマンド

コマンド	説明
bandwidth（インターフェイス）	インターフェイス対して継承され、受け取った帯域幅の値を設定します。
police（パーセント）	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
shape（パーセント）	インターフェイスで使用可能な帯域幅の割合（%）に基づいて、平均レート トラフィック シェーピングとピーク レート トラフィック シェーピングを指定します。

bandwidth remaining ratio

超過帯域幅（優先トラフィックによって使用されていない帯域幅）の量を判断し、非プライオリティ キューに割り当てるために、輻輳時に使用するクラスレベルまたはサブインターフェイスレベルのキューの帯域幅残量割合を指定するには、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、**bandwidthremainingratio** コマンドを使用します。帯域幅残量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。

bandwidth remaining ratio *ratio*
no bandwidth remaining ratio *ratio*
bandwidth remaining ratio *ratio* [**account** {**qinq**|**dot1q**} **[aal5]** {*subscriber-encapsulation*|**user-defined** *offset*}]
no bandwidth remaining ratio *ratio* [**account** {**qinq**|**dot1q**} **[aal5]** {*subscriber-encapsulation*|**user-defined** *offset*}]
bandwidth remaining ratio *ratio*
no bandwidth remaining ratio *ratio*

構文の説明

ratio	その他のサブインターフェイスまたはクラス キューに関する、このサブインターフェイスまたはクラス キューの相対的ウェイト。有効な値は 1 ～ 1000 です。サブインターフェイス レベルでは、デフォルト値はプラットフォームに依存します。クラス キュー レベルでは、デフォルト値は 1 です。
Cisco 7300 シリーズ ルータ、Cisco 7600 シリーズルータ、および Cisco 10000 シリーズ ルータ	
ratio	その他のサブインターフェイスまたはクラス キューに関する、このサブインターフェイスまたはクラス キューの相対的ウェイト。 （注） Cisco 7300 シリーズ ルータおよび 7600 シリーズ ルータの有効値は 1 から 10000 です。また、デフォルト値は 1 です。 （注） Cisco 10000 シリーズ ルータの有効値は 1 ～ 1000 です。また、デフォルト値は 1 です。
account	（オプション）ATM オーバーヘッド アカウンティングを有効にします。
qinq	（オプション）キューインキューのカプセル化を ブロードバンド リモート アクセス サーバ - デジタル加入者線アクセス マルチプレクサ（BRAS-DSLAM）カプセル化タイプとして指定します。

dot1q	（オプション）IEEE 802.1Q VLAN カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。
aal5	（オプション）コネクション型可変ビット レート（VBR）サービスをサポートする ATM アダプテーション層 5 を指定します。
subscriber-encapsulation	（オプション）加入者線でのカプセル化タイプを指定します。カプセル化タイプは、加入者線によって異なります。
user-defined *offset*	（オプション）ルータでの ATM オーバーヘッド計算に使用するオフセット サイズ（バイト単位）を指定します。 （注） Cisco 7300 シリーズ ルータおよび 7600 シリーズ ルータの場合、有効値は -48 ～ +48 です。 （注） Cisco 10000 シリーズ ルータの有効値は -63 ～ +63 です。
Cisco ASR 1000 シリーズ ルータ	
ratio	その他のサブインターフェイスまたはクラス キューに関する、このサブインターフェイスまたはクラス キューの相対的ウェイト。有効な値は 1 ～ 1000 です。サブインターフェイス レベルおよびクラス キュー レベルでは、デフォルトは 1 です。

コマンド デフォルト

ほとんどのプラットフォームでは、デフォルトの帯域幅比率は 1 です。

サブインターフェイス レベルでデフォルトの帯域幅残量割合を使用すると、Cisco 10000 シリーズ ルータは インターフェイス タイプを識別します。サブインターフェイス レベルでは、デフォルトの帯域幅残量割合は、VLAN サブインターフェイスとフレーム リレー データ リンク接続識別子（DLCI）で 1 です。ATM サブインターフェイスの場合、ルータはサブインターフェイス速度に基づいてデフォルトの帯域幅残量割合を計算します。

クラス レベルでデフォルトの帯域幅残量割合を使用すると、Cisco 10000 シリーズ ルータは インターフェイス タイプを識別しません。クラス レベルでは、デフォルトの帯域幅残量割合は 1 です。

コマンド モード

ポリシーマップ クラス（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.2(31)SB2	このコマンドが導入されました。このコマンドが、PRE3 用の Cisco 10000 シリーズ ルータに実装されました。

リリース	変更箇所
12.2(33)SRC	このコマンドが変更されました。コマンドは、Cisco 7600 シリーズ ルータに実装されました。Cisco 7600 シリーズ ルータおよび PRE3 用の Cisco 10000 シリーズ ルータで ATM オーバーヘッド アカウンティング（オプション）をサポートするため、さらにキーワードおよび引数が追加されました。
12.2(33)SB	このコマンドが変更されました。Cisco 7300 シリーズ ルータのサポートが追加されました。ATM オーバーヘッド アカウンティングに関連付けられた追加のキーワードと引数もサポートされるようになりました。
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

Cisco 10000 シリーズ ルータ

スケジューラは、**bandwidthremainingratio** コマンドで指定された比率を使用して、超過帯域幅（優先トラフィックによって使用されていない帯域幅）の量を判断し、輻輳時にクラスレベル キューまたはサブインターフェイスレベル キューの帯域幅残量割合に割り当てます。他のキューまたはサブインターフェイスに対して未使用になっている帯域幅がスケジューラにより割り当てられます。

bandwidthremainingratio コマンドは、同一のポリシー マップの異なるトラフィック クラス内で、別の **bandwidth** コマンドと共存できません。たとえば、次の設定は無効であるため、エラー メッセージが表示されます。

```
policy-map Prec1
 class precedence_0
  bandwidth remaining ratio 10
 class precedence_2
  bandwidth 1000
```

PRE2 の場合、**bandwidthremainingratio** コマンドは、ポリシー マップの同一クラス内で別の **bandwidth** コマンドと共存できます。PRE3 では、**bandwidthremainingratio** コマンドは、同一クラスの別の **bandwidth** コマンドと共存できます。たとえば、PRE3 では、次の設定は無効であるため、エラー メッセージが表示されます。

```
policy-map Prec1
 class precedence_0
  bandwidth 1000
  bandwidth remaining ratio 10
```

階層型ポリシー マップで、適用済みの子キューイング ポリシーで定義された class-default クラスのみしか親ポリシーが持っていない場合、ルータは class-default クラスで **bandwidth** コマンドの **bandwidthremainingratio** 形式のみを受け入れます。

bandwidthremainingratio コマンドは、同一クラスの **priority** コマンドと共存できません。たとえば、次の設定は無効であるため、エラー メッセージが表示されます。

```
policy-map Prec1
```

```
 class precedence_1
  priority
  police percent 30
  bandwidth remaining ratio 10
```

bandwidthremainingratio コマンドが指定されていないすべてのキューは、プラットフォームが指定された最小帯域幅残量割合を取得します。ルータは、設定に基づいて最小の設定情報レート（CIR）を決定します。

ATM オーバーヘッド アカウンティング（オプション）

bandwidthremainingratio コマンドを使用して、ATM オーバーヘッド アカウンティングを有効にすることもできます。ATM オーバーヘッド アカウンティングを有効にするには、「構文の説明」の表で説明されているように **account** キーワードおよび後続のキーワードと引数を使用します。

Cisco 7200 シリーズ ルータ

Cisco 7200 シリーズ ルータでは、**bandwidthremainingratio** コマンドはサポートされていません。Cisco IOS Release 12.2(33)SRD から Cisco IOS Release 12.2(33)SRE にアップグレードした場合は、このコマンドの実行時にパーサー エラーが表示される場合があります。Cisco 7200 シリーズ ルータでは、**bandwidthremainingratio** コマンドの代わりに **bandwidthremainingpercent** コマンドを使用して同じ機能を得ることができます。

例

Cisco 7300 シリーズ ルータ、Cisco 7600 シリーズ ルータ、および Cisco 10000 シリーズ ルータ

ATM サブインターフェイスで帯域幅残量割合を設定する方法を、次の例に示します。この例では、ルータは、可変ビット レートの非リアルタイム（VBR-nrt）PVC 0/200 に対して 50 Mbps のピーク セル レートを保証します。輻輳の期間中、サブインターフェイスは、物理インターフェイスで設定されたその他のサブインターフェイスに対し、帯域幅残量割合 10 をベースとして、超過帯域幅（優先トラフィックによって使用されていない帯域幅）の共有を取得します。

```
policy-map Child
 class precedence_0
  bandwidth 10000
 class precedence_1
  shape average 100000
  bandwidth 100
!
policy-map Parent
 class class-default
  bandwidth remaining ratio 10
  shape average 20000000
  service-policy Child
!
interface ATM2/0/3.200 point-to-point
 ip address 10.20.1.1 255.255.255.0
 pvc 0/200
 protocol ip 10.20.1.2
 vbr-nrt 50000
 encapsulation aal5snap
 service-policy output Parent
```

個々のクラス キューに対して帯域幅残量割合を設定する方法を、次の例に示します。設定済みクラスの一部には、明示的に指定された帯域幅保証と帯域幅残量割合があります。サブインターフェイス レベルで輻輳が発生した場合、クラス キューは、クラス レベルの帯域幅残量割合に基づいて超過帯域幅（優先トラフィックによって使用されていない帯域幅）を取得します。この割合は、precedence_0、precedence_1、precedence_2、および precedence_5 クラスでそれぞれ、20、30、120、および 100 です。通常、precedence_3 クラス（定義済み割合なし）は、子ポリシーに定義された class-default クラスの帯域幅残量割合に基づいて帯域幅を取得します。しかし、この例では、子ポリシーは class-default 帯域幅残量割合を定義していません。したがって、ルータは、precedence_3 トラフィックに対して比率 1 の超過帯域幅を割り当てます。

```
policy-map Child
 class precedence_0
  shape average 100000
  bandwidth remaining ratio 20
 class precedence_1
  shape 10000
  bandwidth remaining ratio 30
 class precedence_2
  shape average 200000
  bandwidth remaining ratio 120
 class precedence_3
  set ip precedence 3
 class precedence_5
  set ip precedence 5
  bandwidth remaining ratio 100
policy-map Parent
 class class-default
  bandwidth remaining ratio 10
  service-policy Child
!
interface GigabitEthernet 2/0/1.10
 encapsulation dot1q 10
 service-policy output Parent
```

オーバーヘッド アカウンティング：例

オプションの **account** キーワードおよび関連付けられたキーワードや引数を使用してオーバーヘッド アカウンティングを設定する方法を、次の例に示します。

```
policy-map subscriber_line
 class class-default
  bandwidth remaining ratio 10 account dot1q aal5 snap-rbe-dot1q
  shape average 512 account dot1q
aal5 snap-rbe-dot1q
  service policy subscriber_classes
```

関連コマンド

コマンド	説明
bandwidthremainingpercent	クラスレベルまたはサブインターフェイスレベルのキューの帯域幅残量パーセンテージを指定します。この帯域幅残量パーセンテージは、優先トラフィックによって使用されていない余分な帯域幅の量を判断し、非プライオリティ キューに割り当てるために輻輳時に使用します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

bump

VC バンドルに割り当てることができる仮想回線（VC）クラスのバンピング ルールを設定するには、VC-class コンフィギュレーション モードで **bump** コマンドを使用します。このクラスに割り当てられている VC の明示的なバンピング ルールを削除し、デフォルトの状態である暗黙的なバンピングに戻すには、**nobumpexplicit** コマンドまたは **bumpimplicit** コマンドを使用します。VC バンドル メンバーがバンピングされたトラフィックを受け入れ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。

バンドルの特定の VC または相手先固定接続（PVC）メンバーにバンピング ルールを設定するには、bundle-vc または SVC-bundle-member コンフィギュレーション モードで **bump** コマンドを使用します。VC または PVC バンドル メンバーの明示的なバンピング ルールを削除し、デフォルトの状態である暗黙的なバンピングに戻すには、**bumpimplicit** コマンドを使用します。VC または PVC バンドル メンバーがバンピングされたトラフィックを受け入れないように指定するには、**nobumptraffic** コマンドを使用します。

bump {**explicit** *precedence-level*|**implicit**|**traffic**}
no bump {**explicit** *precedence-level*|**implicit**|**traffic**}

構文の説明

explicit *precedence-level*	VC または PVC が停止した場合に、VC または PVC 上のトラフィックがバンピングされる優先レベルを指定します。*precedence-level* 引数の有効な値は 0 ～ 7 です。
implicit	デフォルトの暗黙的なバンピング ルールを単一の VC、PVC バンドル メンバー、またはバンドル内のすべての VC に適用します（VC-class モード）。暗黙的なバンピング ルールは、バンピングされたトラフィックが VC または PVC によって低い優先レベルで送信されるように規定します。
traffic	VC または PVC がバンピングされたトラフィックを受け入れるように指定します（デフォルトの状態）。**no** 形式は、VC または PVC がバンピングされたトラフィックを受け入れないように規定します。

コマンド デフォルト

暗黙的なバンピング

バンピングを許可（VC はバンピングされたトラフィックを受け入れます）

コマンド モード

Vc-class コンフィギュレーション（VC クラスの場合）
Bundle-vc コンフィギュレーション（ATM VC バンドル メンバーの場合）
SVC-bundle-member コンフィギュレーション（SVC バンドル メンバーの場合）

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。

リリース	変更箇所
12.2(4)T	このコマンドが、SVC-bundle-member コンフィギュレーション モードで使用できるようになりました。
12.0(23)S	このコマンドが、Cisco 12000 シリーズ インターネット ルータで 8 ポートの OC-3 STM-1 ATM ライン カードの VC-class および bundle-vc コンフィギュレーション モードで使用できるようになりました。
12.0(26)S	このコマンドが Cisco IOS Release 12.0(26)S に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB 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

個々の VC または PVC バンドル メンバーに対してバンピング ルールを設定するには、bundle-vc コンフィギュレーション モード（ATM VC バンドル メンバーの場合）または SVC-bundle-member コンフィギュレーション モード（SVC バンドル メンバーの場合）で **bump** コマンドを使用します。バンドル メンバーに割り当てることができる VC クラスを設定するには、VC-class コンフィギュレーション モードで **bump** コマンドを使用します。

異なるバンピング設定のアプローチの効果は、次のようになります。

- 暗黙的なバンピング：暗黙的なバンピングを設定すると、バンピングされたトラフィックは、次に低い優先レベルを処理するように設定された VC または PVC に送信されます。トラフィックをバンピングした元の VC または PVC が復帰した場合は、その VC または PVC によって送信するように設定されていたトラフィックが復元されます。他のポジティブな形式の **bump** コマンドが設定されていない場合は、**bumpimplicit** コマンドが有効になります。
- 明示的なバンピング：**bumpexplicit** コマンドを使用して VC または PVC を設定する場合は、VC または PVC が停止したときにトラフィックがバンピングされる優先レベルを指定できます。これにより、トラフィックはその優先レベルでマッピングされた VC または PVC に送信されます。そのトラフィックを引き受け、伝送する VC または PVC が停止した場合、トラフィックはその VC または PVC のバンピング ルールに従います。バンピングで指定できる優先レベルは 1 つのみです。
- バンピングを許可：VC または PVC は、デフォルトでバンピングされたトラフィックを受け入れます。VC または PVC がバンピングされたトラフィックを拒否するように以前に設定されていた場合は、**bumptraffic** コマンドを使用して VC または PVC をデフォルトの状態に戻す必要があります。

- バンピングを拒否：個々の VC または PVC に対してバンピングされたトラフィックが送信された場合に拒否するように設定するには、**nobumptraffic** コマンドを使用します。

（注） バンピングされたトラフィックを処理する代替の VC または PVC が見つからない場合は、バンドルは停止したものとして宣言されます。これが発生するのを回避するには、最低の優先レベルを持つバンドル メンバーの VC または PVC を明示的に設定します。

このコマンドを VC-class コンフィギュレーション モードで使用するには、このコマンドを入力する前に **vc-classatm** 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必要があります。

このコマンドを使用して bundle-VC コンフィギュレーション モードで個々のバンドル メンバーを設定するには、まず **bundle** コマンドを発行し、設定する VC メンバーを追加または変更するバンドルのバンドル コンフィギュレーション モードに入ります。その後、**pvc-bundle** コマンドを使用して、作成または変更する VC を指定し、バンドル VC コンフィギュレーション モードにします。

コマンドを含む VC クラスがスタンドアロン VC（バンドル メンバーではない VC）に付加されている場合、このコマンドは効果がありません。この場合、属性は VC によって無視されます。

VC バンドルの VC は、次の設定継承ガイドラインに従います（2 番目に高い優先順位の順にリストされています）。

- bundle-VC モードの VC 設定
- バンドル モードのバンドル設定（および、割り当てられた VC-class コンフィギュレーションの影響）
- サブインターフェイス モードのサブインターフェイス設定

例

次の例では、「five」というクラスを設定し、バンドル内の VC に適用可能なパラメータを定義しています。VC が停止した場合、トラフィックは優先レベル 7 にマッピングされた VC に送信（明示的にバンピング）されます。

```
vc-class atm five
 ubr 5000
 precedence 5
 bump explicit 7
```

次の例では、「premium-class」というクラスを設定し、バンドル内の VC に適用可能なパラメータを定義しています。bundle-vc **bump** 設定で上書きされない限り、このクラスを使用する VC は他のトラフィックがこの VC にバンピングされることを許可しません。

```
vc-class atm premium-class
 no bump traffic
 bump explicit 7
```

関連コマンド

Command	Description
bundle	バンドル コンフィギュレーション モードに入って、バンドルを作成するか、または既存のバンドルを変更します。
class	PVC または PVC バンドル メンバーにマップ クラスまたは VC クラスを割り当てます。
class-vc	VC クラスを ATM PVC、SVC、または VC バンドル メンバーに割り当てます。
dscp(frame-relayvc-bundle-member)	特定のフレーム リレー PVC バンドル メンバーに対して DSCP 値を指定します。
precedence	VC バンドルまたは PVC バンドルに割り当てることができ、したがって、そのバンドルのすべてのメンバーに適用される、VC クラスまたは PVC クラスの優先レベルを設定します。
protect	VC または PVC バンドル メンバーに適用するための保護されたグループあるいは保護された VC または PVC ステータスを使用して、VC または PVC クラスを設定します。
pvc-bundle	バンドルに対してバンドルのメンバーとして PVC を追加し、PVC バンドル メンバーを設定するために bundle-vc コンフィギュレーション モードに入ります。
pvc(frame-relayvc-bundle)	PVC および PVC バンドル メンバーを作成し、frame-relay vc-bundle-member コンフィギュレーション モードに入ります。
svc-bundle	SVC バンドルのメンバーを作成または変更します。
ubr	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レートを指定します。
ubr+	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レートと出力最小保証セル レートを指定します。
vbr-nrt	可変ビット レート非リアルタイム（VBR-NRT）QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レート、出力平均セル レート、および、出力最大バースト セル サイズを指定します。
vc-classatm	VC クラス、ATM VC、またはインターフェイスを設定します。

bundle

バンドルを作成するか、既存のバンドルを変更してバンドル コンフィギュレーション モードに入るには、サブインターフェイス コンフィギュレーション モードで **bundle** コマンドを使用します。指定したバンドルを削除するには、このコマンドの **no** 形式を使用します。

bundle *bundle-name*
no bundle *bundle-name*

構文の説明

bundle-name	作成するバンドルの名前。長さの制限は16文字までです。

コマンド デフォルト

バンドルは指定されていません。

コマンド モード

サブインターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
12.0(26)S	このコマンドが Cisco IOS Release 12.0(26)S に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB 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

バンドル コンフィギュレーション モード内から、バンドルとそのメンバーの特性および属性を設定できます。これには、バンドル内のすべての仮想回線（VC）のカプセル化タイプ、バンドル管理パラメータ、サービス タイプなどがあります。バンドル コンフィギュレーション モードで設定する属性およびパラメータは、バンドルのすべての VC メンバーに適用されます。

VC バンドルの VC は、次の設定継承ガイドラインに従います（2 番目に高い優先順位の順にリストされています）。

- bundle-VC モードの VC 設定
- バンドル モードでのバンドル コンフィギュレーション
- サブインターフェイス モードのサブインターフェイス設定

バンドルのステータスを表示するには、**showatmbundle** コマンドと **showatmbundlestatistics** コマンドを使用します。

例

次に、「bundle1」というバンドルを設定する方法の例を示します。この例では、サブインターフェイスの IP アドレスとルータのプロトコル（ルータは IP ルーティング プロトコルとして Intermediate System-to-Intermediate System（IS-IS）を使用）を指定してからバンドルを設定しています。

```
interface atm1/0.1 multipoint
 ip address 10.0.0.1 255.255.255.0
 ip router isis
 bundle bundle1
```

関連コマンド

コマンド	説明
class-bundle	指定された VC クラスに含まれるバンドル レベルのコマンドで VC バンドルを設定します。
oam-bundle	バンドルのすべての VC メンバー、または VC バンドルに適用できる VC クラスに対して、エンドツーエンドの F5 OAM ループバック セル生成と OAM 管理を有効にします。
pvc-bundle	バンドルに対してバンドルのメンバーとして PVC を追加し、PVC バンドル メンバーを設定するために bundle-vc コンフィギュレーション モードに入ります。
showatmbundle	各バンドルの VC メンバに割り当てられたバンドルの属性と、VC メンバの現在の稼働ステータスを表示します。
showatmbundlestatistics	指定されたバンドルの統計を表示します。

bundle svc

相手先選択接続（SVC）バンドルを作成または変更するには、インターフェイス コンフィギュレーション モードで **bundlesvc** コマンドを使用します。指定したバンドルを削除するには、このコマンドの **no** 形式を使用します。

bundle svc *bundle-name* **nsap** *nsap-address*
no bundle svc *bundle-name* **nsap** *nsap-address*

構文の説明

bundle-name	ルータの SVC バンドルを識別する一意のバンドル名。仮想回線（VC）の各終端のバンドル名は同一である必要があります。長さの制限は 16 文字までです。
nsap *nsap-address*	SVC バンドルの宛先ネットワーク サービス アクセス ポイント（NSAP）アドレス。

コマンド デフォルト

SVC バンドルは作成または変更されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(4)T	このコマンドが導入されました。
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。

使用上のガイドライン

このコマンドにより、システムは SVC バンドル コンフィギュレーション モードを開始します。バンドル名は、VC の両端で同一になっている必要があります。

SVC バンドル コンフィギュレーション モードから、バンドルとそのメンバーの特性および属性を設定できます。これには、バンドル内のすべての仮想回線（VC）のカプセル化タイプ、バンドル管理パラメータ、サービス タイプなどがあります。SVC バンドル コンフィギュレーション モードで設定する属性およびパラメータは、バンドルのすべての VC メンバーに適用されます。

VC バンドルの VC は、次の設定継承ガイドラインに従います（2 番目に高い優先順位の順にリストされています）。

- bundle-VC モードの VC 設定
- バンドル モードでのバンドル コンフィギュレーション

- サブインターフェイス モードのサブインターフェイス設定

バンドルのステータスを表示するには、**showatmbundlesvc** コマンドと **showatmbundlesvcstatistics** コマンドを使用します。

例

次に、「sanfrancisco」という SVC バンドルを設定する方法の例を示します。

```
interface ATM1/0.1 multipoint
 ip address 10.0.0.1 255.255.255.0
 atm esi-address 111111111111.11
 bundle svc sanfrancisco nsap 47.0091810000000003E3924F01.999999999999.99
  protocol ip 10.0.0.2
broadcast
 oam retry 4 3 10
 encapsulation aal5snap
 oam-bundle manage
 svc-bundle seven
  class-vc seven
 svc-bundle six
  class-vc six
 svc-bundle five
  class-vc five
 svc-bundle four
  class-vc four
 svc-bundle three
  class-vc three
 svc-bundle two
  class-vc two
 svc-bundle one
  class-vc one
 svc-bundle zero
  class-vc zero
```

関連コマンド

コマンド	説明
class-bundle	指定された VC クラスに含まれるバンドル レベルのコマンドで VC バンドルを設定します。
oam-bundle	バンドルのすべての VC メンバー、または VC バンドルに適用できる VC クラスに対して、エンドツーエンドの F5 OAM ループバック セル生成と OAM 管理を有効にします。
pvc-bundle	バンドルに対してバンドルのメンバーとして PVC を追加し、PVC バンドル メンバーを設定するために bundle-vc コンフィギュレーション モードに入ります。
showatmbundlesvc	各バンドルの VC メンバに割り当てられたバンドルの属性と、VC メンバの現在の稼働ステータスを表示します。
showatmbundlesvcstatistics	指定されたバンドルの統計を表示します。

class（EtherSwitch）

クラスマップ名またはアクセス グループを使用してポリシーの適用対象となるトラフィック分類を定義するには、ポリシーマップ コンフィギュレーション モードでこの class コマンドを使用します。既存のクラス マップを削除するには、このコマンドの **no** 形式を使用します。

class *class-map-name* [**access-group** *acl-index-or-name*]
no class *class-map-name*

構文の説明

class-map-name	クラス マップの名前。
access-group *acl-index-or-name*	（任意）IP 標準または拡張アクセス コントロール リスト（ACL）の番号または名前。IP 標準 ACL の場合、インデックス範囲は 1 ～ 99 および 1300 ～ 1999 です。また、IP 拡張 ACL の場合、インデックス範囲は 100 ～ 199 および 2000 ～ 2699 です。

コマンド デフォルト

ポリシーマップ クラス マップは定義されません。

コマンド モード

ポリシー マップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに実装されました。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。

使用上のガイドライン

class (EtherSwitch) 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 モードを開始します。ポリシー マップを指定すると、ポリシー マップ内で新規クラスのポリシーを設定したり、既存クラスのポリシーを変更したりすることができます。インターフェイスにポリシー マップを適用するには、**service-policy** インターフェイス コンフィギュレーション コマンドを使用します。ただし、ACL 分類を使用しているポリシー マップを出力方向に適用することはできません。

ポリシーマップで指定したクラス名は、**class-map** グローバル コンフィギュレーション コマンドによる設定に従い、そのクラスの特性をクラス マップおよびその一致基準に連結します。

class (EtherSwitch) コマンドは、**class-map** グローバル コンフィギュレーション コマンドと同一の機能を実行します。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** (EtherSwitch) 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。

（注） ポリシー マップでは、「class-default」という名前のクラスがサポートされていません。イーサネット スイッチ ネットワーク モジュールは、**classclass-default** ポリシーマップ コンフィギュレーション コマンドで定義されるポリシー マップに基づいて、トラフィックをフィルタするわけではありません。

class (EtherSwitch) 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。このモードでは、次のコンフィギュレーション コマンドを使用できます。

- **default**：コマンドをデフォルトに設定します。
- **exit**：ポリシーマップ クラス コンフィギュレーション モードを終了して、ポリシーマップ コンフィギュレーション モードに戻ります。
- **no**：コマンドをデフォルト設定に戻します。
- **police**：分類したトラフィックにポリサーを定義します。ポリサーは、帯域幅の限度およびその限度を超過した場合に実行するアクションを指定します。詳細については、**police** コマンドを参照してください。

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

（注） IP ACL の設定の詳細については、『Cisco IOS IP Application Services Configuration Guide』の「Configuring IP Services」の章を参照してください。

例

次の例では、「policy1」という名前のポリシー マップを作成する方法を示します。このコマンドが入力ポートに適用された場合、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、平均レート 1 Mbps、バースト 131072 バイトでトラフィックをポリシングします。このプロファイルを超えたトラフィックはドロップされます。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police 1000000 131072 exceed-action drop
Router(config-pmap-c)# exit
```

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

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
match(class-mapconfiguration)	トラフィックを分類するための一致条件を定義します。

コマンド	説明
police	トラフィック ポリシングを設定します。
policy-map	サービス ポリシーを指定するための、複数のインターフェイスに適用できるポリシー マップを作成または変更します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showpolicy-map	QoS ポリシー マップを表示します。

class（ポリシー マップ）

ポリシーを作成または変更するクラスの名前を指定するには、またはクラスのポリシーを設定する前にデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定するには、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。クラスをポリシー マップから削除するには、このコマンドの **no** 形式を使用します。

class {*class-name*|**class-default** [**fragment** *fragment-class-name*]} [**insert-before** *class-name*] [**service-fragment** *fragment-class-name*]
no class {*class-name*|**class-default**}

構文の説明

class-name	設定するクラス、またはポリシーを編集するクラスの名前を指定します。クラス名は、クラス マップに使用するとともに、ポリシー マップのクラスにポリシーを設定する場合にも使用します。
class-default	ポリシーを設定または変更できるようデフォルト クラスを指定します。
fragment *fragment-class-name*	（任意）デフォルト トラフィック クラスをフラグメントに指定し、フラグメント トラフィック クラスに名前を付けます。
insert-before *class-name*	（任意）既存の任意の 2 つのクラス マップ間にクラス マップを追加します。 既存の 2 つのクラス マップ間に新しいクラス マップを挿入すると、既存のポリシー マップ コンフィギュレーションの柔軟性が向上します。このオプションを指定しないと、クラス マップはポリシー マップの末尾に追加されます。 このキーワードは、Flexible Packet Matching（FPM）ポリシーでだけサポートされています。
service-fragment *fragment-class-name*	（任意）クラスがフラグメントのコレクションを分類するように指定します。このクラスにより分類されるフラグメントは、すべて同じ *fragment-class-name* を共有している必要があります。

コマンド デフォルト

クラスの指定はありません。

コマンド モード

ポリシー マップ コンフィギュレーション（config-pmap）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。

リリース	変更箇所
12.0(7)S	このコマンドが、Cisco IOS Release 12.0(7)S に統合されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.2(14)SX	このコマンドのサポートが、Cisco 7600 ルータに追加されました。
12.2(17d)SXB	このコマンドが、Cisco 7600 ルータに実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
12.2(18)SXE	**class-default** キーワードが Cisco 7600 ルータに追加されました。
12.4(4)T	**insert-before***class-name* オプションが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(31)SB2	このコマンドが、Cisco 10000 シリーズ ルータの PRE3 に追加されました。
12.2(18)ZY	**insert-before***class-name* オプションが、Catalyst 6500 シリーズの Programmable Intelligent Services Accelerator（PISA）が搭載されているスイッチの Cisco IOS Release 12.2(18)ZY に統合されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。**fragment***fragment-class-name* オプションと *service-fragmentfragment-class-name* オプションが導入されました。

使用上のガイドライン

ポリシー マップ コンフィギュレーション モード

ポリシー マップ内で、**class**(policy-map) コマンドを使用すれば、ポリシーを作成または変更するクラスの名前を指定できます。まず、ポリシー マップを指定する必要があります。

ポリシー マップを指定して必要なポリシーマップ コンフィギュレーション モードを開始するには、**class**(policy-map) コマンドを使用する前に **policy-map** コマンドを使用します。ポリシーマップを指定した後は、新しいクラスのポリシーを設定したり、そのポリシーマップ内の任意の既存クラスのポリシーを変更したりできます。

クラス特性

ポリシーマップで指定するクラス名により、そのクラスの特性（つまりポリシー）が、**class-map** コマンドを使用して設定したとおりに、クラス マップおよびその一致基準に関連付けられます。

クラスのポリシーを設定し、その帯域幅を指定し、ポリシーマップをインターフェイスに割り当てると、クラス ベース Weighted Fair Queueing（CBWFQ）によって、そのクラスの帯域幅要件が満たされているかどうかが判断されます。満たされていれば、CBWFQ がその帯域幅要件のキューを割り当てます。

クラスが削除されると、インターフェイスに使用できる帯域幅が、そのクラスにそれまで割り当てられていた量だけ増加します。

ルータに（つまり 1 つのポリシー マップ内で）設定できるクラスの最大数は、64 個です。

定義済みのデフォルト クラス

class-default と呼ばれる定義済みのデフォルト クラスを指定するには、**class-default** キーワードを使用します。class-default クラスは、トラフィックがクラス マップ内で設定されているどの一致基準とも一致しない場合に、そのトラフィックが送られるクラスです。

テール ドロップまたは WRED

クラス ポリシーを定義するには、テール ドロップを使用（**queue-limit** コマンドを実行）するか、または重み付けランダム早期検出（WRED）を使用（**random-detect** コマンドを実行）することができます。テール ドロップまたは WRED を使用する場合は、次の点に注意してください。

- **queue-limit** コマンドと **random-detect** コマンドの両方を同じクラス ポリシー内で使用することはできませんが、同じポリシー マップ内の 2 つのクラス ポリシー内で使用することは可能です。
- クラス ポリシーで **queue-limit** コマンドまたは **random-detect** コマンドのいずれかを設定すると、**bandwidth** コマンドを設定できます。**bandwidth** コマンドは、クラスに割り当てられる帯域幅の量を指定します。
- 定義済みのデフォルト クラスでは、**fair-queue** (class-default) コマンドを設定できます。**fair-queue** コマンドは、デフォルト クラスのダイナミック キューの数を指定します。**fair-queue** コマンドは、**queue-limit** コマンドまたは **random-detect** コマンドのいずれかと同じクラス ポリシーで使用できます。**bandwidth** コマンドと一緒に使用することはできません。

Fragments

デフォルト トラフィック クラスは、ポリシー マップ クラス ステートメントで **fragment** キーワードを使用して、フラグメントとしてマークされます。これにより、フラグメントを分類して、複数のフラグメントをまとめて **service-fragment** キーワードを使用して作成した別のポリシーマップに入れることができます。フラグメントが使用されると、フラグメントとしてマークされているデフォルト トラフィック クラスに、デフォルト以外のトラフィック クラスとは別に、QoS が適用されます。

フラグメントを使用する場合は、次のガイドラインに従ってください。

- フラグメントとしてマークできるのは、デフォルト トラフィック クラスだけです。
- デフォルト クラス ステートメントでの **fragment***fragment-class-name* オプションが、デフォルト クラスをフラグメントとしてマークします。
- ポリシー マップのクラス定義時には **service-fragment***fragment-class-name* オプションを使用し、同じ *fragment-class-name* を共有するすべてのフラグメントを含む Modular QoS CLI 内のトラフィックのクラスを指定します。
- フラグメントは、同一物理インターフェイス内でしか使用できません。同じ *fragment-class-name* を共有し、異なるインターフェイス上にあるフラグメントを持つポリ

シー マップを、**service-fragment***fragment-class-name* オプションを持つクラスを使用してひとまとめに分類することはできません。

Cisco 10000 シリーズ ルータ

PRE2 では、ポリシー マップで 31 個のクラス キューを設定できます。

PRE3 では、ポリシー マップで優先度レベル 1 のキューを 1 個、優先度レベル 2 のキューを 1 個、クラス キューを 12 個、デフォルト キューを 1 個設定できます。

Cisco ASR 1000 シリーズ ルータ

Cisco ASR 1000 シリーズ ルータに（つまり 1 つのポリシー マップ内で）設定できるクラスの最大数は、8 個です。

例

次に、policy1 というポリシー マップに含まれる 3 つのクラス ポリシーを設定する例を示します。Class1 は、アクセス コントロール リスト 136 に一致するトラフィックのポリシーを指定します。class2 は、インターフェイス ethernet101 のトラフィックのポリシーを指定します。3 つ目のクラスは、設定済みの一致基準を満たさないパケットが送られるデフォルト クラスです。

```
! The following commands create class-maps class1 and class2
! and define their match criteria:
class-map class1
 match access-group 136
class-map class2
 match input-interface ethernet101
! The following commands create the policy map, which is defined to contain policy
! specification for class1, class2, and the default class:
policy-map policy1
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect exponential-weighting-constant 10
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 16
Router(config-pmap-c)# queue-limit 20
```

- class1：輻輳の発生時に、このクラスに最低 2000 kbps の帯域幅が提供されることを予期しています。また、このクラスのために予約されるキューでは、テール ドロップを実行して追加のパケットを処理する前に 40 個のパケットまでキューに登録できます。
- class2：輻輳の発生時に、このクラスに最低 3000 Kbps の帯域幅が提供されることを予期しています。また、平均キュー サイズの計算に重み係数 10 が使用されます。輻輳回避のために、テール ドロップではなく WRED パケットのドロップが使用されます。
- デフォルト クラス：ポリシーがポリシー マップ policy1 で定義されている他のクラスの一致条件を満たさないトラフィック用に、16 個のダイナミック キューが予

約されています。また、キューあたり20個のパケットを超えると、追加でキューに格納されるパケットを処理するためにテール ドロップが実施されます。

（注） このクラスを含むポリシー マップをインターフェイスに付加して、そのインターフェイスのサービス ポリシーを規定するとき、設定されるすべてのクラス ポリシーおよびリソース予約プロトコル（RSVP）を考慮し、使用可能な帯域幅が評価されます。

次に、policy8 というポリシー マップに組み込まれるデフォルト クラスのポリシーを設定する例を示します。デフォルトのクラスには、次の特性があります。他のクラスの一致基準を満たさないトラフィックのために 20 個のダイナミック キューが利用でき、また、そのクラスのポリシーはpolicy8というポリシーマップによって定義され、重み係数 14 を使用して平均キュー サイズを計算します。輻輳回避のために、テール ドロップではなく WRED パケット ドロップが使用されます。

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

次の例では、policy1 というポリシー マップに含まれる acl136 というクラスのためのポリシーを設定する方法を示します。クラス acl136 には、次の特性があります。輻輳の発生時に、このクラスに最低 2000 kbps の帯域幅が提供されることを予期しています。また、このクラスのために予約されるキューでは、テール ドロップを実行して追加のパケットを処理する前に40個のパケットまでキューに登録できます。このクラスを含むポリシー マップをインターフェイスに付加して、そのインターフェイスのサービス ポリシーを規定するとき、設定されるすべてのクラス ポリシーおよびRSVPを考慮し、使用可能な帯域幅が評価されるため、注意してください。

```
Router(config)# policy-map policy1
Router(config-pmap)# class acl136
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40
```

次の例では、policy8 というポリシー マップに含まれる int101 というクラスのためのポリシーを設定する方法を示します。クラス int101 には、次のような特性があります。輻輳の発生時に、このクラスに最低 3000 Kbps の帯域幅が提供されることを予期しています。また、平均キュー サイズの計算に重み係数 10 が使用されます。輻輳回避のために、テール ドロップではなく WRED パケットのドロップが使用されます。このクラス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 ポリシーが規定される場合、使用可能な帯域幅が評価されることに注意してください。

```
Router(config)# policy-map policy8
Router(config-pmap)# class int101
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect exponential-weighting-constant 10
```

次に、policy1 というポリシー マップに組み込まれる **class-default** デフォルト クラスのポリシーを設定する例を示します。**class-default** デフォルト クラスには、次の特性があります。ポリシーがポリシー マップ policy1 で定義されている他のクラスの一致条件を満たさないトラフィック用に、10 個のハッシュ キューが予約されています。また、キューあたり 20 個のパケットを超えると、追加でキューに格納されるパケットを処理するためにテール ドロップが実施されます。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue
Router(config-pmap-c)# queue-limit 20
```

次に、policy8 というポリシー マップに組み込まれる **class-default** デフォルト クラスのポリシーを設定する例を示します。**class-default** デフォルトのクラスには、次の特性があります。他のクラスの一致基準を満たさないトラフィックのために 20 個のハッシュ キューが利用でき、また、そのクラスのポリシーは policy8 というポリシー マップによって定義され、重み係数 14 を使用して平均キュー サイズを計算します。輻輳回避のために、テール ドロップではなく WRED パケット ドロップが使用されます。

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

次に、ブラスタ パケット用に FPM を設定する方法の例を示します。クラス マップには、TCP ポート 135、4444 または UDP ポート 69、および IP ヘッダーの先頭から 3 バイトに 0x0030 のパターンが存在するという一致条件が含まれます。

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
Router(config-cmap)# match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
```

```
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

次の例は、BestEffort というデフォルトのトラフィック クラスを分類するトラフィックのフラグメント クラスを作成する方法を示しています。subscriber1 と subscriber2 というポリシー マップからのすべてのデフォルトのトラフィックは、BestEffort というフラグメント デフォルトのトラフィック クラスの一部です。このデフォルトのトラフィックが、**service-fragment** キーワードと **shape** コマンドを使用する、data というクラスを作成することによってまとめてシェーピングされます。

この例では、次の点に注意してください。

- 各フラグメントデフォルトのトラフィック クラスの *class-name* は「BestEffort」です。
- *class-name* の「BestEffort」は、**service-fragment** キーワードが入力されるクラスの定義にも使用します。このクラスは、「BestEffort」というフラグメントデフォルトのトラフィック クラスを使用して転送されるすべてのトラフィックにシェーピング ポリシーを適用します。

```
policy-map subscriber1
class voice
set cos 5
priority level 1
class video
set cos 4
priority level 2
class class-default fragment BestEffort
shape average 200
bandwidth remaining ratio 10
policy-map subscriber 2
class voice
set cos 5
priority level 1
class video
set cos 4
priority level 2
class class-default fragment BestEffort
shape average 200
bandwidth remaining ratio 10
policy-map input_policy
class class-default
set dscp default
policy-map main-interface
class data service-fragment BestEffort
shape average 400
interface portchannel1.1001
encapsulation dot1q 1001service-policy output subscriber1
service-policy input input_policy
interface portchannel1.1002
encapsulation dot1q 1002
service-policy output subscriber2
service-policy input input_policy
interface gigabitethernet 0/1
description member-link1
port channel 1
service-policy output main-interface
interface gigabitethernet 0/2
```

```
description member-link2
port channel 1
```

service-policy output main-interface

関連コマンド

Command	Description
bandwidth(policy-mapclass)	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
fair-queue(class-default)	デフォルト クラス ポリシーの一部として class-default クラスで使用するために予約するダイナミック キューの数を指定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
queue-limit	キューが保持できる、ポリシー マップ内に設定されるクラス ポリシーのパケットの最大数を指定または変更します。
random-detect(interface)	WRED または DWRED をイネーブルにします。
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detectprecedence	特定の IP Precedence の WRED パラメータと DWRED パラメータを設定します。

class-map arp-peruser

ユーザごとのパケットの Address Resolution Protocol（ARP）に一致するクラス マップを作成するには、グローバル コンフィギュレーション モードで **class-maparp-peruser** 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。

class-map arp-peruser
no class map arp-peruser

構文の説明

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

クラス マップは設定されません。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。

使用上のガイドライン

CoPP の設定時に ARP クラス マップを作成するには、このコマンドを使用します。

例

ARP クラスマップの作成方法を、次の例に示します。

```
Router(config)# class-map arp-peruser
Router(config-cmap)# match protocol arp
Router(config-cmap)# match subscriber access
```

関連コマンド

コマンド	説明
matchprotocolarp	ポリシー マップに対する ARP トラフィックに一致します。
matchsubscriberaccess	ポリシーマップに対する加入者アクセス トラフィックに一致します。

class-bundle

指定した VC クラスに含まれるバンドルレベル コマンドを使用して仮想回線（VC）を設定するには、バンドル コンフィギュレーション モードまたは SVC バンドル コンフィギュレーション モードで **class-bundle** コマンドを使用します。VC バンドルから VC クラス 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。

class-bundle *vc-class-name*
no class-bundle *vc-class-name*

構文の説明

vc-class-name	VC バンドルに割り当てる VC クラスの名前です。

コマンド デフォルト

VC バンドルに割り当てられている VC クラスはありません。

コマンド モード

バンドル コンフィギュレーション
SVC バンドル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0T	このコマンドが導入され、ATM VC バンドルを設定するための **class** コマンドが置き換えられました。
12.0(26)S	このコマンドが Cisco IOS Release 12.0(26)S に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。
12.2(4)T	このコマンドが、SVC バンドル コンフィギュレーション モードで使用できるようになりました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB 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

このコマンドを使用するには、まず **bundle** または **bundlesvc** コマンドを入力してバンドルを作成し、バンドル コンフィギュレーション モードまたは SVC バンドル 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。

このコマンドを使用して、以前に定義した一連のパラメータ（VC クラスで定義）を ATM VC バンドルに割り当てます。VC クラスに含まれるバンドルレベル コマンドを使用して設定されたパラメータは、バンドルとその VC メンバーに適用されます。

VCバンドルを設定するために使用するVCクラスに、次のコマンドを追加できます。**broadcast**、**encapsulation**、**inarp,oam-bundle**、**oamretry,**、**protocol**

バンドルで直接設定されたコマンドを使用して適用されるバンドルレベル パラメータは、**class-bundle** コマンドによって VC クラスを使用して適用されるバンドルレベル パラメータよりも優先されます。VC クラスを通じて適用されたバンドルレベル パラメータやバンドルに直接適用されたバンドルレベルパラメータの一部は、バンドルVCコンフィギュレーションモードで個々の VC に直接適用されたコマンドによって置き換えることができます。

例

次の例では、「class1」という名前のクラスを作成し、「bundle1」という名前のバンドルに適用しています。

```
! The following commands create the class class1:
vc-class atm class1
 encapsulation aal5snap
 broadcast
 protocol ip inarp
 oam-bundle manage 3
 oam 4 3 10
! The following commands apply class1 to the bundle called bundle1:
bundle bundle1
 class-bundle class1
```

階層化された優先ルールを考慮し、「bundle1」という名前のバンドルに属するVCは、aal5snap、カプセル化、ブロードキャスト対象、IP アドレスを解決するための Inverse Address Resolution Protocol（Inverse ARP）の使用、および有効になった運用管理および保守（OAM）といったパラメータによって特徴付けられます。

関連コマンド

Command	Description
broadcast	ブロードキャスト パケットの複製と、ATM VC クラス、PVC、SVC、または VC バンドルへの送信を設定します。
bundle	バンドルを作成するか、または既存のバンドルを修正してバンドル コンフィギュレーション モードを開始します。
bundlesvc	SVC バンドルを作成するか、または既存の SVC バンドルを変更します。
class-int	VC クラスを ATM メイン インターフェイスまたはサブインターフェイスに割り当てます。
class-vc	VCクラスをATM PVC、SVC、またはVCバンドル メンバーに割り当てます。
encapsulation	インターフェイスで使用するカプセル化方式を設定します。
inarp	ATM PVC、VC クラス、または VC バンドルの Inverse ARP の時間を設定します。
oam-bundle	バンドルのすべての VC メンバー、または VC バンドルに適用できる VC クラスに対して、エンドツーエンドの F5 OAM ループバック セル生成と OAM 管理を有効にします。

Command	Description
oamretry	ATM PVC、SVC、VC クラス、または、VC バンドルの OAM 管理に関連するパラメータを設定します。
protocol(ATM)	ATM PVC、SVC、VC クラス、または、VC バンドルのスタティック マップを設定します。PVC、VC バンドルで直接、または VC クラス（IP および IPX プロトコルのみに適用）内で Inverse ARP を設定することで、ATM PVC で Inverse ARP または Inverse ARP ブロードキャストを有効にします。
pvc-bundle	バンドルに対してバンドルのメンバーとして PVC を追加し、PVC バンドル メンバーを設定するために bundle-vc コンフィギュレーション モードに入ります。

class-map

指定したクラスへのパケットの照合に使用するクラス マップを作成し、QoS 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 マップをデバイスから削除するには、このコマンドの **no** 形式を使用します。

Cisco 2600、3660、3845、6500、7200、7401、および 7500 シリーズ ルータ
class-map [**type** {**stack**|**access-control**|**port-filter**|**queue-threshold**|**logging** *log-class*}] [{**match-all**|**match-any**}] *class-map-name*
no class-map [**type** {**stack**|**access-control**|**port-filter**|**queue-threshold**|**logging** *log-class*}] [{**match-all**|**match-any**}] *class-map-name*

Cisco 7600 シリーズ ルータ
class-map *class-map-name* [{**match-all**|**match-any**}]
no class-map *class-map-name* [{**match-all**|**match-any**}]

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor
class-map *class-map-name*
no class-map *class-map-name*

構文の説明

type	（任意）クラスマップ タイプを指定します。
stack	（任意）Flexible Packet Matching（FPM）機能を有効にして、調査するプロトコル スタックを決定します。 **loadprotocol** コマンドを使用し、デバイスで Protocol Header Description File（PHDF）をロードする場合、存在するヘッダーとその順序をフィルタで判定できるように、プロトコル ヘッダーのスタックを定義できます。
access-control	（任意）設定されたプロトコル スタックで検索するパターンを決定します。 （注） スタック クラス マップを指定（**typestack** キーワードを使用）してから、アクセス制御クラス マップを指定（**typeaccess-control** キーワードを使用）する必要があります。
port-filter	（任意）コントロール プレーン パケットの TCP または UDP ポート ポリシングを有効にするポートフィルタ クラスマップを作成します。このキーワードが有効になっている場合、コマンドは、コントロール プレーン ホスト サブインターフェイスの特定のポートが宛先になっているトラフィックをフィルタします。
queue-threshold	（任意）指定されたプロトコルでコントロールプレーン IP 入力キューに入ることができるパケットの総数を制限するキューしきい値を有効にします。このキューしきい値は、コントロール プレーン ホスト サブインターフェイスにしか適用されません。

logging *log-class*	（任意）コントロールプレーン上のパケットトラフィックのロギングを有効にします。*log-class* 引数の値は、ログ クラスの名前です。
match-all	（任意）複数の一致基準が存在する場合に、どのようにしてパケットを評価するかを決定します。このクラスマップの下のステートメントが、論理AND関数に基づいて一致します。パケットが受け入れられるには、すべてのステートメントに一致している必要があります。**match-all** または **match-any** キーワードを指定しない場合に使用されるデフォルト キーワードは、**match-all** です。
match-any	（任意）複数の一致基準が存在する場合に、どのようにしてパケットを評価するかを決定します。このクラス マップの下のステートメントが、論理 OR 関数に基づいて一致します。パケットが受け入れられるには、マッチング ステートメントのいずれかに一致している必要があります。**match-any** または **match-all** キーワードを指定しない場合に使用されるデフォルトのキーワードは、**match-all** です。
class-map-name	クラスマップのクラスの名前です。クラス名は、クラスマップに使用するとともに、ポリシー マップのクラスにポリシーを設定する場合にも使用します。 （注） 引用符で囲んだ *class-map-name* 引数の値を入力できます。引用符なしで入力されたクラスマップ名では、スペースが受け入れられません。

コマンド デフォルト

クラス マップは設定されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。
12.0(7)S	このコマンドが、Cisco IOS Release 12.0(7)S に統合されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.2(14)SX	このコマンドは、Cisco IOS Release 12.2(14)SX に統合され、Cisco 7600 シリーズ ルータに実装されました。
12.2(17d)SXB	このコマンドが、Cisco IOS Release 12.2(17d)SXB に統合され、Cisco 7600 シリーズ ルータに実装されました。
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。

リリース	変更箇所
12.4(4)T	このコマンドが変更されました。FPM をサポートするために **stack** キーワードと **access-control** キーワードが追加されました。コントロール プレーン保護機能をサポートするために **port-filter** キーワードと **queue-threshold** キーワードが追加されました。
12.4(6)T	このコマンドが変更されました。コントロール プレーン パケット ロギングをサポートするために **logging** *log-class* キーワードと引数のペアが追加されました。
12.2(18)ZY	このコマンドが変更されました。**stack** キーワードと **access-control** キーワードが、Catalyst 6500 シリーズの Programmable Intelligent Services Accelerator（PISA）が搭載されているスイッチの Cisco IOS Release 12.2(18)ZY に統合されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。
15.1(3)T	このコマンドが、Cisco Performance Monitor 用の Cisco IOS Release 15.1(3)T に統合され、*class-map-name* 引数が使用可能な唯一の構文要素となりました。
12.2(58)SE	このコマンドが、*class-map-name* 引数とともに Cisco Performance Monitor 用の Cisco IOS Release 12.2(58)SE に統合されました。
12.2(33)SCF	このコマンドが、Cisco IOS リリース 12.2(33)SCF に統合されました。
15.2(3)T	このコマンドが変更されました。引用符なしで入力されたクラス マップ名では、スペースが受け入れられません。
15.1(2)SNG	このコマンドが、Cisco ASR 901 シリーズ アグリゲーション サービス ルータに統合されました。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

class-map-name 引数のみが利用可能です。

Cisco 2600、3660、3845、6500, 7200、7401、7500、および ASR 1000 シリーズ ルータ

class-map コマンドを使用して、クラスマップの一致基準に一致させるために作成または変更するクラスを指定します。このコマンドで QoS クラスマップ コンフィギュレーション モードに入ることができ、そこで 1 つまたは複数の **match** コマンドを入力して、このクラスの一致基準を設定します。入力インターフェイスまたは出力インターフェイスのいずれか（**service-policy** コマンドの設定により決まります）に到達したパケットが、クラスマップに設定されている一致基準に対して照合され、パケットがそのクラスに属するかどうかが判断されます。

クラス マップを設定する際には、1 つまたは複数の **match** コマンドを使用して一致基準を指定できます。たとえば、**matchaccess-group** コマンド、**matchprotocol** コマンド、または

matchinput-interface コマンドを使用できます。**match** コマンドは、Cisco のソフトウェア リリースごとに異なります。一致基準および **match** コマンドの詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Modular Quality of Service Command-Line Interface (CLI) (MQC)」の章を参照してください。

Cisco 7600 シリーズ ルータ

class-map コマンドと、QoS クラスマップ コンフィギュレーション モードで利用できるコマンドをインターフェイス単位ベースで適用し、グローバルに指定されたサービス ポリシーの一環として、パケット分類、マーキング、集約、およびフロー ポリシングを定義します。

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

デバイスが QoS クラスマップ コンフィギュレーション モードになっている場合、次のコンフィギュレーション コマンドが利用可能です。

- **description**：クラスマップ コンフィギュレーションの記述を指定します。
- **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 マップからマッチング ステートメントを削除します。

CLI ヘルプには次のコマンドが表示されますが、Optical Service Module（OSM）の LAN インターフェイスまたは WAN インターフェイスではサポートされません。

- **destination-address mac** *mac-address*
- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **source-address mac** *mac-address*

OSM は、Supervisor Engine 32 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

ポリシー フィーチャ カード（PFC）QoS は、次のコマンドをサポートしません。

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

これらのコマンドを入力した場合、インターフェイスにポリシー マップが付加されないと、PFC QoS はサポートされていないキーワードを検出しません。インターフェイスにポリシー マップを付加しようとすると、エラー メッセージが生成されます。詳細については、『*Cisco*

7600 Series Router Cisco IOS Software Configuration Guide』と Cisco IOS コマンド リファレンスを参照してください。

クラスマップ名およびデバイスの設定後、QoS クラスマップ コンフィギュレーション モードで **match access-group** コマンドと **matchipdscp** コマンドを入力できます。これらのコマンドの構文は次のとおりです。

match [**access-group** {*acl-index* | *acl-name*} | **ip dscp** | **precedence**} *value*]

match コマンド キーワードの説明については、次の表を参照してください。

表 *1 : match* コマンド構文の説明

オプションのコマンド	説明
access-group *acl-index* | *acl-name*	（任意）アクセス リスト インデックスまたはアクセス リスト名を指定します。有効なアクセス リストのインデックス値は、1 ～ 2699 です。
access-group *acl-name*	（任意）名前付きのアクセス リストを指定します。
ipdscp *value1 value2 ...value8*	（任意）照合する IP Diffserv コード ポイント（DSCP）値を指定します。有効な値は 0 ～ 63 です。最大 8 つの DSCP 値をスペースで区切って入力できます。
ipprecedence *value1 value2 ...value8*	（任意）照合する IP プレシデンス値を指定します。有効な値は 0 ～ 7 です。最大 8 つのプレシデンス値をスペースで区切って入力できます。

例

次に、クラスの名前として class101 を指定し、そのクラスに対してクラス マップを定義する方法の例を示します。class101 という名前のクラスは、ACL 101 に一致するトラフィックに対するポリシーを指定します。

```
Device(config)# class-map class101
Device(config-cmap)# match access-group 101
Device(config-cmap)# end
```

次の例は、スラマーおよび UDP パケットの FPM トラフィック クラスを定義する方法を示しています。クラス マップ内で定義されている一致基準は、IP の長さが 404（0x194）を超えず、UDP ポートが 1434（0x59A）であり、IP ヘッダーの先頭から 224 バイトでパターン 0x4011010 となるスラマーおよび UDP パケットを対象としています。

```
Device(config)# load protocol disk2:ip.phdf
Device(config)# load protocol disk2:udp.phdf
Device(config)# class-map type stack match-all ip-udp
Device(config-cmap)# description "match UDP over IP packets"
Device(config-cmap)# match field ip protocol eq 0x11 next udp
Device(config-cmap)#exit
Device(config)# class-map type access-control match-all slammer
Device(config-cmap)# description "match on slammer packets"
```

```
Device(config-cmap)# match field udp dest-port eq 0x59A
Device(config-cmap)# match field ip length eq 0x194
Device(config-cmap)# match start 13-start offset 224 size 4 eq 0x 4011010
Device(config-cmap)# end
```

次に、Simple Network Management Protocol（SNMP）以外の閉じているポート、つまり「リッスンされていない」ポートに宛てられたすべてのトラフィックをドロップするポートフィルタ ポリシーを設定する例を示します。

```
Device(config)# class-map type port-filter pf-class
Device(config-cmap)# match not port udp 123
Device(config-cmap)# match closed-ports
Device(config-cmap)# exit
Device(config)# policy-map type port-filter pf-policy
Device(config-pmap)# class pf-class
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

次の例は、ipp5 というクラス マップを設定して、IP プレシデンス 5 のマッチング ステートメントを入力する方法を示しています。

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

802.1p ドメイン内のクラス マップの設定

次の例は、クラスマップを設定し、802.1p ドメインに対してパケットのサービス クラス（CoS）値を使用してトラフィック クラスに照合する方法の例を示しています。

```
Device> enable
Device# configure terminal
Device(config)# class-map cos1
Device(config-cmap)# match cos 0
Device(config-pmap-c)# end
```

MPLS ドメイン内のクラス マップの設定

次の例は、クラス マップを設定し、マルチプロトコル ラベル スイッチング（MPLS）ドメインに対してパケットの Experimental（EXP）値を使用してトラフィック クラスに照合する方法の例を示しています。

```
Device> enable
Device# configure terminal
Device(config)# class-map exp7
Device(config-cmap)# match mpls experimental topmost 2
Device(config-pmap-c)# end
```

関連コマンド

コマンド	説明
description	クラス マップまたはポリシー マップのコンフィギュレーションの記述を指定します。

コマンド	説明
drop	特定のクラス マップに属するパケットを廃棄するトラフィック クラスを設定します。
class(policy-map)	ポリシーを作成または変更するクラスの名前を指定し、ポリシーを設定する前にデフォルト クラスを指定します。
load protocol	PHDF をルータにロードします。
match (class-map)	ポート フィルタやプロトコル キュー ポリシーに基づいて、クラス マップの一致基準を設定します。
matchaccess-group	指定した ACL をベースにクラス マップに対して一致基準を設定します。
matchinput-interface	指定された入力インターフェイスを一致基準として使用するクラス マップを設定します。
matchipdscp	1 つまたは複数の DSCP 値、AF 値、および CS 値を一致基準として指定します。
matchmplsexperimental	指定した EXP フィールド値を一致基準として使用するクラス マップを設定します。
matchprotocol	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
protocol	制御インターフェイスのタイマーと認証方法を設定します。
qos-group	クラス マップに対して QoS グループ値を関連付けます。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showclass-map	クラス マップ情報を表示します。
showpolicy-mapinterface	インターフェイスに適用された入力および出力ポリシーの統計情報および設定を表示します。
source-address	ポートで送信元アドレスの制御を設定します。

class-map arp-peruser

ユーザごとのパケットの Address Resolution Protocol（ARP）に一致するクラス マップを作成するには、グローバル コンフィギュレーション モードで **class-maparp-peruse**r 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。

class-map arp-peruser
no class map arp-peruser

構文の説明

arpper-user	ユーザごとの Address Resolution Protocol を指定します。

コマンド デフォルト

有効

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。

使用上のガイドライン

CoPP の設定時に ARP クラス マップを作成するには、このコマンドを使用します。

例

ARP クラスマップの作成例を、次に示します。

```
Router(config)#class-map arp-peruser
Router(config-cmap)#match protocol arp
Router(config-cmap)#match subscriber access
```

関連コマンド

コマンド	説明
matchprotocolarp	ポリシー マップに対する ARP トラフィックに一致します。
matchsubscriberaccess	ポリシーマップに対する加入者アクセス トラフィックに一致します。

class type tag

クラス マップをポリシー マップと関連付けるには、ポリシー マップ コンフィギュレーション モードで、**classtypetag** コマンドを使用します。コマンド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。

class type tag *class-name* [**insert-before** *class-name*]
no class type tag *class-name* [**insert-before** *class-name*]

構文の説明

class-name	クラス マップの名前。
insert-before *class-name*	（任意）既存の任意の 2 つのクラス マップ間にクラス マップを追加します。 （注） 既存の2つのクラスマップ間に新しいクラスマップを挿入すると、既存のポリシーマップ設定をより柔軟に変更できるようになります。このオプションを指定しないと、クラスマップはポリシー マップの末尾に追加されます。

コマンド デフォルト

クラス マップは、ポリシー マップに関連付けられていません。

コマンド モード

ポリシー マップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.4(6)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

このコマンドを使用していてもクラスが設定されていない場合は、エラーが発生します。エラーは、「% クラス マップ {名} は設定されていません。（% class map {*name*} not configured.）」のような内容です。特定のクラスマップの前にクラスを挿入する必要がある場合は、**insert-before** キーワードを使用できます。**insert-before** キーワードは通常、管理者がホストごとのクラス マップを設定し、それを特定のクラスマップの前に挿入する場合に必要となります。**classtypetag** コマンドは、ポリシーマップ クラス コンフィギュレーション モードを作成します。ポリシーマップの下に複数のクラスを配置できます。

例

クラスマップ「usergroup1_class」をポリシーマップと関連付ける方法を、次の例に示します。

```
class type tag usergroup1_class
```

関連コマンド

コマンド	説明
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

clear control-plane

コントロールプレーンのインターフェイスまたはサブインターフェイスのカウンタをクリアするには、特権 EXEC モードで **clearcontrol-plane** コマンドを使用します。

clear control-plane [{*****|**aggregate**|**host**|**transit**|**cef-exception**}]

構文の説明

*	（任意）すべてのコントロール プレーンの機能に対するカウンタをクリアします。
aggregate	（任意）コントロール プレーンの集約パスのすべての機能に対するカウンタをクリアします。
host	（任意）コントロール プレーン ホスト機能のパスのすべての機能に対するカウンタをクリアします。
transit	（任意）コントロール プレーンの中継機能パスのすべての機能に対するカウンタをクリアします。
cef-exception	（任意）コントロール プレーンの CEF 例外機能パスのすべての機能に対するカウンタをクリアします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)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

コントロールプレーンのインターフェイスまたはサブインターフェイスのすべての機能に対するカウンタをクリアするには、**clearcontrol-plane** コマンドを使用します。

例

次の例は、コントロールプレーン ホスト機能のパスのすべての機能に対するカウンタをクリアします。

```
Router# clear control-plane host
```

関連コマンド

コマンド	説明
control-plane	コントロール プレーン コンフィギュレーション モードを開始します。このモードでは、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更ができます。

コマンド	説明
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-planecef-exceptioncounters	コントロール プレーン CEF 例外のサブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planecef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-planecounters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planefeatures	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-planehostcounters	コントロール プレーン ホスト サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-planehostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planetransitfeatures	コントロールプレーン中継サブインターフェイスに対して設定された機能を表示します。

clear ip nbar

Network-Based Application Recognition（NBAR）によって収集されたバッファ、フィルタ、およびポートの統計情報をクリアするには、特権 EXEC モードで **clear ip nbar** コマンドを使用します。

clear ip nbar [{**capture**|**filter**|**trace**{**detail**|**summary**}|**statistics**|**unclassified-port-stats**}]

構文の説明

capture	（任意）パケット キャプチャ バッファを指定します。
filter	（任意）セッション選択フィルタを指定します。
trace	（任意）状態グラフ トレース バッファを指定します。
detail	（任意）NBAR の詳細な分類情報を指定します。
summary	（任意）NBAR の分類概要を指定します。
unclassified-port-stats	（任意）未分類パケットのポート統計情報を指定します。
statistics	（任意）パケットの NBAR 統計情報を指定します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRC	このコマンドは、Cisco IOS Release 12.2(33)SRC よりも前のリリースに統合されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI よりも前のリリースに統合されました。
15.0(1)M	このコマンドは、Cisco IOS Release 15.0(1)M よりも前のリリースに導入されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズの集約サービス ルータに実装されました。
15.2(4)M	このコマンドが変更されました。**statistics**、**trace**、および **detail** キーワードが追加されました。

例

次に、NBAR によって収集されたポートの統計情報をクリアする例を示します。

```
Device# clear ip nbar unclassified-port-stats
```

次に、NBAR によって収集された統計情報をクリアする例を示します。

```
Device# clear ip nbar statistics
```

関連コマンド

コマンド	説明
clearipnbarprotocol-discovery	NBAR Protocol Discovery によって収集された統計情報をクリアします。
show ip nbar statistics	NBAR によって収集された統計情報を表示します。

clear ip nbar classification auto-learn top-hosts

ジェネリックとして分類されたネットワーク トラフィックの上位ホストの統計およびデータベースをクリアするには、**clear ip nbar classification auto-learn top-hosts** コマンドを使用します。

clear ip nbar custom auto-learn top-hosts {**restart** | **statistics**}

構文の説明

restart	表示のクリア後に、ジェネリックとして分類されたトラフィックの上位ホストの統計およびデータベースの表示を再開します。
statistics	統計およびデータベースの表示をクリアします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
15.5(2)T	このコマンドが導入されました。

例

次の例に、ジェネリックとして分類されたネットワーク トラフィックの上位ホストの統計およびデータベースをクリアする方法を示します。

```
Device# clear ip nbar classification auto-learn statistics
```

関連コマンド

コマンド	説明
ipnbarclassificationauto-learntop-hosts	ジェネリックとして分類されたネットワーク トラフィックの上位ホストの統計およびデータベースを示す NBAR の機能を有効にします。
showipnbarclassificationauto-learntop-hosts	ジェネリックとして分類されたネットワーク トラフィックの上位ホストの統計およびデータベースを表示します。

clear ip nbar protocol-discovery

Network-Based Application Recognition（NBAR）Protocol Discovery 機能によって収集された統計情報をクリアするには、特権 EXEC モードで **clearipnbarprotocol-discovery** コマンドを使用します。

clear ip nbar protocol-discovery [**interface** *type number*]

構文の説明

interface	（任意）設定するインターフェイスのタイプを指定します。
type	（任意）インターフェイスのタイプです。
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。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
15.0(1)M	このコマンドは、Cisco IOS Release 15.0(1)M よりも前のリリースに導入されました。
12.2(33)SRC	このコマンドは、Cisco IOS Release 12.2(33)SRC よりも前のリリースに統合されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI よりも前のリリースに統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズの集約サービス ルータに実装されました。

使用上のガイドライン

NBAR Protocol Discovery 機能によって収集された統計情報をクリアするには、**clearipnbarprotocol-discovery** コマンドを使用します。このコマンドは、デフォルトでは、Protocol Discovery 機能が有効になっているすべてのインターフェイスの統計情報をクリアします。

例

次の例は、NBAR Protocol Discovery 機能によって収集された統計情報をクリアする方法を示しています。

```
Router# clear ip nbar protocol-discovery interface serial 3/1
```

関連コマンド

コマンド	説明
clearipnbar	NBAR 機能によって収集されたバッファ、フィルタ、およびポートの統計情報をクリアします。

clear ip rsvp authentication

ライフタイムの期限が切れる前にリソース予約プロトコル（RSVP）セキュリティ アソシエーションを削除するには、特権 EXEC モードで clear **iprsvpauthentication** コマンドを使用します。

clear ip rsvp authentication [{*ip-addresshostname*}]

構文の説明

ip-address	（任意）特定のネイバーとのセキュリティ アソシエーションを解除します。
hostname	（任意）特定のホストとのセキュリティ アソシエーションを解除します。

（注） *ip-address* 引数と *hostname* 引数の違いは、ネイバーを IP アドレスで指定するか、その名前で指定するかの違いです。

コマンド デフォルト

デフォルトの動作では、すべてのセキュリティ アソシエーションがクリアされます。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(15)T	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

次の場合に、clear **iprsvpauthentication** コマンドを使用します。

- ライフタイムの期限が切れる前にセキュリティ アソシエーションを削除する場合
- メモリを解放する場合
- 一部の独立ステートにあるセキュリティ アソシエーションの問題を解決する場合
- ネイバーの再認証を強制する場合

IP アドレスまたはホスト名を入力しないことで、すべての RSVP セキュリティ アソシエーションを削除できます。また、特定の RSVP ネイバーまたはホストのみを入力して削除することができます。

セキュリティ アソシエーションを削除すると、信頼された RSVP ネイバーが RSVP メッセージをさらに送信しはじめたとき、必要に応じて再度作成されます。

例

次のコマンドは、期限切れになる前にすべてのセキュリティ アソシエーションを削除する方法を示します。

```
Router# clear ip rsvp authentication
```

関連コマンド

コマンド	説明
iprsvpauthenticationlifetime	信頼できる他の RSVP ネイバーとのセキュリティ アソシエーションを RSVP が保持する期間を制御します。
showiprsvpauthentication	RSVP によって他の RSVP ネイバーとの間で確立されたセキュリティ アソシエーションを表示します。

clear ip rsvp counters

保持されているすべての IP リソース予約プロトコル（RSVP）カウンタをクリア（0 に設定）するには、特権 EXEC モードで **cleariprsvpcounters** コマンドを使用します。

clear ip rsvp counters [confirm]

構文の説明

confirm	（任意）すべての IP RSVP カウンタがクリアされたことの確認を要求します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(14)ST	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T 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、変更を容易に確認できるように、すべての IP RSVP カウンタを 0 に設定できます。

例

次の例では、保持しているすべての IP RSVP のカウンタをクリアしています。

```
Router# clear ip rsvp counters
Clear rsvp counters [confirm]
```

関連コマンド

コマンド	説明
showiprsvpcounters	送受信された RSVP メッセージのカウントを表示します。

clear ip rsvp hello instance counters

hello インスタンス カウンタの値をクリア（更新）するには、特権 EXEC モードで **cleariprsvphelloinstancecounters** コマンドを使用します。

clear ip rsvp hello instance 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 モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(31)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

例

showiprsvphelloinstancedetail コマンドと、**cleariprsvphelloinstancecounters** コマンドからの出力例を、次に示します。「Statistics」フィールドがクリアされ、0 になっていることに注意してください。

```
Router# show ip rsvp hello instance detail
Neighbor 10.0.0.2  Source  10.0.0.1
 State: UP      (for 2d18h)
 Type: PASSIVE  (responding to requests)
 I/F: Et1/1
 LSPs protecting: 0
 Refresh Interval (msec) (used when ACTIVE)
  Configured: 100
  Statistics: (from 2398195 samples)
   Min:      100
   Max:      132
   Average:  100
   Waverage: 100 (Weight = 0.8)
   Current:  100
 Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
 Counters:
 Communication with neighbor lost:
  Num times: 0
  Reasons:
   Missed acks:             0
   Bad Src_Inst received:   0
   Bad Dst_Inst received:   0
```

```
   I/F went down:           0
   Neighbor disabled Hello: 0
  Msgs Received:   2398194
   Sent:       2398195
   Suppressed: 0
Router# clear ip rsvp hello instance counters
Neighbor 10.0.0.2  Source  10.0.0.1
 State: UP      (for 2d18h)
 Type: PASSIVE  (responding to requests)
 I/F: Et1/1
 LSPs protecting: 0
 Refresh Interval (msec) (used when ACTIVE)
  Configured: 100
  Statistics:
   Min:        0
   Max:        0
   Average:    0
   Waverage:   0
   Current:    0
 Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
 Counters:
  Communication with neighbor lost:
  Num times: 0
  Reasons:
   Missed acks:             0
   Bad Src_Inst received:   0
   Bad Dst_Inst received:   0
   I/F went down:           0
   Neighbor disabled Hello: 0
  Msgs Received:   2398194
   Sent:       2398195
   Suppressed: 0
```

関連コマンド

Command	説明
iprsvpsignallinghello(configuration)	ルータで hello をグローバルに有効にします。
iprsvpsignallinghello(interface)	Fast Reroute の保護が必要なインターフェイスでの hello を有効にします。
iprsvpsignallinghellostatistics	ルータで hello 統計を有効にします。
showiprsvphellostatistics	hello パケットが hello 入力キューに入っていた時間を表示します。

clear ip rsvp hello instance statistics

インスタンスの hello 統計をクリアするには、特権 EXEC モードで **cleariprsvphelloinstancestatistics** コマンドを使用します。

clear ip rsvp hello instance 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

インスタンスに対して Hello 統計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	変更箇所
12.0(22)S	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(31)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

例

次の例は、**showiprsvphellostatistics** コマンドからの出力例と、**cleariprsvphelloinstancestatistics** コマンドの入力後のフィールド内の値を示しています。

```
Router# show ip rsvp hello statistics
 Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
   Weighted Average:0 (weight = 0.8)
   Max:4
  Current length: 0 (max:500)
 Number of samples taken: 2398525


Router# clear ip rsvp hello instance statistics
Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
   Weighted Average:0 (weight = 0.8)
```

```
  Max:0
 Current length: 0 (max:500)
Number of samples taken: 0
```

関連コマンド

コマンド	説明
iprsvpsignallinghello(configuration)	ルータで hello をグローバルに有効にします。
iprsvpsignallinghello(interface)	Fast Reroute の保護が必要なインターフェイスでの hello を有効にします。
iprsvpsignallinghellostatistics	ルータで hello 統計を有効にします。
showiprsvphellostatistics	hello パケットが hello 入力キューに入っていた時間を表示します。

clear ip rsvp hello statistics

hello 統計をグローバルにクリアするには、特権 EXEC モードで **cleariprsvphellostatistics** コマンドを使用します。

clear ip rsvp hello 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

Hello 統計はグローバルにクリアされません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2s	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(31)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

hello インプット キューに hello パケットが入っていた時間に関するすべての情報を削除するには、このコマンドを使用します。

例

showiprsvphellostatistics コマンドと **cleariprsvphellostatistics** コマンドからの出力例を、次に示します。「Packet arrival queue」フィールドの値がクリアされていることに注意してください。

```
Router# show ip rsvp hello statistics
Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
   Weighted Average:0 (weight = 0.8)
   Max:4
  Current length: 0 (max:500)
Number of samples taken: 2398525
Router# clear ip rsvp hello statistics
Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
```

```
  Average:0
  Weighted Average:0 (weight = 0.8)
  Max:0
 Current length: 0 (max:500)
Number of samples taken: 16
```

関連コマンド

コマンド	説明
iprsvpsignallinghellostatistics	ルータで hello 統計を有効にします。
showiprsvphellostatistics	hello パケットが hello 入力キューに入っていた時間を表示します。

clear ip rsvp high-availability counters

ルートプロセッサ（RP）によって保持されているリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）高可用性（HA）カウンタをクリア（0 に設定）するには、特権 EXEC モードで **cleariprsvphigh-availabilitycounters** コマンドを使用します。

clear ip rsvp high-availability 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 モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(33)SRA	このコマンドが導入されました。
12.2(33)SRB	インサービス ソフトウェア アップグレード（ISSU）のサポートが追加されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

状態、リソース障害、および履歴情報を含む HA カウンタをクリア（0 に設定）するには、**cleariprsvphigh-availabilitycounters** コマンドを使用します。

例

次の例は、現在 RP が保持しているすべての HA 情報をクリアします。

```
Router# clear ip rsvp high-availability counters
```

関連コマンド

コマンド	説明
showiprsvphigh-availabilitycounters	RP によって保持されている RSVP TE HA カウンタを表示します。

clear ip rsvp msg-pacing

（注） Cisco IOS Release 12.4(20)T では、Cisco IOS ソフトウェアで **cleariprsvpmsg-pacing** コマンドを使用できません。このコマンドが、**cleariprsvpsignallingrate-limit** コマンドによって置き換えられました。

showiprsvpneighbor コマンドからのリソース予約プロトコル（RSVP）メッセージ ペーシング出力をクリアするには、特権 EXEC モードで **cleariprsvpmsg-pacing** コマンドを使用します。

clear ip rsvp msg-pacing

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(14)ST	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
12.2(13)T	このコマンドが、**cleariprsvpsignallingrate-limit** コマンドによって置き換えられました。
12.4(20)T	このコマンドは削除されました。

例

次の例は、RSVP メッセージ ペーシング出力をクリアします。

```
Router# clear ip rsvp msg-pacing
```

関連コマンド

コマンド	説明
showiprsvpcounters	送受信された RSVP メッセージの数を表示します。

コマンド	説明
showiprsvpneighbor	現在の RSVP ネイバーを表示し、指定されたインターフェイスまたはすべてのインターフェイスに対して、そのネイバーが IP カプセル化と UDP カプセル化のどちらを使用しているのかを示します。

clear ip rsvp reservation

現在データベースに格納されているリソース予約プロトコル（RSVP）RESV 関連の受信側情報を削除するには、EXEC モードで **cleariprsvpreservation** コマンドを使用します。

clear ip rsvp reservation {*session-ip-address sender-ip-address* {**tcp**|**udp***ip-protocol*} *session-dport sender-sport*|*****}

構文の説明

session-ip-address	ユニキャストセッションの場合、これは目的の受信者のアドレスです。また、マルチキャストセッションの場合、これはセッションの IP マルチキャスト アドレスです。
sender-ip-address	送信者の IP アドレス。
tcp | **udp** | *ip-protocol*	TCP、User Datagram Protocol（UDP）、または IP プロトコル（0 ～ 65535 の範囲）です。
session-dport	宛先ポート。 （注） ポート番号は、すべてのケースで指定します。IP ヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先が 0 の場合は送信元も 0 でなくてはなりません。また、これはポートがチェックされていない可能性を示します。宛先が 0 以外の場合、送信元も 0 以外でなくてはなりません（送信元ポートが常に無視され、0 となるワイルドカード フィルタ（wf）予約を除く）。
sender-sport	送信元ポート。 （注） ポート番号は、すべてのケースで指定します。IP ヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先が 0 の場合は送信元も 0 でなくてはなりません。また、これはポートがチェックされていない可能性を示します。宛先が 0 以外の場合、送信元も 0 以外でなくてはなりません（送信元ポートが常に無視され、0 となるワイルドカード フィルタ（wf）予約を除く）。
*	すべての送信者をクリアするためにワイルドカードが使用されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。

リリース	変更箇所
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。

使用上のガイドライン

予約要求を受信した場合に、RSVP アドミッション ポリシーに基づいて関連するものを再確立できるよう、現在データベースに格納されている RESV 関連の送信者情報を削除するには、**cleariprsvpreservation** コマンドを使用します。

クロックレートやインターフェイスの帯域幅を変更するたびに、RSVP が変更を反映してデータベースを更新することはありません。これは、新しいクロックレートまたは帯域幅の値に基づき、このような変更で RSVP が予約を再確立する必要があるためです。また、一部の予約を任意で破棄してその他を保持することが好ましくないためです。解決策は、**cleariprsvpreservation** コマンドを発行することで RESV 状態をクリアすることです。

cleariprsvpreservation コマンドは、コマンドを発行したルータから RESV 状態をクリアし、ルータから PATH TEAR メッセージを上流に位置するルータに送信させ、その上流に位置するすべてのルータの予約に対する RESV 状態をクリアします。

例

次の例は、現在データベースに格納されている RESV 関連の受信側情報のすべてをクリアします。

```
Router# clear ip rsvp reservation *
```

次の例は、現在データベースに格納されている特定の予約に対する RESV 関連の受信側情報のすべてをクリアします。

```
Router# clear ip rsvp reservation 10.2.1.1 10.1.1.2 udp 10 20
```

関連コマンド

コマンド	説明
cleariprsvpsender	現在データベースに存在する RSVP PATH 関連の送信者情報を削除します。

clear ip rsvp sender

現在データベースに格納されているリソース予約プロトコル（RSVP）PATH 関連の送信者情報を削除するには、EXEC モードで **cleariprsvpsender** コマンドを使用します。

clear ip rsvp sender {*session-ip-address sender-ip-address* {**tcp**|**udp***ip-protocol*} *session-dport sender-sport*|*****}

構文の説明

session-ip-address	ユニキャストセッションの場合、これは目的の受信者のアドレスです。また、マルチキャストセッションの場合、これはセッションの IP マルチキャスト アドレスです。
sender-ip-address	送信者の IP アドレス。
tcp | **udp** | *ip-protocol*	TCP、User Datagram Protocol（UDP）、または IP プロトコル（0 ～ 65535 の範囲）です。
session-dport	宛先ポート。 （注） ポート番号は、すべてのケースで指定します。IP ヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先が 0 の場合は送信元も 0 でなくてはなりません。また、これはポートがチェックされていない可能性を示します。宛先が 0 以外の場合、送信元も 0 以外でなくてはなりません（送信元ポートが常に無視され、0 となるワイルドカード フィルタ（wf）予約を除く）。
sender-sport	送信元ポート。 （注） ポート番号は、すべてのケースで指定します。IP ヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先が 0 の場合は送信元も 0 でなくてはなりません。また、これはポートがチェックされていない可能性を示します。宛先が 0 以外の場合、送信元も 0 以外でなくてはなりません（送信元ポートが常に無視され、0 となるワイルドカード フィルタ（wf）予約を除く）。
*	すべての送信者をクリアするためにワイルドカードが使用されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。

リリース	変更箇所
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。

使用上のガイドライン

予約要求を受信した場合に、RSVP アドミッション ポリシーに基づいて関連するものを再確立できるよう、現在データベースに格納されている PATH 関連の送信者情報を削除するには、**cleariprsvpsender** コマンドを使用します。

クロックレートやインターフェイスの帯域幅を変更するたびに、RSVP が変更を反映してデータベースを更新することはありません。これは、新しいクロックレートまたは帯域幅の値に基づき、このような変更で RSVP が予約を再確立する必要があるためです。また、一部の予約を任意で破棄してその他を保持することが好ましくないためです。解決策は、**cleariprsvpsender** コマンドを発行することで PATH 状態をクリアすることです。

cleariprsvpsender コマンドは、コマンドを発行したルータから PATH 状態をクリアし、ルータから PATH TEAR メッセージを下流に位置するルータに送信させ、その下流に位置するすべてのルータの予約に対する PATH 状態をクリアします。

例

次の例は、現在データベースに格納されている PATH 関連の送信者情報のすべてをクリアします。

```
Router# clear ip rsvp sender *
```

次の例は、現在データベースに格納されている特定の予約に対する PATH 関連の送信者情報のすべてをクリアします。

```
Router# clear ip rsvp sender 10.2.1.1 10.1.1.2 udp 10 20
```

関連コマンド

コマンド	説明
cleariprsvpreservation	現在データベースに存在する RSVP RESV 関連の受信側情報を削除します。

clear ip rsvp signalling fast-local-repair statistics

リソース予約プロトコル（RSVP）高速ローカル修復（FLR）カウンタをクリア（0に設定）するには、ユーザ EXEC モードまたは特権 EXEC モードで **cleariprsvpsignallingfast-local-repairstatistics** コマンドを使用します。

clear ip rsvp signalling fast-local-repair 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

デフォルトでは、すべての RSVP FLR カウンタをクリアします。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

すべての RSVP FLR カウンタを 0 に設定するには、**cleariprsvpsignallingfast-local-repairstatistics** コマンドを使用します。統計には、現在の状態、開始時刻、および修復レートなど、FLR 手順に関する情報が含まれます。

例

次の例は、データベースで保持されているすべての RSVP FLR カウンタをクリアします。

```
Router# clear ip rsvp signalling fast-local-repair statistics
```

関連コマンド

コマンド	説明
showiprsvpsignallingfast-local-repair	FLR 関連情報を表示します。

clear ip rsvp signalling rate-limit

キューがいっぱいのため破棄されたリソース予約プロトコル（RSVP）メッセージの数をクリア（0 に設定）するには、特権 EXEC モードで **cleariprsvpsignallingrate-limit** コマンドを使用します。

clear ip rsvp signalling rate-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 モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。このコマンドは **cleariprsvpmsg-pacing** コマンドを置き替えます。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

破棄されたメッセージを記録しているカウンタをクリアするには、**cleariprsvpsignallingrate-limit** コマンドを使用します。

例

次のコマンドで、すべての破棄されたメッセージをクリアする方法を示します。

```
Router# clear ip rsvp signalling rate-limit
```

関連コマンド

コマンド	説明
debugiprsvprate-limit	RSVP レート制限イベントのデバッグ メッセージを表示します。
iprsvpsignallingrate-limit	指定の期間中に隣接ルータに送信される RSVP メッセージの伝送レートを制御します。
showiprsvpsignallingrate-limit	RSVP メッセージのレート制限パラメータを表示します。

clear ip rsvp signalling refresh reduction

再送信回数および誤った順序のリソース予約プロトコル（RSVP）メッセージの番号に関連付けられたカウンタをクリア（0 に設定）するには、EXEC モードで **cleariprsvpsignallingrefreshreduction** コマンドを使用します。

clear ip rsvp signalling refresh reduction

構文の説明

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

EXEC

コマンド履歴

リリース	変更箇所
12.2(13)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

再送信や誤った順序の RSVP メッセージを記録しているカウンタをクリアするには、**cleariprsvpsignallingrefreshreduction** コマンドを使用します。

例

次のコマンドは、すべての再送信および誤った順序のメッセージをクリアする方法を示しています。

```
Router# clear ip rsvp signalling refresh reduction
```

関連コマンド

コマンド	説明
iprsvpsignallingrefreshreduction	リフレッシュ削減をイネーブルにします。
showiprsvpsignallingrefreshreduction	RSVP メッセージのリフレッシュ削減パラメータを表示します。

clear mls qos

マルチレイヤ スイッチング（MLS）集約の Quality of Service（QoS）統計をクリアするには、特権 EXEC モードで **clearmlsqos** コマンドを使用します。

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

構文の説明

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

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 2 に追加されました。
12.2(17a)SX	このコマンドが変更され、**mpls** キーワードが追加されました。
12.2(17d)SXB	スーパーバイザ エンジン 2 上のこのコマンドのサポートが Release 12.2(17d)SXB に拡張されました。

リリース	変更箇所
12.2(18)SXD	このコマンドが変更され、**arp** キーワードが追加されました。
12.2(18)SXE	このコマンドが変更され、**ipv6** および **arp** キーワードが Supervisor Engine 2 のみで追加されました。
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。

使用上のガイドライン

interface-type の有効値には、**ge-wan**、**atm**、および **pos** キーワードがあり、Supervisor Engine 2 で設定された Cisco 7600 シリーズ ルータでサポートされています。

ipx キーワードは、Supervisor Engine 2 で設定された Cisco 7600 シリーズ ルータでのみサポートされます。

ipv6 および **arp** キーワードは、Supervisor Engine 720 で設定された Cisco 7600 シリーズ ルータでのみサポートされます。

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

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

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

（注） **clearmlsqos** コマンドを入力すると、ポリシングのトークン バケット カウンタが影響を受け、ポリシングされるはずのトラフィックがわずかに転送される可能性があります。

例

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

```
Router# clear mls qos
```

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

```
Ro
uter# clear mls qos ip
```

関連コマンド

コマンド	説明
showmlsqos	MLS QoS 情報を表示します。

clear service-group traffic-stats

サービス グループのいずれか、またはすべてに対するトラフィック統計情報をクリアするには、特権 EXEC モードで **clearservice-grouptraffic-stats** コマンドを使用します。

clear service-group traffic-stats [**group** *service-group-identifier*]

構文の説明

group	（任意）サービス グループ。
service-group-identifier	（任意）サービス グループ番号。統計をクリアするサービス グループ番号を入力します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(33)SRE	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 グループ番号を指定しない場合は、すべてのサービス グループの統計がクリアされます。

（注） サービス グループのトラフィック統計情報をクリアしてもグループ メンバーのトラフィック統計情報はクリアされません。グループ メンバーのトラフィック統計情報をクリアするには、**clearethernetserviceinstance** コマンドを使用します。**clearethernetserviceinstance** コマンドの詳細については、『*Cisco IOS Carrier Ethernet Command Reference*』を参照してください。

例

すべてのサービス グループのトラフィック統計情報をクリアする方法を、次に示します。

```
Router> enable
Router# clear service-group traffic-stats
```

関連コマンド

コマンド	説明
clearethernetserviceinstance	MAC アドレスなどのイーサネット サービス インスタンス属性と統計をクリアし、イーサネット サービス インスタンスのエラーを消去します。

compression header ip

特定のクラスに対して Real-time Transport Protocol（RTP）または TCP IP ヘッダー圧縮を設定するには、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 **compressionheaderip** コマンドを使用します。特定のクラスに対して RTP または TCP IP ヘッダー圧縮を削除するには、このコマンドの **no** 形式を使用します。

compression header ip [{**rtp**|**tcp**}]
no compression header ip

構文の説明

rtp	（任意）RTPヘッダー圧縮を設定します。
tcp	（任意）TCPヘッダー圧縮を設定します。

コマンド デフォルト

RTP または TCP ヘッダー圧縮を指定しない（つまり、コマンド名の後で Enter キーを押す）場合、RTP と TCP ヘッダー圧縮の両方が設定されます。これは「全体で圧縮を使用する」というシナリオに対応することを目的としています。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(13)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

すべての形式の **compressionheaderip** コマンドは、以前に入力された形式を上書きします。

compressionheaderip コマンドは、モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）機能を使用して設定されたポリシーマップ階層の任意のレベルで使用できます。

例

次の例では、「class1」というクラスに対して RTP ヘッダー圧縮を使用するように **compressionheaderip** コマンドが設定されています。class1 は、「policy1」というポリシー マップの一部です。

```
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# compression header ip rtp
Router(config-pmap-c)# end
```

関連コマンド

コマンド	説明
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapclass	指定されたポリシーマップの指定されたクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

control-plane

コントロール プレーン コンフィギュレーション モードでは、デバイスのコントロール プレーンに関連付けられた属性またはパラメータ（サービス ポリシーなど）の関連付けまたは変更を実行できます。この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 **control-plane** コマンドを使用します。既存のコントロール プレーン コンフィギュレーションをルータから削除するには、このコマンドの **no** 形式を使用します。

T リリースの構文
control-plane [{**host**|**transit**|**cef-exception**}]
no control-plane [{**host**|**transit**|**cef-exception**}]

12.0S リリースの構文
control-plane [**slot** *slot-number*] [{**host**|**transit**|**cef-exception**}]
no control-plane [**slot** *slot-number*] [{**host**|**transit**|**cef-exception**}]

Cisco 7600 シリーズ ルータ用 12.2S リリースの構文
control-plane
no control-plane

ASR 1000 シリーズ ルータの構文
control-plane [host]
no control-plane [host]

構文の説明

host	（任意）ホスト コントロール プレーン トラフィックにポリシーを適用します。
transit	（任意）中継コントロール プレーン トラフィックにポリシーを適用します。
cef-exception	（任意）CEF 例外コントロール プレーン トラフィックにポリシーを適用します。
slot *slot-number*	（任意）QoS ポリシーをアタッチして、分散コントロール プレーン（CP）サービスを設定するライン カードのスロット番号を指定します。

コマンド デフォルト

コントロール プレーン サービス ポリシーは定義されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.2(18)S	このコマンドが導入されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.0(29)S	このコマンドが、Cisco IOS Release 12.0(29)S に統合されました。

リリース	変更箇所
12.0(30)S	**slot***slot-number* パラメータが、分散コントロール プレーン（CP）サービスを設定するために追加されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
12.4(4)T	**host**,**transit** および **cef-exception** キーワードが追加されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.2	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

control-plane コマンドの入力後、コントロール プレーン ポリシング（CoPP）、ポートフィルタ、またはキューしきい値ポリシーを適用し、コントロールプレーン宛のトラフィックをポリシングできます。ルート プロセッサ（RP）に対する集約 CoPP を定義し、サービス ポリシーを設定してコントロール プレーン宛のすべてのトラフィックを次のようにポリシングできます。

- ルータ（集計 CP サービス）のすべてのラインカードから
- ライン カードのすべてのインターフェイスから（分散 CP サービス）

集約 CP サービスは、コントロール プレーン宛のトラフィックと、ルータのすべてのライン カードから中央のスイッチ エンジンで受信したトラフィックを管理します。

分散 CP サービスは、集計 CP サービスが適用される中央のスイッチ エンジンに対して CP パケットが転送される前に、指定したライン カード上のインターフェイスから CP トラフィックを管理します。

（注） Cisco 12000 シリーズ インターネット ルータでは、分散 CP サービスと集約 CP サービスを組み合わせて、DoS 攻撃からコントロール プレーンを保護し、パケットの QoS を提供できます。**slot***slot-number* パラメータは、分散 CP サービス設定にのみ使用します。

コントロール プレーン ポリシングには、強化されたコントロール プレーン機能が含まれています。ルータ上の閉じたまたはリッスンされていない Cisco IOS TCP/UPD ポート宛てにダイレクトされたパケットを早期にドロップするメカニズムを提供します。また、正常に動作していない単一のプロトコル プロセスがコントロール プレーン インターフェイス ホールド キューに割り込みをしないように、プロトコル キューの使用率を制限する機能を提供します。

（注） **control-plane** コマンドは、Cisco IOS Release 12.2S により、Cisco 7600 ルータに対してのみサポートされています。その他の Cisco IOS リリースでは、Cisco 7600 は **nocontrol-plane** コマンドのみをサポートし、以前の既存の設定条件は廃止されました。

この機能強化により、コントロール プレーン トラフィックを異なるカテゴリのトラフィックに分類できます。これらのカテゴリは次のとおりです。

- コントロール プレーン ホスト サブインターフェイス：ルータ インターフェイスのいずれかが直接の宛先となるすべてのコントロール プレーン IP トラフィックを受信するサブインターフェイス。コントロール プレーン ホスト IP トラフィックの例には、トンネル終端トラフィック、管理トラフィック、ルーティング プロトコルなど（SSH、SNMP、BGP、OSPF、EIGRP など）があります。すべてのホスト トラフィックは、ルータによって終端し、処理されます。ほとんどのコントロールプレーン保護機能とポリシーは、コントロールプレーン ホストサブインターフェイス上で厳格に運用されます。ほとんどの重要なルータ コントロール プレーン サービス（ルーティング プロトコルや管理トラフィックなど）がコントロール プレーン ホスト サブインターフェイス上で受信されるため、ポリシングおよび保護ポリシーによってこのトラフィックを保護することは不可欠です。CoPP機能、ポート フィルタリング機能、およびプロトコルごとのキューしきい値保護機能をコントロール プレーン ホスト サブインターフェイスに適用できます。
- コントロールプレーン中継サブインターフェイス：ルートプロセッサによってソフトウェア スイッチングされるすべてのコントロール プレーン IP トラフィックを受信するサブインターフェイス。つまり、パケットは、ルータ自体を直接の宛先とするのではなく、ルータを経由して移動します。ルータによって処理される非終端トンネルは、このタイプのコントロール プレーン トラフィックの一例です。コントロール プレーン保護機能では、このサブインターフェイスで受信されるすべてのトラフィックに特定の集約ポリシングを適用できます。
- コントロール プレーン CEF 例外サブインターフェイス：プロセス スイッチング用に CEF パケット転送パスで設定された入力機能の結果としてリダイレクトされるか、インターフェイス ドライバによってコントロール プレーン入力キューに直接追加されるすべてのトラフィック（ARP、L2 キープアライブ、および非 IP ホスト トラフィック）を受信するサブインターフェイス。コントロールプレーン保護機能を使用すると、この特定のタイプのコントロール プレーン トラフィックに対する特定の集約ポリシングを実行できます。

例

次の例では、送信元アドレス 10.1.1.1 および 10.1.1.2 を持つ信頼できるホストを設定し、制約を設けずに Telnet パケットをコントロール プレーンに転送する方法を示します。残りのすべての Telnet パケットは、指定したレートでポリシングされるようにします。次に、集約CPサービスに対し、ルータのすべてのライン カードからコントロール プレーンに入るすべてのパケットに QoS ポリシーが適用されます。

```
! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
```

```
! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class map "telnet-class."
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-in
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control-plane service for the active route processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# end
```

次の例では、送信元アドレス 10.1.1.1 および 10.1.1.2 を持つ信頼できるホストを設定し、制約を設けずに Telnet パケットをコントロール プレーンに転送する方法を示します。スロット 1 経由で入る残りのすべての Telnet パケットは、指定したレートでポリシングされるようにします。QoS ポリシーは、分散 CP サービスに対し、スロット 1 のライン カードのインターフェイスを経由して入り、コントロールプレーンを宛先とするすべてのパケットに適用されます。

```
! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class map "telnet-class."
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-in
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control-plane service for the active route processor.
Router(config)# control-plane slot 1
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# end
```

次の例は、集約 CoPP ポリシーをホスト コントロール プレーン機能パスに適用することで、ホスト コントロール プレーン トラフィックに適用する方法を示しています。

```
Router(config)# control-plane host
Router(config-cp)# service-policy input cpp-policy-host
```

次の例は、集約 CoPP ポリシーを中継コントロール プレーン機能パスに適用することで、中継コントロールプレーン トラフィックに適用する方法を示しています。

```
Router(config)# control-plane transit
Router(config-cp)# service-policy input cpp-policy-transit
```

次の例は、集約 CoPP ポリシーを CEF 例外コントロール プレーン機能パスに適用することで、例外コントロール プレーン トラフィックに適用する方法を示しています。

```
Router(config)# control-plane cef-exception
Router(config-cp)# service-policy input cpp-policy-cef-exception
```

関連コマンド

コマンド	説明
class(policy-map)	作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルト クラス（一般に class-default クラスといいます）を指定します。
class-map	QoS クラス マップ コンフィギュレーション モードにアクセスして QoS クラス マップを設定します。
drop	特定のクラスに属するパケットを廃棄するトラフィック クラスを設定します。
matchaccess-group	指定した ACL をベースにクラス マップに対して一致基準を設定します。
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。
service-policy(control-plane)	集約コントロール プレーン サービスまたは分散コントロール プレーン サービス用に、ポリシー マップをコントロール プレーンにアタッチします。
showpolicy-mapcontrol-plane	コントロール プレーンにアタッチされたポリシー マップのあるクラス、またはすべてのクラスの設定を表示します。

copy interface

コマンドで指定されているインターフェイスに対し、特定のクラスに属するパケットをコピーするトラフィック クラスを設定するには、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 **copyinterface** コマンドを使用します。パケットがコピーされるのを防ぐには、このコマンドの **no** 形式を使用します。

copy interface *interface type number*
no copy interface *interface type number*

構文の説明

interface type number	パケットを送信する必要があるインターフェイスのタイプおよび数です。

コマンド デフォルト

このコマンドを指定しないと、パケットはインターフェイスにコピーされません。

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.2(18)ZYA1	このコマンドが導入されました。

使用上のガイドライン

定義済みのインターフェイスにパケットをコピーするには、このコマンドを使用します。元のパケットは定義済みの宛先に送信され、コピーされたパケットはコピー先のインターフェイスに送信されます。**copyinterface** コマンドは **log** コマンドとともに設定することもできますが、**drop** コマンドまたは **redirectinterface** コマンドとともに設定することはできません。スタック クラスのサービス ポリシーを使用して、このコマンドを構成することはできません。パケットは、次のインターフェイスにのみコピーできます。

- Ethernet
- ファスト イーサネット
- ギガビット イーサネット
- Ten Gigabit Ethernet

例

次の例では、cmtest というトラフィック クラスを作成し、pmtest というポリシー マップで使用できるように設定しています。ポリシー マップ（サービス ポリシー）は、FastEthernet インターフェイス 4/18 に適用されます。cmtest クラスのすべてのパケットは、FastEthernet インターフェイス 4/15 にコピーされます。

```
Router(config)# policy-map type access-control pmtest
Router(config-pmap)# class cmtest
Router(config-pmap-c)# copy interface FastEthernet 4/15
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
```

```
Router(config)# interface FastEthernet 4/18
Router(config-if)#
service-policy input pmtest
```

関連コマンド

コマンド	説明
log	ポリシーマップ クラス コンフィギュレーション モードまたはクラス マップ コンフィギュレーション モードでログ メッセージを生成します。
showclass-map	すべてのクラス マップおよびその一致基準を表示します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

custom-queue-list

（注） Cisco IOS XE Release 2.6 および Cisco IOS Release 15.1(3)T 以降では、**custom-queue-list** コマンドは表示されません。このコマンドはCisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンド シーケンス）を使用する必要があります。詳細（代替コマンドのリストを含む）については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**custom-queue-list** コマンドは、モジュラ QoS CLI（MQC）コマンド（または MQC コマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

インターフェイスにカスタム キュー リストを割り当てるには、インターフェイス コンフィギュレーション モードで **custom-queue-list** コマンドを使用します。特定のリストまたはすべてのリストの割り当てを削除するには、このコマンドの **no** 形式を使用します。

custom-queue-list [*list-number*]
no custom-queue-list [*list-number*]

構文の説明

list-number	カスタム キュー リストのための 1 ～ 16 の番号です。

コマンド デフォルト

カスタム キュー リストは割り当てられていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
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。

リリース	変更箇所
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。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

使用上のガイドライン

1 つのインターフェイスに 1 つのキュー リストのみを割り当てることができます。**priority-listinterface** コマンドの代わり（追加はせず）に、このコマンドを使用してください。カスタム キューイングでは、プライオリティ キューイングで提供されない均等性が実現されます。カスタム キューイングを使用すると、インターフェイスでキューに入れられた集約トラフィックに対応できない場合に、インターフェイスで利用可能な帯域幅を制御できます。それぞれの出力キューに関連付けられるのは設定可能なバイト カウントであり、これによりシステムが次のキューに移動する前に現在のキューから送信するバイト数が指定されます。特定のキューが処理されている間は、パケットは、送信されたバイト数がキューのバイト カウントを超えるまで、またはキューが空になるまで送信されます。

カスタム出力キューの現在の状態を表示するには、**showqueueingcustom** コマンドと **showinterfaces** コマンドを使用します。

例

次の例では、シリアル インターフェイス 0 にカスタム キュー リスト番号 3 が割り当てられています。

```
interface serial 0
 custom-queue-list 3
```

関連コマンド

Command	Description
priority-listinterface	特定のインターフェイスから着信するパケットのキューイング プライオリティを確立します。
queue-listdefault	キュー リストの他のルールに一致しないパケット用にプライオリティ キューを割り当てます。
queue-listinterface	インターフェイスに着信するパケットのキューイング プライオリティを確立します。

Command	Description
queue-listqueuebyte-count	特定のサイクル中に特定のキューからシステムが配信できるバイト数を指定します。
queue-listqueuelimit	キューに対してキューの長さ制限を指定します。
showinterfaces	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

D から F

- default ip nbar protocol-pack （121 ページ）
- description（クラスマップ） （122 ページ）
- description（サービス グループ） （124 ページ）
- df （125 ページ）
- disconnect qdm （126 ページ）
- drop （128 ページ）
- dscp （130 ページ）
- dscp（カスタム） （133 ページ）
- estimate bandwidth （135 ページ）
- exponential-weighting-constant （137 ページ）
- fair-queue（class-default） （139 ページ）
- fair-queue（DWFQ） （142 ページ）
- fair-queue（policy-map クラス） （145 ページ）
- fair-queue (WFQ) （147 ページ）
- air-queue aggregate-limit （154 ページ）
- fair-queue individual-limit （156 ページ）
- fair-queue limit （158 ページ）
- fair-queue qos-group （160 ページ）
- fair-queue tos （162 ページ）
- fair-queue weight （164 ページ）
- feedback （166 ページ）
- flow idle-timeout （168 ページ）
- flow rate fixed （169 ページ）
- frame-relay interface-queue priority （170 ページ）
- frame-relay ip rtp compression-connections （173 ページ）
- frame-relay ip rtp header-compression （175 ページ）
- frame-relay ip rtp priority （177 ページ）
- frame-relay ip tcp compression-connections （181 ページ）
- frame-relay ip tcp header-compression （183 ページ）

- frame-relay map ip compress （185 ページ）
- frame-relay map ip nocompress （187 ページ）
- frame-relay map ip rtp header-compression （189 ページ）
- group（サービス グループ） （192 ページ）
- hw-module slot（ESP スケジューリング） （194 ページ）
- hw-module subslot（チャネライズド SPA スケジューリング） （197 ページ）

default ip nbar protocol-pack

Cisco ルータの Cisco IOS イメージに存在するプロトコル パックのベース バージョンをロードし、他のすべてのプロトコルのパックを削除するには、グローバル コンフィギュレーション モードで **default ip nbar protocol-pack** コマンドを使用します。

default ip nbar protocol-pack [*protocol-pack*]

構文の説明

protocol-pack	（オプション）プロトコル パック ファイルのパスおよび名前。

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	変更箇所
Cisco IOS XE リリース 3.3S	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

プロトコル パックは、複数のプロトコル記述言語（PDL）ファイルとマニフェスト ファイルを含む単一の圧縮ファイルです。このプロトコル パックが導入される前は、PDL を個別にロードする必要がありました。Network-Based Application Recognition（NBAR）プロトコル パックを使用すると、プロトコル セットをロードできます。このプロトコル セットは、ネットワーク分類のために NBAR で追加のプロトコルを認識するために役立ちます。

default ip nbar protocol-pack コマンドを使用すると、すべてのプロトコル パックはルータから削除されます（ルータの Cisco IOS イメージに付属するベース バージョンは除く）。

例

次の例は、デフォルトのプロトコル パックをロードし、他のすべてのプロトコル パックを削除する方法を示しています。

```
Router# configure terminal
Router(config)# default ip nbar protocol-pack
```

関連コマンド

コマンド	説明
ipnbarprotocol-pack	プロトコル パックをロードします。
showipnbarprotocol-pack	プロトコルパック情報を表示します。

description（クラスマップ）

クラス マップまたはポリシー マップに説明を追加するには、クラスマップ コンフィギュレーションまたはポリシー マップ 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。クラスマップまたはポリシーマップから説明を削除するには、このコマンドの **no** フォームを使用します。

description *character-string*
no description

構文の説明

character-string	クラス マップまたはポリシー マップに追加されるコメントまたは説明。文字列は 161 文字を超えることはできません。

コマンド デフォルト

このコマンドが発行されていない場合、説明はありません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

ポリシー マップ コンフィギュレーション（config-pmap）

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。
12.2(18)ZY	このコマンドが、Catalyst 6500 シリーズの Programmable Intelligent Services Accelerator（PISA）が搭載されているスイッチの Cisco IOS Release 12.2(18)ZY に統合されました。

使用上のガイドライン

description コマンドは、単に設定にコメントを含めることで、クラス マップにどのパケットを含めるかなど、クラス マップまたはポリシー マップに関する情報を覚えやすくすることを目的にしています。

例

次の例は、「ip-udp」およびポリシーマップ「fpm-policy」内の説明を指定する方法を示しています。

```
class-map type stack match-all ip-udp
 description “match UDP over IP packets”
 match field ip protocol eq 0x11 next udp
!
policy-map type access-control fpm-policy
 description “drop worms and malicious attacks”
 class ip-udp
 service-policy fpm-udp-policy
!
!
```

```
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラスマップを作成します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

description（サービス グループ）

サービス グループの説明を追加するには、サービス グループ 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。サービス グループの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 *descriptive-text*
no description

構文の説明

descriptive-text	サービス グループの説明。240 文字以内で、サービス グループの説明を入力します。

コマンド デフォルト

サービス グループの説明は追加されません。

コマンド モード

サービス グループ コンフィギュレーション（config-service-group）

コマンド履歴

リリース	変更箇所
12.2(33)SRE	このコマンドが導入されました。

使用上のガイドライン

アカウント番号、場所、サブスクライバ名など、サービス グループについての追加情報を提供するには、**description**（サービス グループ）コマンドを使用します。

例

次の例は、サービス グループ 1 を作成する方法、およびサブスクライバのアカウント番号を識別する情報をどのように説明に追加するかを示しています。

```
Router> enable
Router# configure terminal
Router(config)# service-group 1
Router(config-service-group)# description
 subscriber account number 105AB1
Router(config-service-group)# end
```

df

遅延要因（DF）の計算用アルゴリズムを変更するには、モニタ パラメータ モードで **df** コマンドを使用します。デフォルトの DF アルゴリズム（rfc4445）を使用するには、このコマンドの **no** 形式を使用します。

df *algorithm_name*
no df *algorithm_name*

構文の説明

algorithm_name	遅延要因を計算するために使用するアルゴリズム。次のアルゴリズムがサポートされています。 • **ipdv** • **rfc4445**

コマンド デフォルト

rfc4445 アルゴリズムが使用されます。

コマンド モード

モニタのパラメータ（config-map-c-monitor）

コマンド履歴

リリース	変更箇所
15.1(1)S	このコマンドが導入されました。

使用上のガイドライン

遅延要因アルゴリズムを変更するには、**df** コマンドを使用します。設定されたアルゴリズムは、クラスの IP-CBR フローと MDI フローの両方に使用されます。ipdv ベースのアルゴリズムはフロー レートに依存せず、ネットワークによって生じる遅延のみを報告します。rfc4445 ベースのアルゴリズムはレートに依存し、設定されたフロー レートを使用します。rfc4445 ベースのアルゴリズムは、パケット間遅延とネットワークによって生じる遅延の合計をレポートします。

例

次の例は、ipdv ベースのアルゴリズムに対する遅延要因の設定方法を示しています。

```
router(config-pmap-c-monitor)# df ipdv
```

関連コマンド

Command	Description
showpolicy-maptypeperformance-traffic	使用する DF アルゴリズムとともに、ポリシー マップ情報を表示します。

disconnect qdm

Quality of Service Device Manager（QDM）クライアントを切断するには、EXEC モードまたは特権 EXEC モードで **disconnectqdm** コマンドを使用します。

disconnect qdm [**client** *client-id*]

構文の説明

client	（オプション）特定の QDM クライアントが切断されるよう指定します。
client-id	（オプション）切断する特定の QDM 識別番号を指定します。QDM 識別番号の範囲は、0 ～ 2,147,483,647 です。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

EXEC
特権 EXEC

コマンド履歴

リリース	変更箇所
12.1(1)E	このコマンドが導入されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

ルータに接続されるすべての QDM クライアントを切断するには、**disconnectqdm** コマンドを使用します。

ルータに接続された特定の QDM クライアントを切断するには、**disconnectqdm** [**client***client-id*] コマンドを使用します。たとえば、**disconnectqdmclient42** コマンドを使用すると、ID 42 の QDM クライアントを切断します。

（注） Cisco 7600 シリーズでは、QDM は Cisco Optical Services Module（OSM）インターフェイスでサポートされていません。

例

次の例は、すべての接続済み QDM クライアントを切断するための方法を示しています。

```
Router# disconnect qdm
```

次の例は、クライアント ID 9 の 特定の QDM クライアントを切断する方法を示しています。

```
Router# disconnect qdm client 9
```

関連コマンド

コマンド	説明
showqdmstatus	接続済みQDMクライアントの状態を表示します。

drop

特定のクラスに属するパケットを廃棄するようにトラフィック クラスを設定するには、ポリシー クラス コンフィギュレーション モードで **drop** コマンドを使用します。トラフィック クラスのパケット廃棄処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

drop
no drop

構文の説明

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

無効

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.2(13)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

トラフィック クラス内のパケットを無条件に廃棄するために **drop** コマンドを設定する場合は、次の点に注意してください。

- パケットの廃棄は、トラフィック クラスで設定できる唯一のアクションです。つまり、トラフィック クラス内ではその他の処理は一切設定できません。
- トラフィック クラスを **drop** コマンドで設定する場合、この特定のトラフィック クラスの「子」（入れ子になっている）ポリシーは、**servicepolicy** コマンドを使用して設定することはできません。
- パケットの廃棄は、デフォルト クラス（class-default クラス）には設定できません。

例

次に、「class1」というトラフィック クラスを作成し、それを「policy1」というポリシー マップに使用するように設定する例を示します。ポリシー マップ（サービス ポリシー）は、出力シリアル インターフェイス 2/0 に適用されます。access-group 101 に一致するすべてのパケットが class1 に配置されます。このクラスに属しているパケットが廃棄されます。

```
Router(config)# class-map class1
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

```
Router(config)# interface serial2/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

関連コマンド

コマンド	説明
showclass-map	すべてのクラス マップおよびその一致基準を表示します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

dscp

Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値の最小および最大パケットしきい値を変更するには、random-detect-group 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。最小および最大パケットしきい値を DSCP 値の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。

dscp *dscp-value min-threshold max-threshold* [*mark-probability-denominator*]
no dscp *dscp-value min-threshold max-threshold* [*mark-probability-denominator*]

構文の説明

dscp-value	DSCP 値を指定します。DSCP 値は、0 ～ 63 の値にすることができます。または、次のキーワードのいずれかにすることができます。**ef**、**af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、または **cs7**
min-threshold	パケット数での最小しきい値。この引数に指定できる値の範囲は、1 ～ 4096 です。キューの平均の長さが最小しきい値に達すると、重み付けランダム早期検出（WRED）は指定した DSCP 値の一部のパケットをランダムにドロップします。
max-threshold	パケット数での最大しきい値。この引数に指定できる値の範囲は、*min-threshold* の値 ～ 4096 です。キューの平均の長さが最大しきい値を超えると、WRED は指定した DSCP 値のすべてのパケットをドロップします。
mark-probability-denominator	（任意）キューの平均の深さが最大しきい値にあるときにドロップされたパケットの割合の分母。たとえば、分母が 512 の場合、512 パケットごとに 1 つのパケットが、平均キューが最大しきい値にあるときにドロップします。値の範囲は、1 ～ 65536 です。デフォルトは 10 で、最大しきい値では 10 パケットごとに 1 つのパケットがドロップされます。

コマンド デフォルト

WRED がパケットをドロップする可能性の計算に DSCP 値を使用している場合は、DSCP テーブルのすべてのエントリが、「使用上のガイドライン」の表に示されているデフォルト設定で初期化されます。

コマンド モード

Random-detect-group コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(5)T	このコマンドが導入されました。
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。

リリース	変更箇所
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

このコマンドは、**random-detect-group** コマンドと組み合わせて使用する必要があります。

さらに、**dscp** コマンドは、**random-detect-group** コマンドの使用時に *dscp-based* 引数を指定した場合にのみ利用できます。

次の表に、**dscp** コマンドが使用する DSCP のデフォルト設定を示します。次の表に、DSCP 値と、その対応する最小しきい値、最大しきい値、およびマーク確率を示します。表の最後の行（「デフォルト」というラベルが付いている行）は、この表には登場しない DSCP 値すべてで使用されるデフォルト設定を表します。

表 *2 : dscp* のデフォルト設定

DSCP（優先順位）	最小しきい値	最大しきい値	マーク確率
af11	32	40	1/10
af12	28	40	1/10
af13	24	40	1/10
af21	32	40	1/10
af22	28	40	1/10
af23	24	40	1/10
af31	32	40	1/10
af32	28	40	1/10
af33	24	40	1/10
af41	32	40	1/10
af42	28	40	1/10
af43	24	40	1/10
cs1	22	40	1/10
cs2	24	40	1/10
cs3	26	40	1/10
cs4	28	40	1/10

DSCP（優先順位）	最小しきい値	最大しきい値	マーク確率
cs5	30	40	1/10
cs6	32	40	1/10
cs7	34	40	1/10
ef	36	40	1/10
rsvp	36	40	1/10
[デフォルト（default）]	20	40	1/10

例

次に、DSCP 値 af22 を使用するように WRED をイネーブル化する例を示します。DSCP 値 af22 の最小しきい値は 28、最大しきい値は 40、マーク確率は 10 です。

```
Router> enable
Router# configure terminal
Router(config)# random-detect-group class1 dscp-based
Router(cfg-red-group)# dscp af22 28 40 10
Router(cfg-red-group)# end
```

関連コマンド

Command	Description
random-detect-group	per-VC WRED または per-VC DWRED をイネーブルにします。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。
showqueueinginterface	インターフェイスまたは VC のキューイングの統計情報を表示します。

dscp（カスタム）

Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を指定するには、カスタム 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。指定した DSCP 値を関連付け解除するには、このコマンドの no 形式を使用します。

dscp *dscp-value*
no dscp *dscp-value*

構文の説明

dscp-value	DSCP 値を指定します。DSCP 値は、0 ～ 63 の数値にすることができます。または、次のキーワードのいずれかにすることができます。**ef**、**af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs7**、または **default**

コマンド デフォルト

NBAR は、DSCP 値を使用するトラフィックを認識しません。

コマンド モード

カスタム コンフィギュレーション（config-custom）

コマンド履歴

リリース	変更箇所
15.5(2)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

このコマンドは、**ip nbar custom transport** コマンドと組み合わせて使用する必要があります。

次の表に、**dscp** コマンドが使用する DSCP のデフォルト設定を示します。

表 *3 : dscp* のデフォルト設定

DSCP（優先順位）	**説明**
af11	パケットを AF11 DSCP（001010）と一致させます。
af12	パケットを AF12 DSCP（001100）と一致させます。
af13	パケットを AF13 DSCP（001110）と一致させます。
af21	パケットを AF21 DSCP（010010）と一致させます。
af22	パケットを AF22 DSCP（010100）と一致させます。
af23	パケットを AF23 DSCP（010110）と一致させます。
af31	パケットを AF31 DSCP（011010）と一致させます。

DSCP （優先順位）	説明
af32	パケットを AF32 DSCP（011100）と一致させます。
af33	パケットを AF33 DSCP（011110）と一致させます。
af41	パケットを AF41 DSCP（100010）と一致させます。
af42	パケットを AF42 DSCP（100100）と一致させます。
af43	パケットを AF43 DSCP（100110）と一致させます。
cs1	パケットを CS1（precedence 1）DSCP（001000）と一致させます。
cs2	パケットを CS2（precedence 2）DSCP（010000）と一致させます。
cs3	パケットを CS3（precedence 3）DSCP（011000）と一致させます。
cs4	パケットを CS4（precedence 4）DSCP（100000）と一致させます。
cs5	パケットを CS5（precedence 5）DSCP（101000）と一致させます。
cs6	パケットを CS6（precedence 6）DSCP（110000）と一致させます。
cs7	パケットを CS7（precedence 7）DSCP（111000）と一致させます。
ef	パケットを EF DSCP（101110）と一致させます。
[デフォルト（default）]	パケットをデフォルトの DSCP（000000）と一致させます。

例

次の例は、DSCP 値を指定する方法を示しています。

```
Router> enable
Router# configure terminal
Router(config)#  ip nbar custom mycustom transport tcp id 100
Router(config-custom)#  dscp ef
Router(config-custom)# end
```

関連コマンド

Command	Description
ip nbar custom transport	NBAR を有効にして、IP アドレス、ポート、および DSCP に基づいてトラフィックを認識し、アプリケーション ID を関連付けます。

estimate bandwidth

トラフィック データに基づき、特定の Quality of Service（QoS）目標のトラフィック クラスごとに必要な帯域幅を推定するには、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 **estimatebandwidth** コマンドを使用します。推定帯域幅残量を無効にするには、このコマンドの **no** 形式を使用します。

estimate bandwidth [**drop-one-in** *n*] [**delay-one-in** *n* **milliseconds** *n*]
no estimate bandwidth

構文の説明

drop-one-in *n*	（オプション）パケット損失率。たとえば、値が 999 の場合、999 個のパケットのうちで破棄されるのは最大で 1 個という意味です。*n* の範囲は、50 ～ 1000000 パケットです。
delay-one-in *n* **milliseconds** *n*	（オプション）パケットの遅延時間と遅延確率。*n* の範囲は、50 ～ 1000000 パケットです。遅延しきい値。*n* の範囲は 8 ～ 1000 ミリ秒です。

コマンド デフォルト

無効

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.3(14)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

目標の廃棄確率、遅延時間と遅延確率、およびタイムフレームを指定するには、**estimatebandwidth** コマンドを使用します。

遅延時間を指定する場合は、遅延しきい値も指定する必要があります。

キーワードなしで **estimatebandwidth** コマンドを発行すると、デフォルト ターゲットは、2 パーセント未満の破棄です。これは、**estimatebandwidthdrop-one-in500** と入力するのと同じです。

例

次の例の QoS 目標は、破棄が 100 個のパケットのうち 1 個未満、遅延が 100 個のパケットのうち 1 個未満で 50 ミリ秒超です。

```
Router(config-pmap-c)# estimate bandwidth drop-one-in 100 delay-one-in 100 milliseconds
 50
```

関連コマンド

コマンド	説明
bandwidth(policy-mapclass)	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。

exponential-weighting-constant

重み付けランダム早期検出（WRED）パラメータ グループのための平均キュー サイズの指数加重係数を設定するには、random-detect-group コンフィギュレーション モードで **exponential-weighting-constant** コマンドを使用します。グループの指数加重係数をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

exponential-weighting-constant *exponent*
no exponential-weighting-constant

構文の説明

exponent	平均キュー サイズの計算で使用される 1 ～ 16 の指数。

コマンド デフォルト

デフォルトの加重係数は 9 です。

コマンド モード

random-detect-group コンフィギュレーション（cfg-red-group）

コマンド履歴

リリース	変更箇所
11.1(22)CC	このコマンドが導入されました。
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。

使用上のガイドライン

使用時には、このコマンドは **random-detect-group** コマンドの入力後に発行されます。

WRED パラメータ グループの平均キュー サイズ計算に使用される指数を変更するには、このコマンドを使用します。平均キューサイズは、キューの前回の平均と現在のサイズを基にしています。式は次のようになります。

average = (old_average * (1-1/2^x)) + (current_queue_size * 1/2^x)

ここで、*x* は、このコマンドで指定される指数加重係数です。したがって、係数が大きいほど、この平均は前回の平均への依存が大きくなります。

（注） デフォルトの WRED パラメータ値は、最高の使用可能データに基づきます。値を変更することでアプリケーションに利点があると判断した場合を除き、パラメータのデフォルト値を変更しないことを推奨します。

x を高い値にすると、前回の平均が重要視されます。係数を大きくすると、キューの長さの最大値と最小値が滑らかになります。平均キュー サイズは、すぐには変化しない傾向があります。WRED 処理で、パケットのドロップの開始が遅くなりますが、実際のキュー サイズが最

低しきい値を下回った時点でも、パケットのドロップが続く場合があります。結果的に平均がゆっくり変化し、トラフィックの一時的なバーストに対応します。

x の値が高すぎる場合、WRED は輻輳に反応しません。パケットは、WRED が無効のときのように送信またはドロップします。

x の値が低い場合、平均キューサイズは現在のキューサイズ付近を追跡します。結果、平均はトラフィック レベルの変化とともに上下します。この場合、WRED 処理は、長いキューに素早く応答します。キューが最低しきい値を下回ると、パケットのドロップ処理が停止します。

x の値が低すぎると、WRED は一時的なトラフィック バーストに過剰に反応し、不必要にトラフィックをドロップします。

例

次の例は、加重係数 10 の sanjose という WRED グループを設定する方法を示しています。

```
random-detect-group sanjose
 exponential-weighting-constant 10
```

関連コマンド

Command	Description
protect	VC または PVC バンドル メンバーに適用するための保護されたグループあるいは保護された VC または PVC ステータスを使用して、VC または PVC クラスを設定します。
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detect-group	WRED または DWRED パラメータ グループを定義します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。
showqueueinginterface	インターフェイスまたは VC のキューイングの統計情報を表示します。

fair-queue（class-default）

class-default クラスで使用するために予約するダイナミック キューの数をデフォルト クラス ポリシーの一部として指定するには、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 **fair-queue** コマンドを使用します。class-default ポリシーから設定済みのダイナミック キューの数を削除するには、このコマンドの **no** 形式を使用します。

fair-queue [*number-of-dynamic-queues*]
no fair-queue [*number-of-dynamic-queues*]

構文の説明

number-of-dynamic-queues	（任意）ダイナミック キューの数を指定する 2 の累乗。範囲は 16 ～ 4096 です。

コマンド デフォルト

ダイナミック キューの数は、インターフェイスまたは ATM 相手先固定接続（PVC）の帯域幅から導出されます。重み付け均等化キューイング（WFQ）およびクラスベース WFQ（CBWFQ）がインターフェイスで有効になっている場合に使用するダイナミック キューのデフォルト数については、「使用上のガイドライン」の表を参照してください。WFQ または CBWFQ が ATM PVC で有効になっている場合に使用するダイナミック キューのデフォルト数については、「使用上のガイドライン」の表を参照してください。

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
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。

使用上のガイドライン

このコマンドは、デフォルト クラス（一般に class-default クラスとして知られているクラス）にしか使用できません。**queue-limit** コマンドまたは **random-detect** コマンドのいずれかと組み合わせて使用できます。

class-default クラスは、トラフィックがポリシー マップ内でポリシーの定義されている他のどのクラスの条件も満たさなかった場合に、そのトラフィックの送信先となるデフォルト クラスです。

次の表は、重み付け均等化キューイング（WFQ）およびクラスベース WFQ（CBWFQ）がインターフェイスで有効になっている場合に使用するダイナミック キューのデフォルト数を示しています。

表 *4:* インターフェイス帯域幅の関数としてのデフォルトのダイナミック キュー数

帯域幅範囲	ダイナミック キューの数
64 kbps 以下	16
64 kbps より大きく 128 kbps 以下	32
128 kbps より大きく 256 kbps 以下	64
256 kbps より大きく 512 kbps 以下	128
512 kbps より大きい	256

次の表に、WFQ または CBWFQ が ATM PVC 上で有効になっている場合に使用するダイナミック キューのデフォルト数を示します。

表 *5: ATM PVC* 帯域幅の関数としてのデフォルトのダイナミック キュー数

帯域幅範囲	ダイナミック キューの数
128 kbps 以下	16
128 kbps より大きく、512 kbps 以下	32
512 kbps より大きく、2000 kbps 以下	64
2000 kbps より大きく、8000 kbps 以下	128
8000 kbps より大きい	256

例

次に、policy9 というポリシー マップに組み込まれるデフォルト クラスのポリシーを設定する例を示します。同じサービス ポリシー内でポリシーが設定されているその他のクラスに指定されている一致基準を満たさないパケットは、デフォルト クラスに送られます。このデフォルト クラスには、16 個のダイナミック キューが予約されています。**queue-limit** コマンドが設定されているため、各ダイナミック キューには、最大数のパケットがキューに格納されたうえでさらにパケットが到着した場合には、テール ドロップが使用されます。

```
policy-map policy9
 class class-default
 fair-queue 16
 queue-limit 20
```

次に、policy8 というポリシー マップに組み込まれるデフォルト クラスのポリシーを設定する例を示します。**fair-queue** コマンドが、デフォルト クラスに使用するために 20 個のダイナミック キューを予約します。輻輳回避には、テール ドロップではなく、Weighted Random Early Detection（WRED）パケット ドロップが使用されます。

```
policy-map policy8
 class class-default
 fair-queue 64
 random-detect
```

関連コマンド

Command	Description
queue-limit	キューが保持できる、ポリシー マップ内に設定されるクラス ポリシーのパケットの最大数を指定または変更します。
random-detect(interface)	WRED または DWRED をイネーブルにします。

fair-queue（DWFQ）

Versatile Interface Processor（VIP）による分散重み付け均等化キューイング（DWFQ）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 **fair-queue** コマンドを使用します。DWFQ を無効にするには、このコマンドの **no** 形式を使用します。

fair-queue
no fair-queue

構文の説明

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

DWFQ は、帯域幅が 2.048 以下の物理インターフェイスでデフォルトで有効です。

デフォルトのキューの長さおよびしきい値については、このコマンドの「使用上のガイドライン」のセクションにある表を参照してください。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
11.1	このコマンドが導入されました。
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。

使用上のガイドライン

fair-queue（DWFQ）コマンドは、VIP2-40 以降のインターフェイス プロセッサを使用するインターフェイスで DWFQ を有効にします。

DWFQ を使用すると、パケットはフローによって分類されます。パケットは、同じ発信元 IP アドレス、宛先 IP アドレス、発信元 TCP または User Datagram Protocol（UDP）ポート、宛先 TCP または UDP ポート、および同じフローに属するプロトコルを持ちます。

DWFQ は、各フローに、帯域幅の共有を均等に割り当てます。

次の表に、デフォルトのキューの長さとしきい値を示します。

表 *6:* デフォルトの均等化キューの長さとしきい値

キューまたはしきい値	デフォルト
輻輳の破棄しきい値	64 メッセージ

キューまたはしきい値	デフォルト
ダイナミック キュー	256 キュー
予約可能キュー	0 キュー

DWFQ はインターフェイスで設定できますが、サブインターフェイスでは設定できません。Fast EtherChannel、トンネル、またはマルチリンク PPP（MLP）などの他の論理インターフェイスや仮想インターフェイスではサポートされません。

（注） [**no**] **fair-queue** インターフェイス コンフィギュレーション コマンドは、マルチリンク PPP インターフェイスのメンバー リンクに対して有効な設定ではありません。このコマンドは、マルチリンク インターフェイス上で設定するときにのみ有効です。双方向のトラフィック フローがあるときに、[**no**] **fair-queue** をメンバー リンク インターフェイス上で設定すると、マルチリンク インターフェイスで出力キューが詰まってしまう可能性があります。このような場合に問題を解決するには、インターフェイスの **shut**/**noshut** またはルータのリロードが必要になることがあります。この問題の原因を説明するため、「例」のセクションに設定例が示されています。

例

次の例は、High-Speed Serial Interface（HSSI）0/0/0 で DWFQ を有効にする方法を示しています。

```
interface Hssi0/0/0
 description 45Mbps to R2
 ip address 10.200.14.250 255.255.255.252
 fair-queue
```

次の例は、**nofair-queue** コマンドにより、2 つのシリアル インターフェイスの基本的な設定で、出力キューがマルチリンク インターフェイスで詰まってしまった結果を示しています。

```
configure terminal
interface serial0/0/0:0
no fair-queue
no max-reserved-bandwidth 90
tx-queue-limit 19
!
interface serial0/0/1:0
no fair-queue
no max-reserved-bandwidth 90
tx-queue-limit 19
```

（注） このサンプル設定は、問題の説明のために提供されています。この構成は使用しないでください。

関連コマンド

Command	Description
fair-queue(WFQ)	インターフェイスに対する WFQ を有効にします。
fair-queueaggregate-limit	DWFQ のすべての組み合わせのキューのパケットの最大数を設定します。
fair-queueindividual-limit	DWFQ に対する個々のキューの最大深度を設定します。
fair-queuelimit	特定の DWFQ クラスの最大キューの深さを設定します。
fair-queueqos-group	DWFQ を有効にし、内部 QoS グループ番号に基づいてパケットを分類します。
fair-queuetos	DWFQ を有効にし、パケットの ToS フィールドを使用してパケットを分類します。
showinterfaces	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。
showinterfacesfair-queue	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。

fair-queue（policy-map クラス）

トラフィック クラスで使用するために予約するキューの数を指定するには、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 **fair-queue** コマンドを使用します。トラフィック クラスから設定済みのキューの数を削除するには、このコマンドの **no** 形式を使用します。

fair-queue [*dynamic-queues*]
no fair-queue [*dynamic-queues*]

構文の説明

dynamic-queues	（任意）ダイナミック カンバセーション キューの数を指定する数字。指定できる値の範囲は 16 ～ 4096 です。

コマンド デフォルト

キューは予約されていません。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合され、Versatile Interface Processor（VIP）対応型 Cisco 7500 シリーズ ルータに実装されました。
12.1(5)T	このコマンドが Cisco IOS Release 12.1(5)T に統合され、VIP 対応の Cisco 7500 シリーズ ルータに実装されました。
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。

使用上のガイドライン

VIP では、**fair-queue** コマンドは、任意のトラフィック クラスに使用できます（非 VIP プラットフォームでは、これとは逆に **fair-queue** コマンドをデフォルト トラフィック クラスでしか使用できません）。**fair-queue** コマンドは、**queue-limit** コマンドまたは **random-detectexponential-weighting-constant** コマンドを併用して使用できます。

例

次に、policy9 というポリシー マップのデフォルト トラフィック クラスを設定して、同じサービス ポリシー内でポリシーが設定されているその他のトラフィック クラスに指定されている一致基準を満たさなかったパケット用に 10 個のキューを予約する例を示します。**queue-limit** コマンドが設定されているため、各キューには、最大数のパケットがキューに格納されたうえでさらにパケットが到着した場合には、テール ドロップが使用されます。

```
policy-map policy9
 class class-default
 fair-queue 10
 queue-limit 20
```

次に、class1 というユーザ定義のトラフィック クラスに関連付けられている policy8 というサービス ポリシーを設定する例を示します。**fair-queue** コマンドは、サービス ポリシーに使用するために 20 個のキューを予約します。輻輳回避には、テール ドロップではなく、Weighted Random Early Detection（WRED）または分散 WRED（DWRED）パケット ドロップが使用されます。

```
policy-map policy8
 class class1
 fair-queue 20
   random-detect exponential-weighting-constant 14
```

関連コマンド

コマンド	説明
classclass-default	サービス ポリシー マップのデフォルト トラフィック クラスを指定します。
queue-limit	キューが保持できる、ポリシー マップ内に設定されるクラス ポリシーのパケットの最大数を指定または変更します。
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。

fair-queue (WFQ)

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、インターフェイス コンフィギュレーション モードで **fair-queue** コマンドは表示されなくなりました。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンド シーケンス）を使用する必要があります。詳細（代替コマンドのリストを含む）については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S 以降では、**fair-queue** コマンドはモジュラ QoS CLI (MQC) コマンド（または MQC コマンドのシーケンス）に置き換えられています。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

Weighted Fair Queuing（WFQ; 重み付け均等化キューイング）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 モードまたはポリシー マップ クラス コンフィギュレーション モードで **fair-queue** コマンドを使用します。WFQ を無効にするには、このコマンドの **no** 形式を使用します。

fair-queue [*congestive-discard-threshold* [*dynamic-queues* [*reservable-queues*]]]
no fair-queue

構文の説明

congestive-discard-threshold	（オプション）各キューで許可されるメッセージ数。指定できる範囲は 1 ～ 4096 であり、デフォルトは 64 メッセージに設定されています。会話がこのしきい値に到達すると、新しいメッセージ パケットは廃棄されます。 （注） 階層型キューイング フレームワーク（HQF）を設定している場合、値は 16 ～ 4096 です。
dynamic-queues	（オプション）ベストエフォート型会話（特殊なネットワーク サービスを必要としない通常の会話）に使用されるダイナミック キューの数。値は、**16**、**32**、**64**、**128**、**256**、**512**、**1024**、**2048**、および **4096** です。デフォルトのダイナミック キューの数については、**fair-queue**（class-default）コマンドの表を参照してください。

reservable-queues	（オプション）0 ～ 1000 の範囲の予約された会話に使用される予約可能なキューの数。デフォルトは0です。予約可能なキューは、リソース予約プロトコル（RSVP）などの機能に設定されるインターフェイスで使用されます。

コマンド デフォルト

均等化キューイングは、2.048 Mbps以下の帯域幅かつ次のものを使用しない物理インターフェイスに対してデフォルトで有効になっています。

- X.25 および Synchronous Data Link Control（SDLC）カプセル化
- Link Access Procedure, Balanced（LAPB; 平衡型リンク アクセス手順）
- Tunnels
- ループバック
- ダイヤラ
- ブリッジ
- 仮想インターフェイス

上記のプロトコルでは、均等化キューイングはオプションではありません。ただし、カスタム キューイングまたはプライオリティ キューイングを対象のリンクに有効にすると、均等化キューイングは上書きされて無効になります。さらに、自律スイッチング エンジンまたはシリコン スイッチング エンジン メカニズムを有効にすると、均等化キューイングは自動的に無効になります。

（注） 各種キューイング メカニズムは、マルチシャーシ マルチリンク PPP（MMP）などのマルチリンクを使用して設定できます。ただし、PPPのみがトンネルされたインターフェイスに使用されている場合、たとえば仮想プライベート ダイヤルアップ ネットワーク（VPDN）、PPP over Ethernet（PPPoE）、PPP over Frame Relay（PPPoFR）などの場合は、仮想インターフェイスでキューイングは設定されません。

ダイナミック キューの数は、インターフェイスまたは ATM 相手先固定接続（PVC）の帯域幅から導出されます。WFQ およびクラスベース WFQ（CBWFQ）がインターフェイスで有効になっている場合に使用するダイナミック キューのデフォルト数については、**fair-queue**（class-default）コマンドの表を参照してください。WFQ または CBWFQ が ATM PVC で有効になっている場合に使用するダイナミック キューのデフォルト数については、**fair-queue**（class-default）コマンドの表を参照してください。

コマンド モード

インターフェイス コンフィギュレーション（config-if）
ポリシー マップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
11.0	このコマンドが導入されました。
12.2(13)T	このコマンドが変更され、プロトコルおよびトラフィック ストリーム識別フィールドのリストから Apollo、VINES、および XNS が削除されました。Apollo Domain、Banyan VINES、および Xerox Network Systems（XNS）がこのリリースで削除されたため、これらのプロトコルは削除されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。
12.2(33)SB	このコマンドの動作が、PRE3 用と PRE4 用の Cisco 10000 シリーズ ルータで変更されました。
12.4(20)T	モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）を使用した HQF およびユーザ定義クラスのサポートが追加されました。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

使用上のガイドライン

概要

このコマンドはWFQを有効にします。WFQを使用すると、パケットはフローによって分類されます。たとえば、パケットは、同じ発信元 IP アドレス、宛先 IP アドレス、発信元 TCP または User Datagram Protocol（UDP）ポート、宛先 TCP または UDP ポート、および同じフローに属するプロトコルを持ちます。プロトコルとトラフィック ストリーム識別フィールドの詳細なリストについては、下の表を参照してください。

WFQ をインターフェイスで有効にすると、WFQ によってトラフィックの優先順位管理が提供され、最初にアクセス リストを定義しなくても個々のトラフィック ストリームが自動的にソートされます。WFQ を有効にするために必要なのは、このコマンドのみです。

インターフェイスでWFQを有効にすると、輻輳の破棄しきい値（設定したもの、またはデフォルト）に達した後、高帯域幅トラフィック ストリームの新しいメッセージは破棄されます。ただし、コントロール メッセージの通信など、低帯域幅の通信ではデータのキューイング処理が続行されます。その結果、均等化キューには、設定したしきい値の数よりも多いメッセージが含まれることがあります。

WFQ は、トラフィック データ ストリームの識別登録サービスを使用してトラフィック ストリームが属するメッセージを決定します。各転送プロトコルについて、トラフィックをデータ ストリームに分類するために使用するメッセージ属性を、次の表に示します。

表 *7:* 重み付け均等化キューイングのトラフィック ストリーム識別フィールド

フォワーダ	使用されるフィールド
AppleTalk	• 送信元ネットワーク/ノード/ソケット • 宛先ネットワーク/ノード/ソケット • タイプ
コネクションレス型ネットワーク サービス（CLNS）	• 送信元ネットワーク サービス アクセス ポイント（NSAP） • 宛先 NSAP
DECnet	• 送信元アドレス • 接続先アドレス
フレーム リレー スイッチング	• データ リンク接続識別子（DLCI）の値
IP	• タイプ オブ サービス（ToS） • IP プロトコル • 送信元 IP アドレス（メッセージがフラグメント化されていない場合） • 宛先 IP アドレス（メッセージがフラグメント化されていない場合） • 送信元 TCP/UDP ポート • 宛先 TCP/UDP ポート
トランスペアレント ブリッジング	• ユニキャスト：送信元 MAC、宛先 MAC • Ethertype Service Advertising Protocol（SAP）/Subnetwork Access Protocol（SNAP）マルチキャスト：宛先 MAC アドレス

フォワーダ	使用されるフィールド
ソースルート ブリッジング	• ユニキャスト：送信元 MAC、宛先 MAC • SAP/SNAP：宛先 MAC アドレス
Novell NetWare	• 送信元/宛先ネットワーク/ホスト/ソケット • レベル 2 プロトコル
その他すべて（デフォルト）	• 制御プロトコル（プロトコルごとに 1 つのキュー）

IP precedence

IP プレシデンス、フレーム リレー スイッチングの輻輳、および廃棄適性（DE）フラグは、キューイングの重みに影響します。

ホストまたはポリシーマップによって設定される IP プレシデンスは、0 ～ 7 の範囲の数です。プレシデンス値のデータ ストリームは、プレシデンス 0（通常）のデータ ストリームと比較して値 + 1 倍の速度の実効ビット レートが提供されるように重み付けされます。

FECN および BECN

フレーム リレー スイッチングでは、Forward Explicit Congestion Notification（FECN; 順方向明示的輻輳通知）のメッセージフラグ、逆方向明示的輻輳通知（BECN）のメッセージフラグ、および DE メッセージフラグにより、アルゴリズムは効果的に低い優先順位を適用する重みを選択します。キューの優先順位が低くなることで、アプリケーションに「減速」のフィードバックを提供してトラフィックをソートし、設定情報レート（CIR）の範囲内で最高のサービスを提供します。

均等化キューイング、カスタム キューイング、およびプライオリティ キューイング

均等化キューイングは、X.25 を除くすべての LAN および回線（WAN）プロトコル（LAPB と SDLC を含む）に対してサポートされています。「コマンドデフォルト」セクションの注を参照してください。トンネルは物理的なインターフェイスを介してルーティングされるソフトウェア インターフェイスであるため、トンネルに対して均等化キューイングはサポートされません。均等化キューイングは、2 Mbps 以下の帯域幅のインターフェイスに対してはデフォルトです。

（注） Route Switch Processor（RSP）カードを備えた Cisco 7000 および 7500 ルータの Release 10.3 以降で、**tx-queue-limit** コマンドを使用して、Multiport Communications Interface（MCI）または Serial Port Communications Interface（SCI）カードのインターフェイスに利用可能な送信制限を設定し、そのインターフェイスにカスタム キューイングまたはプライオリティ キューイングを設定した場合、設定した送信制限は自動的に上書きされ、1 に設定されていました。Cisco IOS Release 12.0 以降のリリースでは、WFQ、カスタム キューイング、およびプライオリティ キューイングに対して、インターフェイスに設定された帯域幅の値から、**bandwidth**（インターフェイス）コマンドを使用して送信制限が取得されます。帯域幅の値を 512 で割って切り上げると、実効送信制限値を算出できます。ただし、算出された値は、**tx-queue-limit** コマンドが使用されていない場合にのみ適用されます。つまり、設定された送信制限は、この算出値を上書きします。

RSVP

均等化キューイングをサポートするインターフェイス、または予約可能なキューを 0（デフォルト）に設定して均等化キューイングのために設定されたインターフェイスにリソース予約プロトコル（RSVP）を設定する場合、予約可能なキューサイズは、32 kbps でインターフェイスの帯域幅を割ることで自動的に設定されます。0 以外の予約キューを指定することによって、このデフォルト値を上書きできます。RSVP の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Configuring RSVP」の章を参照してください。

Cisco 10000 シリーズ ルータ

Cisco IOS Release 12.2(33)SB では、シリアル インターフェイスからの no fair-queue コマンドはルータによって削除されます。

HQF

Cisco IOS Release 12.4(20)T 以降では、イメージが HQF サポートを備えている場合、クラスのデフォルトで **fair-queue** コマンドが自動的に有効になることはありません。HQF 対応のイメージを使用する前に、fair-queue コマンドと、その他のサポートされるキューイング機能を有効にする必要があります。

例

次の例は、シリアル インターフェイス 0 で WFQ を有効にして輻輳しきい値を 300 にします。このしきい値は、300 以上のメッセージがキューに入れられ、キュー内に複数のメッセージが存在するデータ ストリーム内のキューにそのメッセージが入れられた場合にのみ、キューイング システムからメッセージが破棄されることを意味します。中継キュー制限は、**bandwidth** コマンドによって設定される 384 キロビット（Kb）回線に基づいて 2 に設定されます。

```
interface serial 0
 bandwidth 384
 fair-queue 300
```

パラメータが指定されていない場合は、デフォルト値になります。

次に、64 メッセージ、512 ダイナミック キュー、および 18 RSVP キューを含む均等化キューを要求する例を示します。

```
interface serial 3/0
 ip unnumbered ethernet 0/0
 fair-queue 64 512 18
```

次の例に示すように、ユーザ定義クラスに対して**fair-queue**コマンドを適用できます。

```
policy-map p1
 class c1
  bandwidth 1000
  fair-queue
```

関連コマンド

Command	Description
bandwidth(interface)	インターフェイスの帯域幅値を設定します。
custom-queue-list	カスタム キュー リストをインターフェイスに割り当てます。
fair-queue(class-default)	デフォルト クラス ポリシーの一部として class-default クラスで使用するために予約するダイナミック キューの数を指定します。
fair-queue(DWFQ)	DWFQ を有効にします。
priority-group	指定した優先リストをインターフェイスに割り当てます。
priority-listdefault	優先リストの他の規則に一致しないパケット用にプライオリティ キューを割り当てます。
showinterfaces	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。
showqueue	特定のインターフェイスまたはVCのキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。
tx-queue-limit	MCIおよびSCIカードの指定したインターフェイスに使用可能な中継バッファの数を制御します。

air-queue aggregate-limit

Versatile Interface Processor（VIP）による分散重み付け均等化キューイング（DWFQ）のために組み合わせられるすべてのキューにパケット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 **fair-queueaggregate-limit** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

fair-queue aggregate-limit *aggregate-packets*
no fair-queue aggregate-limit

構文の説明

aggregate-packets	一部のパケットが破棄されるまでにバッファが許可されるパケットの合計数。この制限を下回る場合、パケットはドロップされません。

コマンド デフォルト

許可されるパケットの合計数は、インターフェイスの転送速度と VIP の利用可能なバッファスペースに基づきます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
11.1 CC	このコマンドが導入されました。
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。

使用上のガイドライン

一般に、すべてのキューで許可されるパケットの最大数は、デフォルトから変更するべきではありません。特定の状況で、異なる値を使用することで利点を得られると判断した場合にのみ、このコマンドを使用してください。

DWFQ では、それぞれのキューにパケットの数のトラックと、すべてのキューにパケットの合計数を保持しています。

パケットの合計数が集約制限より少ない場合、キューは個々のキュー制限よりも多くのパケットをバッファできます。

パケットの合計数が集約制限に達した場合、インターフェイスは個別のキュー制限の適用を開始します。新しいパケットの到着で個別のキュー制限を超える場合、そのパケットは破棄されます。キュー内にすでに存在するパケットは、キューが個別の制限を超えた場合でも削除されません。

場合によっては、すべてのキューにあるパケットの合計数が集約制限を超えてしまう場合があります。

例

次の例では、集約制限を 54 パケットに設定する方法を示しています。

```
interface Fddi9/0/0
 fair-queue tos
 fair-queue aggregate-limit 54
```

関連コマンド

Command	Description
fair-queuelimit	特定の DWFQ クラスの最大キューの深さを設定します。
fair-queueqos-group	DWFQ を有効にし、内部 QoS グループ番号に基づいてパケットを分類します。
fair-queuetos	DWFQ を有効にし、パケットの ToS フィールドを使用してパケットを分類します。
showinterfaces	ルータまたはアクセスサーバで設定されているすべてのインターフェイスの統計情報を表示します。
showinterfacesfair-queue	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。

fair-queue individual-limit

Versatile Interface Processor（VIP）による分散重み付け均等化キューイング（DWFQ）のために個々のキューの最大深度を設定するには、インターフェイス コンフィギュレーション モードで **fair-queueindividual-limit** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

fair-queue individual-limit *individual-packet*
no fair-queue individual-limit

構文の説明

individual-packet	輻輳期間に各フロー別または各クラス別キューで許容する最大パケット数。

コマンド デフォルト

集約キュー制限の半分

コマンド 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	変更箇所
11.1 CC	このコマンドが導入されました。
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。

使用上のガイドライン

一般に、個々のキューの最大深度は、デフォルトから変更するべきではありません。特定の状況で、異なる値を使用することで利点を得られると判断した場合にのみ、このコマンドを使用してください。

DWFQ では、それぞれのキューにパケットの数のトラックと、すべてのキューにパケットの合計数を保持しています。

パケットの合計数が集約制限より少ない場合、キューは個々のキュー制限よりも多くのパケットをバッファできます。

パケットの合計数が集約制限に達した場合、インターフェイスは個別のキュー制限の適用を開始します。新しいパケットの到着で個別のキュー制限を超える場合、そのパケットは破棄されます。キュー内にすでに存在するパケットは、キューが個別の制限を超えた場合でも削除されません。

場合によっては、すべてのキューにあるパケットの合計数が集約制限を超えてしまう場合があります。

例

次の例は、個々のキュー制限を 27 に設定する方法を示しています。

```
interface Fddi9/0/0
 mac-address 0000.0c0c.2222
 ip address 10.1.1.1 255.0.0.0
 fair-queue tos
 fair-queue individual-limit 27
```

関連コマンド

Command	Description
fair-queue(class-default)	DWFQ のすべての組み合わせのキューのパケットの最大数を設定します。
fair-queuelimit	特定の DWFQ クラスの最大キューの深さを設定します。
fair-queueqos-group	DWFQ を有効にし、内部 QoS グループ番号に基づいてパケットを分類します。
fair-queuetos	DWFQ を有効にし、パケットの ToS フィールドを使用してパケットを分類します。
showinterfaces	ルータまたはアクセスサーバで設定されているすべてのインターフェイスの統計情報を表示します。
showinterfacesfair-queue	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。

fair-queue limit

Versatile Interface Processor（VIP）による分散重み付け均等化キューイング（DWFQ）のために特定のキューの最大深度を設定するには、インターフェイス コンフィギュレーション モードで **fair-queuelimit** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

fair-queue {**qos-group** *number*|**tos** *number*} **limit** *class-packet*
no fair-queue {**qos-group** *number*|**tos** *number*} **limit** *class-packet*

構文の説明

qos-group *number*	Border Gateway Protocol（BGP）機能経由の専用アクセス レート（CAR）ポリシーまたはポリシーの伝播によって割り当てられる QoS グループの数。値の範囲は 1 ～ 99 です。
tos *number*	タイプ オブ サービス（ToS）フィールドの 2 つの低次 IP プレシデンス ビット。
class-packet	輻輳の期間中に、クラスのキューで許可されるパケットの最大数。

コマンド デフォルト

fair-queueindividual-limit コマンドによって指定された個々のキュー深度。
fair-queueindividual-limit コマンドが設定されていない場合、デフォルトは集約キュー制限の半分です。

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	変更箇所
11.1 CC	このコマンドが導入されました。
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。

使用上のガイドライン

クラスベースの DWFQ のために特定のクラスのキュー深度の値を指定するには、このコマンドを使用します。このコマンドは、**fair-queueindividual-limit** コマンドによって指定されたグローバルな個々の制限を上書きします。

一般に、この値はデフォルトから変更するべきではありません。特定の状況で、異なる値を使用することで利点を得られると判断した場合にのみ、このコマンドを使用してください。

例

次の例は、ToS グループの個々のキュー制限を 3 ～ 20 に設定する方法を示しています。

```
interface Fddi9/0/0
 mac-address 0000.0c0c.2222
 ip address 10.1.1.1 255.0.0.0
 fair-queue tos
 fair-queue tos 3 limit 20
```

関連コマンド

Command	Description
fair-queue(class-default)	DWFQ のすべての組み合わせのキューのパケットの最大数を設定します。
fair-queueqos-group	DWFQ を有効にし、内部 QoS グループ番号に基づいてパケットを分類します。
fair-queuetos	DWFQ を有効にし、パケットの ToS フィールドを使用してパケットを分類します。
showinterfaces	ルータまたはアクセスサーバで設定されているすべてのインターフェイスの統計情報を表示します。
showinterfacesfair-queue	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。

fair-queue qos-group

Versatile Interface Processor（VIP）による分散重み付け均等化キューイング（DWFQ）を有効にし、内部 QoS グループ番号に基づいてパケットを分類するには、インターフェイス コンフィギュレーション モードで **fair-queueqos-group** コマンドを使用します。QoS グループベースの DWFQ を無効にするには、このコマンドの **no** 形式を使用します。

fair-queue qos-group
no fair-queue qos-group

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

QoS グループベースの DWFQ 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	変更箇所
11.1CC	このコマンドが導入されました。
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。

使用上のガイドライン

QoS グループベースの DWFQ（クラスベースの DWFQ のタイプ）を有効にするには、このコマンドを使用します。クラスベースの DWFQ は、フローベースの DWFQ を上書きします。したがって、このコマンドは **fair-queue**（DWFQ）コマンドを上書きします。

このコマンドが有効な場合、パケットは QoS グループに基づいて異なるキューに割り当てられます。QoS グループは、DWFQ や専用アクセス レート（CAR）など、特定の QoS 機能によってパケットの処理方法を決定するためにルータが使用する、パケットに対する内部の分類です。ボーダー ゲートウェイ プロトコル（BGP）機能経由の CAR ポリシーまたは QoS ポリシーの伝播に使用し、パケットを QoS グループに割り当てます。

各クラスの重みを指定します。輻輳の期間に、各グループはクラスの重みに等しい出力帯域幅のパーセンテージを割り当てられます。たとえば、クラスに 50 の重みが割り当てられている場合、このクラスからのパケットには輻輳の期間に発信帯域幅の少なくとも 50% が割り当てられます。

例

次の例では、QoS ベースの DWFQ を有効にし、9 個の QoS グループ（QoS グループ 0 ～ 8）の帯域幅を割り当てます。

```
interface Hssi0/0/0
```

```
description 45Mbps to R2
ip address 10.200.14.250 255.255.255.252
fair-queue qos-group
fair-queue qos-group 1 weight 5
fair-queue qos-group 2 weight 5
fair-queue qos-group 3 weight 10
fair-queue qos-group 4 weight 10
fair-queue qos-group 5 weight 10
fair-queue qos-group 6 weight 15
fair-queue qos-group 7 weight 20
fair-queue qos-group 8 weight 29
```

関連コマンド

Command	Description
fair-queue(class-default)	DWFQ のすべての組み合わせのキューのパケットの最大数を設定します。
fair-queuelimit	特定の DWFQ クラスの最大キューの深さを設定します。
fair-queuetos	DWFQ を有効にし、パケットの ToS フィールドを使用してパケットを分類します。
fair-queueweight	DWFQ のクラスに重みを割り当てます。
showinterfaces	ルータまたはアクセスサーバで設定されているすべてのインターフェイスの統計情報を表示します。
showinterfacesfair-queue	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。

fair-queue tos

Versatile Interface Processor（VIP）による分散重み付け均等化キューイング（DWFQ）を有効にし、パケットのタイプ オブ サービス（ToS）フィールドに基づいてパケットを分類するには、インターフェイス コンフィギュレーション モードで **fair-queuetos** コマンドを使用します。ToS ベースの DWFQ を無効にするには、このコマンドの **no** 形式を使用します。

fair-queue tos
no fair-queue tos

構文の説明

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

無効

デフォルトでは、クラス 0 には 10 の重み、クラス 1 には 20 の重み、クラス 2 には 30 の重み、クラス 3 には 40 の重みが割り当てられます。

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	変更箇所
11.1CC	このコマンドが導入されました。
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。

使用上のガイドライン

ToS ベースの DWFQ（クラスベースの DWFQ のタイプ）を有効にするには、このコマンドを使用します。クラスベースの DWFQ は、フローベースの DWFQ を上書きします。したがって、このコマンドは **fair-queue**（DWFQ）コマンドを上書きします。

このコマンドを有効にすると、パケットは、パケット ヘッダーの ToS フィールドの 2 つの低次 IP プレシデンスのビットに基づいて、異なるキューに割り当てられます。

輻輳の期間に、各グループはクラスの重みに等しい出力帯域幅のパーセンテージを割り当てられます。たとえば、クラスに 50 の重みが割り当てられている場合、このクラスからのパケットには輻輳の期間に発信帯域幅の少なくとも 50% が割り当てられます。

重みを変更する場合は、**fair-queueweight** コマンドを使用します。

例

次の例は、High-Speed Serial Interface（HSSI）0/0/0 で ToS ベースの DWFQ を有効にする方法を示しています。

```
interface Hssi0/0/0
```

```
description 45Mbps to R2
ip address 10.200.14.250 255.255.255.252
fair-queue
fair-queue tos
```

関連コマンド

Command	Description
fair-queue(class-default)	DWFQ のすべての組み合わせのキューのパケットの最大数を設定します。
fair-queuelimit	特定の DWFQ クラスの最大キューの深さを設定します。
fair-queueqos-group	DWFQ を有効にし、内部 QoS グループ番号に基づいてパケットを分類します。
fair-queueweight	DWFQ のクラスに重みを割り当てます。
showinterfaces	ルータまたはアクセスサーバで設定されているすべてのインターフェイスの統計情報を表示します。
showinterfacesfair-queue	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。

fair-queue weight

Versatile Interface Processor（VIP）による分散重み付け均等化キューイング（DWFQ）のためにクラスに重みを割り当てるには、インターフェイス コンフィギュレーション モードで **fair-queueweight** コマンドを使用します。クラスに対する帯域幅の割り当てを削除するには、このコマンドの **no** 形式を使用します。

fair-queue {**qos-group** *number*|**tos** *number*} **weight** *weight*
no fair-queue {**qos-group** *number*|**tos** *number*} **weight** *weight*

構文の説明

qos-group *number*	Border Gateway Protocol（BGP）機能経由の専用アクセス レート（CAR）ポリシーまたはポリシーの伝播によって割り当てられる Quality of Service（QoS）グループの数。値の範囲は、1 ～ 99 です。
tos *number*	タイプ オブ サービス（ToS）フィールドの 2 つの低次 IP プレシデンス ビット。値の範囲は、1 ～ 3 です。
weight	このクラスに割り当てられている出力リンクの帯域幅のパーセンテージ。すべてのクラスに対する重みの合計は、99以下にならなくてはなりません。

コマンド デフォルト

QoS DWFQ の場合、未割り当ての帯域幅は QoS グループ 0 に割り当てられます。

ToS ベースの DWFQ の場合、クラス 0 には 10 の重み、クラス 1 には 20 の重み、クラス 2 には 30 の重み、クラス 3 には 40 の重みが割り当てられます。

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	変更箇所
11.1CC	このコマンドが導入されました。
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。

使用上のガイドライン

特定の DWFQ クラスの帯域幅のパーセンテージを割り当てるには、このコマンドを使用します。また、**fair-queueqos-group** コマンドまたは **fair-queuetos** コマンドのいずれかを使用し、インターフェイスにクラス ベースの DWFQ を割り当てる必要があります。

すべてのクラスにこのコマンドを 1 回実行し、クラスに対して帯域幅を割り当てます。

QoS グループ ベースの DWFQ の場合、どの QoS グループにも割り当てられていないパケットは、QoS グループ 0 に割り当てられます。QoS グループ クラスに対して重みを割り当てる場合は、次のガイドラインに注意してください。

- 利用可能な帯域幅の 1% は、自動的に QoS グループ 0 に割り当てられます。
- その他すべての QoS グループの重みを合わせた合計は、99 以下でなくてはなりません。
- 未割り当ての帯域幅は QoS グループ 0 に割り当てられます。

ToS ベースの DWFQ では、次のガイドラインに注意してください。

- 利用可能な帯域幅の 1% は、自動的に ToS クラス 0 に割り当てられます。
- その他すべての ToS グループの重みを合わせた合計は、99 以下でなくてはなりません。
- 未割り当ての帯域幅は ToS クラス 0 に割り当てられます。

例

次の例は、異なる QoS グループに帯域幅を割り当てます。残りの帯域幅（5 パーセント）は、QoS グループ 0 に割り当てられます。

```
interface Fddi9/0/0
 fair-queue qos-group
 fair-queue qos-group 1 weight 10
 fair-queue qos-group 2 weight 15
 fair-queue qos-group 3 weight 20
 fair-queue qos-group 4 weight 20
 fair-queue qos-group 5 weight 30
```

関連コマンド

Command	Description
fair-queueqos-group	DWFQ を有効にし、内部 QoS グループ番号に基づいてパケットを分類します。
fair-queuetos	DWFQ を有効にし、パケットの ToS フィールドを使用してパケットを分類します。
showinterfaces	ルータまたはアクセスサーバで設定されているすべてのインターフェイスの統計情報を表示します。
showinterfacesfair-queue	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。

feedback

インターフェイスまたはリンクからのコンテキスト ステータスのフィードバック メッセージを有効にするには、IP Header Compression（IPHC）プロファイル コンフィギュレーション モードで **feedback** コマンドを使用します。コンテキスト ステータスのフィードバック メッセージを無効にするには、このコマンドの **no** 形式を使用します。

feedback
no feedback

構文の説明

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

コンテキスト ステータスのフィードバック メッセージは有効になります。

コマンド モード

IPHC プロファイル コンフィギュレーション（config-iphcp）

コマンド履歴

リリース	変更箇所
12.4(9)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

IPHC プロファイルでの使用目的

feedback コマンドは、IPHCプロファイルの一部として使用することを目的としています。IPHC プロファイルは、ネットワークでのヘッダー圧縮を有効および設定するために使用されます。IPHC プロファイルを使用してヘッダー圧縮を設定する詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、リリース 12.4T の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

制約事項

IPHC プロファイルには、Internet Engineering Task Force（IETF）プロファイルと van-jacobson プロファイルという 2 つのタイプがあります。**feedback** コマンドは、IETF IPHC プロファイルのみに対してサポートされています。**feedback** コマンドは、van-jacobson IPHC プロファイルに対してサポートされていません。IPHC プロファイル タイプの詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、Release 12.4T の「Header Compression」セクションを参照してください。

前提条件

feedback コマンドを使用する前に、TCP ヘッダー圧縮または非 TCP ヘッダー圧縮を有効にする必要があります。TCP ヘッダー圧縮を有効にするには、**tcp** コマンドを使用します。非 TCP ヘッダー圧縮を有効にするには、**non-tcp** コマンドを使用します。

コンテキスト ステータス メッセージの無効化

ヘッダー圧縮時に、セッション コンテキストが定義されます。コンテキストごとに、セッションの状態が確立され、コンプレッサとデコンプレッサ間で共有されます。コンテキストの状態は、IP/UDP/RTP ヘッダー全体、IP/UDP ヘッダー、IP/TCP ヘッダー、一次微分値、リンクのシーケンス番号、世代番号、および差分エンコーディング テーブルから構成されます。

デコンプレッサがコンプレッサとの同期を失った場合、無効化するコンテキスト ID のリストとともにデコンプレッサからコンプレッサにコンテキスト ステータス メッセージが送信されます。次にコンプレッサは、一貫性のある状態を再確立するため、デコンプレッサにフルヘッダー パケットを送信します。コンテキスト ID のためのフル ヘッダー パケットが受信されるまで、無効なコンテキスト ID のすべてのパケットが破棄されることに注意してください。

データ パスのアップリンクおよびダウンリンク部分をパケットが通過するときにかかる時間が、更新間隔よりも長い場合（この場合、コンテキスト ステータス メッセージの送信は役に立ちません）、またはフィードバック パスが存在しない場合、コンテキスト ステータス メッセージの送信を無効にできます。

例

profile2 という IPHC プロファイルの例を、次に示します。この例では、コンテキスト ステータスのフィードバック メッセージが無効になっています。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# no
 feedback
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
iphc-profile	IPHC プロファイルを作成します。
non-tcp	IPHC プロファイルの非 TCP ヘッダー圧縮を有効にします。
tcp	IPHC プロファイル内の TCP ヘッダー圧縮を有効にします。

flow idle-timeout

フローのタイムアウト値を設定するには、Per-Flow Admission コンフィギュレーション モードで **flowidle-timeout** コマンドを使用します。タイムアウト値をリセットするには、このコマンドの **no** 形式を使用します。

flow idle-timeout *timeout-value*
no flow idle-timeout *timeout-value*

構文の説明

timeout-value	秒単位のタイムアウトの長さ。デフォルトは10です。

コマンド デフォルト

このコマンドを使用しない場合、フローのタイムアウト値は 10 秒です。

コマンド モード

Per-Flow Admission コンフィギュレーション モード（config-pmap-admit-cac）

コマンド履歴

リリース	変更箇所
15.4(2)T	このコマンドが導入されました。

例

次の例は、**flow idle-timeout** コマンドの使用方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# policy-map test
Device(config-pmap-admit-cac)#flow idle-timeout 50
Device(config-pmap)# class af4
Device(config-pmap-c)# bandwidth 200
Device(config-pmap-c)# admit cac local
Device(config-pmap-admit-cac)# rate percent 80
Device(config-pmap-admit-cac)# flow rate fixed 100
Device(config-pmap-admit-cac)# flow idle-timeout 50
```

関連コマンド

コマンド	説明
rate	帯域幅プールのサイズを kbps 単位で設定するか、出力クラスの帯域幅のパーセンテージとして設定します。

flow rate fixed

各フローに帯域幅を割り当てるには、Per-Flow Admission コンフィギュレーション モードで **flow rate fixed** コマンドを使用します。帯域幅の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。

flow rate fixed *flow-bit-rate*
no flow rate fixed *flow-bit-rate*

構文の説明

flow-bit-rate	kbps 単位でビットレートを指定します。

コマンド デフォルト

明示的に設定されていない場合は、すべてのフローが定期的に帯域幅を学習します。

コマンド モード

Per-Flow Admission コンフィギュレーション モード（config-pmap-admit-cac）

コマンド履歴

リリース	変更箇所
15.4(2)T	このコマンドが導入されました。

例

次の例は、**flow rate fixed** コマンドの使用方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# policy-map test
Device(config-pmap-admit-cac)#flow idle-timeout 50
Device(config-pmap)# class af4
Device(config-pmap-c)# bandwidth 200
Device(config-pmap-c)# admit cac local
Device(config-pmap-admit-cac)# rate percent 80
Device(config-pmap-admit-cac)# flow rate fixed 100
```

関連コマンド

コマンド	説明
rate	帯域幅プールのサイズを kbps 単位で設定するか、出力クラスの帯域幅のパーセンテージとして設定します。

frame-relay interface-queue priority

フレーム リレー PVC インターフェイス プライオリティ キューイング（FR PIPQ）機能を有効にするには、インターフェイス コンフィギュレーション モードで **frame-relayinterface-queuepriority** コマンドを使用します。FR PIPQ を無効にするには、このコマンドの **no** 形式を使用します。フレーム リレー マップ クラス内で相手先固定接続（PVC）に優先度を割り当てるには、マップクラス コンフィギュレーション モードで **frame-relayinterface-queuepriority** コマンドを使用します。フレーム リレー マップ クラス内の PVC から優先度を削除するには、このコマンドの **no** 形式を使用します。

frame-relay interface-queue priority [*high-limit medium-limit normal-limit low-limit*]
no frame-relay interface-queue priority
frame-relay interface-queue priority {**high**|**medium**|**normal**|**low**}
no frame-relay interface-queue priority

構文の説明

high-limit	（任意）パケットの最大数で指定される高プライオリティ キューのサイズです。
medium-limit	（任意）パケットの最大数で指定される中プライオリティ キューのサイズです。
normal-limit	（任意）パケットの最大数で指定される標準プライオリティ キューのサイズです。
low-limit	（任意）パケットの最大数で指定される低プライオリティ キューのサイズです。
high	PVC に高プライオリティを割り当てます。
medium	PVC に中プライオリティを割り当てます。
normal	PVC に標準プライオリティを割り当てます。
low	PVC に低プライオリティを割り当てます。

コマンド デフォルト

高、中、標準、および低プライオリティ キューのデフォルト サイズは、それぞれ、20、40、60、および 80 パケットです。

FR PIPQ がインターフェイスで有効になっている場合、デフォルトの PVC プライオリティは標準プライオリティです。

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）
マップクラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(2)T	このコマンドが導入されました。
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。

リリース	変更箇所
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

PVC プライオリティのマップクラスの設定を有効にするには、FR PIPQ がインターフェイスで有効になっている必要があります。

frame-relayinterface-queuepriority コマンドを使用して FR PIPQ を設定する前に、次の条件を満たす必要があります。

- PVC は単一種類のトラフィックを伝送するよう設定する必要があります。
- ネットワークは、適切なコール アドミッション コントロールを用いて、プライオリティ キューのいずれかが足りなくならないようにする必要があります。

ファーストイン ファーストアウト（FIFO）キューイング以外のキューイングがインターフェイス レベルですでに設定されている場合、FR PIPQ を設定することはできません。重み付け均等化キューイング（WFQ）を使用している場合は、WFQ がデフォルトのインターフェイス キューイング方式になっていれば、FR PIPQ を設定できます。FR PIPQ を無効にすると、FRF.12 が有効な場合はインターフェイスがデュアル FIFO キューイングに戻り、フレーム リレー トラフィック シェーピング（FRTS）が有効な場合は FIFO キューイングに戻ります。または、インターフェイスのデフォルトのキューイング方式に戻ります。

例

次の例は、シリアル インターフェイス 0 で FR PIPQ を有効にし、高、中、標準、および低プライオリティ キューの制限をそれぞれ 10、20、30、および 40 パケットに設定する方法を示しています。PVC 100 には高プライオリティが割り当てられており、PVC 100 宛てのすべてのトラフィックは高プライオリティのインターフェイス キューに送信されます。

```
interface serial0
 encapsulation frame-relay
 frame-relay interface-queue priority 10 20 30 40
 frame-relay interface-dlci 100
  class high_priority_class
 !
 map-class frame-relay high_priority_class
  frame-relay interface-queue priority high
```

関連コマンド

コマンド	説明
debugpriority	プライオリティ キューイング イベントを表示します。
showframe-relaypvc	フレームリレー インターフェイス対応 PVC に関する統計情報を表示します。
showinterfaces	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。

コマンド	説明
showqueue	特定のインターフェイスまたはVCのキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

frame-relay ip rtp compression-connections

フレーム リレー インターフェイスに存在できる Real-time Transport Protocol（RTP）ヘッダー圧縮接続の最大数を指定するには、インターフェイス コンフィギュレーション モードで **frame-relayiprtpcompression-connections** コマンドを使用します。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。

frame-relay ip rtp compression-connections *number*
no frame-relay ip rtp compression-connections

構文の説明

number	RTP ヘッダー圧縮接続の最大数。範囲は 3 ～ 256 です。

コマンド デフォルト

256 のヘッダー圧縮接続

コマンド 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	変更箇所
12.1(2)T	このコマンドが導入されました。
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。

使用上のガイドライン

最大接続数を設定する前に、**frame-relayiprtpheader-compression** コマンドを使用し、インターフェイスに RTP ヘッダー圧縮を設定する必要があります。

RTP ヘッダー圧縮接続数は、接続の両端で同じ値に設定されている必要があります。

例

次の例は、シリアル インターフェイス 0 で RTP ヘッダー圧縮接続の最大数を 150 にする設定を示しています。

```
interface serial 0
 encapsulation frame-relay
 frame-relay ip rtp header-compression
 frame-relay ip rtp compression-connections 150
```

関連コマンド

Command	Description
frame-relayiprtpheader-compression	物理インターフェイス上のすべてのフレームリレーマップについて RTP ヘッダー圧縮をイネーブルにします。

Command	Description
frame-relaymapipcompress	RTP と TCP の両方のヘッダー圧縮をリンクで有効にします。
frame-relaymapiprtpheader-compression	DLCI ごとに RTP ヘッダー圧縮を有効にします。
showframe-relayiprtpheader-compression	フレーム リレーの RTP ヘッダー圧縮の統計情報を表示します。

frame-relay ip rtp header-compression

物理インターフェイスのすべてのフレーム リレー マップの Real-time Transport Protocol（RTP）ヘッダー圧縮を有効にするには、インターフェイス コンフィギュレーション モードで **frame-relayiprtpheader-compression** コマンドを使用します。圧縮を無効にするには、このコマンドの **no** 形式を使用します。

frame-relay ip rtp header-compression [{**active**|**passive**}] **[periodic-refresh]**
no frame-relay ip rtp header-compression [{**active**|**passive**}] **[periodic-refresh]**

構文の説明

active	（任意）すべての発信 RTP パケットを圧縮します。
passive	（任意）着信パケットに圧縮されたヘッダーがあった場合のみ、発信 RTP/User Datagram Protocol（UDP）/IP ヘッダーを圧縮します。
periodic-refresh	（任意）圧縮された IP ヘッダーを定期的にリフレッシュすることを意味します。

コマンド デフォルト

ディセーブル。

デフォルトでは、インターフェイスにどのようなタイプのヘッダー圧縮が設定されていても、継承されます。インターフェイスにヘッダー圧縮が設定されていない場合、**active** キーワードを使用しますが、**showrunning-config** コマンドの出力には **header-compression** キーワードは表示されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
11.3	このコマンドが導入されました。
12.3(2)T	このコマンドが、Cisco IOS Release 12.3(2)T に統合されました。このコマンドは、**periodic-refresh** キーワードを含むように変更されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
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。

使用上のガイドライン

frame-relayiprtpheader-compression コマンドを物理インターフェイスに使用すると、すべてのインターフェイス マップがこのコマンドを継承します。つまり、すべてのマップで UDP および RTP IP ヘッダー圧縮が実行されます。

例

次の例では、物理インターフェイス上のすべてのフレーム リレーマップに対してRTP ヘッダー圧縮を有効にする方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.1
Router(config-if)# frame-relay ip rtp header-compression
Router(config-if)# end
```

次の例では、RTP ヘッダー圧縮を有効にする方法を示します。また、オプションの **periodic-refresh** キーワードが指定されています。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.2
Router(config-if)# frame-relay ip rtp header-compression periodic-refresh
Router(config-if)# end
```

関連コマンド

Command	Description
frame-relayiprtpcompression-connections	フレーム リレー インターフェイスの RTP ヘッダー圧縮接続の最大数を指定します。
frame-relaymapipnocompress	RTP と TCP の両方のヘッダー圧縮をリンクで無効にします。
showframe-relayiprtpheader-compression	フレーム リレーの RTP ヘッダー圧縮の統計情報を表示します。

frame-relay ip rtp priority

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**frame-relayiprtppriority** コマンドは非表示です。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンド シーケンス）を使用する必要があります。詳細（代替コマンドのリストを含む）については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**frame-relayiprtppriority** コマンドは、モジュラ QoS CLI（MQC）コマンド（または MQC コマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

フレーム リレー相手先固定接続（PVC）で、User Datagram Protocol（UDP）宛先ポートの範囲に属する Real-time Transport Protocol（RTP）パケット フローのセットのために絶対優先キューを予約するには、マップクラス コンフィギュレーション モードで **frame-relayiprtppriority** コマンドを使用します。絶対優先キュ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。

frame-relay ip rtp priority *starting-rtp-port-number port-number-range bandwidth*
no frame-relay ip rtp priority

構文の説明

starting-rtp-port-number	開始 UDP ポート番号。パケットが送信先となる最小のポート番号です。ポート番号の範囲は、2000 ～ 65535 です。
port-number-range	UDP 宛先ポートの範囲。*starting-rtp-port-number* 引数に追加される番号です。最大の UDP ポート番号を算出する基になります。範囲は 0 ～ 16383 です。
bandwidth	許可される最大の帯域幅（kbps 単位）。帯域幅は、0 ～ 2000 kbps の範囲で指定できます。

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

Map-class コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(7)T	このコマンドが導入されました。
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。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

使用上のガイドライン

このコマンドは、音声アプリケーション、またはその他の遅延の影響を受けやすいアプリケーションに最も効果的です。このコマンドを使用するには、**map-classframe-relay** コマンドを最初に入力する必要があります。フレーム リレー マップ クラスを設定した後、PVC に適用する必要があります。

このコマンドは、フレーム リレー PVC をサポートすることにより、**iprtppriority** コマンドによって提供される機能を拡張します。このコマンドを使用して、同じ出力インターフェイスを使用したその他のキューまたはクラスで絶対優先サービスが音声トラフィックに保証される UDP ポートの範囲を指定できます。絶対優先とは、パケットがプライオリティ キューに存在する場合、そのパケットのキューが解除され、最初に送信されるということです。つまり、キューが解除されたその他のパケットよりも先に送信されます。

frame-relayiprtppriority コマンドを使用する前に、フレーム リレー トラフィック シェーピング（FRTS）およびフレーム リレー フラグメンテーション（FRF.12）を設定する必要があります。

音声コールごとに必要な帯域幅を減らすため、圧縮 RTP（CRTP）を使用できます。フレーム リレーとともに CRTP を使用するには、**encapsulationframe-relayietf** コマンドの代わりに、**encapsulationframe-relaycisco** コマンドを使用する必要があります。

bandwidth パラメータを設定する場合は、次のガイドラインを念頭に置いてください。

- プライオリティ キューに、必要だとわかっている帯域幅の量より少し多めに割り当てるのが最も安全です。これにより、ネットワーク バーストが発生しても対応できます。
- IP RTP プライオリティ アドミッション コントロール ポリシーは、RTP ヘッダー圧縮を考慮します。したがって、**iprtppriority** コマンドで *bandwidth* パラメータを設定している間

は、圧縮コールの帯域幅の設定のみが必要です。*bandwidth* パラメータは最大の合計帯域幅であるため、複数のコールがある場合は、すべてのコールに十分な帯域幅を割り当てる必要があります。

- レイヤ2ヘッダーに対応できる帯域幅を設定します。帯域幅の割り当てでは、ペイロードと IP、UDP、および RTP ヘッダーについては考慮されていますが、レイヤ 2 ヘッダーは考慮されていません。他のオーバーヘッドに対し 25 % の帯域幅を割り当てるのが、慎重で安全です。
- デフォルトの予約可能な最大帯域幅を変更していない限り、インターフェイス上の音声およびデータ フローのためのすべての帯域幅割り当ての合計は、利用可能な全帯域幅の 75 % を超えないようにしてください。予約可能な最大帯域幅を変更するには、そのインターフェイスで **max-reserved-bandwidth** コマンドを使用します。

IP RTP プライオリティ帯域幅割り当ての詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の章「Congestion Management Overview」のセクション「IP RTP Priority」を参照してください。

例

次は、最初に voip というフレームリレー マップ クラスを設定し、そのマップ クラスを PVC 100 に適用して、RTP パケットが一致する厳密なプライオリティ サービスを提供する例です。

```
map-class frame-relay voip
 frame-relay cir 256000
 frame-relay bc 2560
 frame-relay be 600
 frame-relay mincir 256000
 no frame-relay adaptive-shaping
 frame-relay fair-queue
 frame-relay fragment 250
 frame-relay ip rtp priority 16384 16380 210
interface Serial5/0
 ip address 10.10.10.10 255.0.0.0
 no ip directed-broadcast
 encapsulation frame-relay
 no ip mroute-cache
 load-interval 30
 clockrate 1007616
 frame-relay traffic-shaping
 frame-relay interface-dlci 100
  class voip
 frame-relay ip rtp header-compression
 frame-relay intf-type dce
```

この例では、16384 ～ 32764 の範囲の UDP ポート（32764 = 16384 + 16380）を使用する PVC 100 の RTP パケットに一致し、絶対優先サービスが提供されます。

関連コマンド

Command	Description
encapsulationframe-relay	フレームリレー カプセル化をイネーブルにします。

Command	Description
iprtppriority	UDP 宛先ポートの範囲に属する RTP パケット フロー セットについて、完全プライオリティ キューを予約します。
map-classframe-relay	SVC 用の QoS 値を定義するマップ クラスを指定します。
max-reserved-bandwidth	CBWFQ、LLQ、およびIP RTPプライオリティに割り当てるインターフェイス帯域幅のパーセント比率を変更します。
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与えます。
showframe-relaypvc	フレームリレーインターフェイス対応PVCに関する統計情報を表示します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showtraffic-shapequeue	インターフェイス レベルまたはDLCI レベルで、トラフィック シェーピングによってキューに入れられた要素に関する情報を表示します。

frame-relay ip tcp compression-connections

フレーム リレー インターフェイスに存在できる TCP ヘッダー圧縮接続の最大数を指定するには、インターフェイス コンフィギュレーション モードで**frame-relayiptcpcompression-connections** コマンドを使用します。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。

frame-relay ip tcp compression-connections *number*
no frame-relay ip tcp compression-connections

構文の説明

number	TCP ヘッダー圧縮接続の最大数。範囲は 3 ～ 256 です。

コマンド デフォルト

256 のヘッダー圧縮接続

コマンド 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	変更箇所
12.1(2)T	このコマンドが導入されました。
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。

使用上のガイドライン

最大接続数を設定する前に、**frame-relayiptcpheader-compression** コマンドを使用し、インターフェイスに TCP ヘッダー圧縮を設定する必要があります。

TCP ヘッダー圧縮接続数は、接続の両端で同じ値に設定されている必要があります。

例

次の例は、シリアル インターフェイス 0 で TCP ヘッダー圧縮接続の最大数を 150 にする設定を示しています。

```
interface serial 0
 encapsulation frame-relay
 frame-relay ip tcp header-compression
 frame-relay ip tcp compression-connections 150
```

関連コマンド

コマンド	説明
frame-relayiptcpheader-compression	物理インターフェイス上のすべてのフレームリレーマップについて TCP ヘッダー圧縮をイネーブルにします。

コマンド	説明
frame-relaymapipcompress	RTP と TCP の両方のヘッダー圧縮をリンクで有効にします。
frame-relaymapiptcpheader-compression	IP マップが関連付けられているインターフェイスの圧縮特性とは異なる IP マップに対して、ヘッダー圧縮特性を割り当てます。
showframe-relayiptcpheader-compression	インターフェイスの統計および TCP/IP ヘッダー圧縮情報を表示します。

frame-relay ip tcp header-compression

関連付けられた相手先固定接続（PVC）が常に圧縮形式で発信 TCP/IP ヘッダーを伝送するようにインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **frame-relayiptcpheader-compression** コマンドを使用します。インターフェイスの TCP/IP パケット ヘッダーの圧縮を無効にするには、このコマンドの **no** 形式を使用します。

frame-relay ip tcp header-compression [passive]
no frame-relay ip tcp header-compression

構文の説明

passive	（任意）着信パケットに圧縮されたヘッダーがあった場合のみ、発信 TCP/IP パケット ヘッダーを圧縮します。

コマンド デフォルト

アクティブな TCP/IP ヘッダー圧縮。すべての発信 TCP/IP パケットは、ヘッダー圧縮の対象となります。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
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。

使用上のガイドライン

このコマンドは、フレーム リレーのカプセル化をサポートするインターフェイス（具体的にはシリアル ポートと High-Speed Serial Interface（HSSI））に適用されます。

このコマンドを使用する前に、インターフェイスでフレーム リレーが設定されている必要があります。

TCP/IP ヘッダー圧縮と Internet Engineering Task Force（IETF）カプセル化は、相互に排他的です。インターフェイス を IETF カプセル化に変更すると、すべてのカプセル化および圧縮特性が失われます。

TCP/IP ヘッダー圧縮を有効にするためにこのコマンドを使用すると、すべての IP マップがインターフェイスの圧縮特性を継承します。ただし、ヘッダー圧縮が明示的に拒否された場合、または **frame-relaymapiptcpheadercompression** コマンドを使用して変更された場合を除きます。

カプセル化タイプを変更する前に、インターフェイスをシャットダウンすることをお勧めします。これは必須ではありませんが、インターフェイスをシャットダウンすると、新しいタイプのために確実にインターフェイスをリセットできます。

例

次の例では、シリアル インターフェイス 1 でデフォルトのカプセル化（cisco）とパッシブ TCP ヘッダー圧縮を使用するように設定しています。

```
interface serial 1
 encapsulation frame-relay
 frame-relay ip tcp header-compression passive
```

関連コマンド

Command	Description
frame-relaymapiptcpheader-compression	IP マップが関連付けられているインターフェイスの圧縮特性とは異なる IP マップに対して、ヘッダー圧縮特性を割り当てます。

frame-relay map ip compress

リンクで Real-time Transport Protocol（RTP）と TCP ヘッダー圧縮を有効にするには、インターフェイス コンフィギュレーション モードで **frame-relaymapipcompress** コマンドを使用します。

frame-relay map ip *ip-address dlci* **[broadcast] compress** [{**active**|**passive**}] [**connections** *number*]

構文の説明

ip-address	宛先またはネクスト ホップの IP アドレスです。
dlci	データリンク接続識別子（DLCI）番号です。
broadcast	（任意）指定した IP アドレスにブロードキャストを転送します。
active	（任意）すべての発信 RTP および TCP パケットを圧縮します。これがデフォルトです。
passive	（任意）着信パケットに圧縮されたヘッダーがあった場合のみ、発信 RTP および TCP ヘッダーを圧縮します。
connections *number*	（任意）RTP および TCP ヘッダー圧縮接続の最大数を指定します。範囲は 3 ～ 256 です。

コマンド デフォルト

RTP および TCP ヘッダー圧縮は無効になります。

デフォルトのヘッダー圧縮接続の最大数は、256 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	変更箇所
11.3	このコマンドが導入されました。
12.1(2)T	このコマンドが、ヘッダー圧縮接続の最大数の設定を有効にするように変更されました。
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。

使用上のガイドライン

このコマンドには「no」形式はありません。つまり、**noframe-relaymapipcompress** というコマンドは存在しません。

例

次の例は、シリアルインターフェイス 1 の RTP および TCP ヘッダー圧縮を有効にし、RTP および TCP ヘッダーの接続の最大数を 16 に設定します。

```
interface serial 1
 encapsulation frame-relay
 ip address 10.108.175.110 255.255.255.0
 frame-relay map ip 10.108.175.220 180 compress connections 16
```

関連コマンド

Command	Description
frame-relayiprtpcompression-connections	フレーム リレー インターフェイスの RTP ヘッダー圧縮接続の最大数を指定します。
frame-relayiptcpheader-compression	物理インターフェイス上のすべてのフレームリレーマップについて TCP ヘッダー圧縮をイネーブルにします。
frame-relaymapipnocompress	RTP と TCP の両方のヘッダー圧縮をリンクで無効にします。
frame-relaymapiprtpheader-compression	物理インターフェイス上のすべてのフレームリレーマップについて RTP ヘッダー圧縮をイネーブルにします。
showframe-relayiprtpheader-compression	フレーム リレーの RTP ヘッダー圧縮の統計情報を表示します。
showframe-relayiptcpheader-compression	インターフェイスの統計および TCP/IP ヘッダー圧縮情報を表示します。

frame-relay map ip nocompress

リンクで Real-time Transport Protocol（RTP）と TCP ヘッダー圧縮を無効にするには、インターフェイス コンフィギュレーション モードで **frame-relaymapipnocompress** コマンドを使用します。

frame-relay map ip *ip-address dlci* **[broadcast] nocompress**

構文の説明

ip-address	宛先またはネクスト ホップの IP アドレスです。
dlci	データリンク接続識別子（DLCI）番号です。
broadcast	（任意）指定した IP アドレスにブロードキャストを転送します。

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

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	変更箇所
11.3	このコマンドが導入されました。
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。

使用上のガイドライン

このコマンドには「no」形式はありません。つまり、**noframe-relaymapipnocompress** というコマンドは存在しません。

例

次の例は、DLCI 180 で RTP および TCP ヘッダー圧縮を無効にします。

```
interface serial 1
 encapsulation frame-relay
 frame-relay map ip 10.108.175.220 180 nocompress
```

関連コマンド

Command	Description
frame-relayiprtpheader-compression	物理インターフェイス上のすべてのフレームリレーマップについて RTP ヘッダー圧縮をイネーブルにします。

Command	Description
frame-relayiptcpheader-compression	物理インターフェイス上のすべてのフレームリレーマップについてTCPヘッダー圧縮をイネーブルにします。
frame-relaymapipcompress	リンクでRTPとTCPの両方のヘッダー圧縮を有効にします。
showframe-relayiprtpheader-compression	フレームリレーのRTPヘッダー圧縮の統計情報を表示します。
showframe-relayiptcpheader-compression	インターフェイスの統計およびTCP/IPヘッダー圧縮情報を表示します。

frame-relay map ip rtp header-compression

データリンク接続識別子（DLCI）ごとの Real-time Transport Protocol（RTP）ヘッダーを有効にするには、インターフェイス コンフィギュレーション モードで **frame-relaymapiprtpheader-compression** コマンドを使用します。DLCI ごとの RTP ヘッダー圧縮を無効にし、DLCI を削除するには、このコマンドの **no** 形式を使用します。

frame-relay map ip *ip-address dlci* **[broadcast] rtp header-compression** [{**active**|**passive**}] **[periodic-refresh]** [**connections** *number*]
no frame-relay map ip *ip-address dlci* **[broadcast] rtp header-compression** [{**active**|**passive**}] **[periodic-refresh]** [**connections** *number*]

構文の説明

ip-address	宛先またはネクスト ホップの IP アドレスです。
dlci	DLCI 番号です。
broadcast	（任意）指定した IP アドレスにブロードキャストを転送します。
active	（任意）発信 RTP パケットを圧縮します。
passive	（任意）着信パケットに圧縮されたヘッダーがあった場合のみ、発信 RTP/User Datagram Protocol（UDP）/IP ヘッダーを圧縮します。
periodic-refresh	（任意）圧縮された IP ヘッダーを定期的に更新します。
connections *number*	（任意）RTP ヘッダー圧縮接続の最大数を指定します。範囲は 3 ～ 256 です。

コマンド デフォルト

ディセーブル。

デフォルトでは、インターフェイスにどのようなタイプのヘッダー圧縮が設定されていても、継承されます。インターフェイスにヘッダー圧縮が設定されていない場合、**active** キーワードを使用しますが、**showrunning-config** コマンドの出力には、**header-compression** キーワードは表示されません。

デフォルトのヘッダー圧縮接続の最大数は、256 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	変更箇所
11.3	このコマンドが導入されました。
12.1(2)T	このコマンドは、Cisco IOS Release 12.1(2)T に統合されました。このコマンドが、ヘッダー圧縮接続の最大数の設定を有効にするように変更されました。
12.3(2)T	**periodic-refresh** キーワードが含まれるように、このコマンドが変更されました。

リリース	変更箇所
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
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。

使用上のガイドライン

このコマンドを設定すると、指定したマップがRTPヘッダー圧縮を継承します。RTPヘッダー圧縮あり、またはRTP ヘッダー圧縮なしの複数のフレーム リレー マップを持つことができます。RTPヘッダー圧縮接続の数を指定しない場合、マップはインターフェイスから現在の値を継承します。

例

次の例で、Serial1/2.1 サブインターフェイスでRTPヘッダー圧縮を有効にし、RTPヘッダー圧縮接続の最大数を 64 にする方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/2.1
Router(config-if)# encapsulation frame-relay
Router(config-if)# ip address 10.108.175.110 255.255.255.0
Router(config-if)# frame-relay map ip 10.108.175.220 180 rtp header-compression connections
 64
Router(config-if)# end
```

次の例は、Serial1/1.0 サブインターフェイスで RTP ヘッダー圧縮を有効にし、設定の中でオプションの **periodic-refresh** キーワードを使用する方法を示しています。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/1.0
Router(config-if)# encapsulation frame-relay
Router(config-if)# ip address 10.108.175.110 255.255.255.0
Router(config-if)# frame-relay map ip 10.108.175.220 180 rtp header-compression
periodic-refresh
Router(config-if)# end
```

関連コマンド

Command	Description
frame-relayiprtpcompression-connections	フレーム リレー インターフェイスの RTP ヘッダー圧縮接続の最大数を指定します。
frame-relayiprtpheader-compression	物理インターフェイス上のすべてのフレームリレーマップについてRTPヘッダー圧縮をイネーブルにします。
frame-relaymapipcompress	RTP と TCP の両方のヘッダー圧縮をリンクで有効にします。

Command	Description
showframe-relayiprtpheader-compression	フレーム リレーの RTP ヘッダー圧縮の統計情報を表示します。

group（サービス グループ）

サービス グループにメンバーを追加するには、イーサネット サービス コンフィギュレーション モードで **group** コマンドを使用します。サービス 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。

group *service-group-identifier*
no group *service-group-identifier*

構文の説明

service-group-identifier	メンバーが追加または削除される既存のサービス グループの数です。

コマンド デフォルト

メンバーは追加されません。

コマンド モード

イーサネット サービス コンフィギュレーション（config-if-srv）

コマンド履歴

リリース	変更箇所
12.2(33)SRE	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 グループにメンバー（サービス インスタンスなど）を追加する、およびサービス グループからメンバーを削除するには、**group**（サービス グループ）コマンドを使用します。

Cisco 7600 シリーズ ルータおよび複数のインターフェイスからのサービス インスタンスは許可されない

Cisco 7600 シリーズ ルータは、複数のインターフェイスから同じグループに参加するサービス インスタンスを許可しません。Cisco 7600 シリーズ ルータでは、グループのメンバーは、以下の設定例で示すように同じインターフェイスからのものでなくてはなりません。

```
interface GigabitEthernet 2/0/0
service instance 1 ethernet
 group 32
 service-policy output policy3
service instance 2 ethernet
 group 32
   service instance 3 ethernet
 group 37
interface GigabitEthernet 2/0/1
 service instance 1 ethernet
  group 32 |<--Disallowed because this group has members in g2/0/0 already| |
```

例

次の例では、サービス インスタンス 200 をサービス グループ 20 に追加する方法を示しています。

```
Router> enable
Router# configure terminal
Router# interface GigabitEthernet 1/0/0
```

```
Router(config-if)# service instance 200 ethernet
Router(config-if-srv)# group 20
Router(config-if-srv)# end
```

hw-module slot（ESP スケジューリング）

Embedded Service Processor の入力側のパケットのオーバーサブスクリプションを処理するには、SIP（シリアルインターフェイスプロセッサ）の低プライオリティパケット間で分割される超過帯域幅に基づき、SIP に対して最小帯域幅または特定の重みのいずれかを提供します。グローバル コンフィギュレーション モードで **hw-moduleslot** コマンドを実行します。SIP（シリアルインターフェイスプロセッサ）に割り当てる最小帯域幅を削除するか、SIPに設定された過剰な重みを削除するには、このコマンドの **no** 形式を使用します。

hw-module slot *slot-number* **qos input link** {**A**|**B**} [**bandwidth** *bandwidth_value*] [**weight** *weightage_value*]

構文の説明

slot-number	最小帯域幅または過剰な重みを設定する SIP（シリアル インターフェイス プロセッサ）のスロット番号です。
qos	Quality of Service（QoS）ポリシーの設定を有効にして、入力側でオーバーサブスクリプションの問題を解決します。
input	入力側でパケットのスケジューリングを有効にします。
link	SIP（シリアル インターフェイス プロセッサ）と ESP 間の各 ESI リンクの設定を有効にします。
A	A 入力 QoS リンク を指定してパラメータを設定します。
B	B 入力 QoS リンク を指定してパラメータを設定します。
bandwidth	指定した SIP（シリアル インターフェイス プロセッサ）に対する最小の認定帯域幅の設定をプロビジョニングします。
bandwidth_value	SIP（シリアル インターフェイス プロセッサ）に割り当てられる Kbps の最小帯域幅値です。
weight	共有可能な過剰な重みを SIP（シリアル インターフェイス プロセッサ）に割り当てます。SIPに割り当てられる過剰な重みに基づいて、高プライオリティパケットの処理後に利用できる残された帯域幅は、低プライオリティ パケットの SIP 間で分割されます。
weightage_value	SPA 間で空いている帯域幅を分割するため、SIP（シリアル インターフェイス プロセッサ）に割り当てられる重みの値です。重みの値の有効範囲は 5 ～ 100 です。

コマンド デフォルト

デフォルトでは、高プライオリティ パケットが最初に処理されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
Cisco IOS Release XE 2.1	このコマンドが、**hw-moduleslot**（QoS）コマンドとして導入されました。
Cisco IOS リリース XE 3.1S	コマンドが変更されました。コマンドが **hw-moduleslot**（ESP スケジューリング）コマンドに変更され、**link** キーワードが追加されました。
Cisco IOS Release XE 3.1.0	このコマンドが変更されました。QoS 入力リンクのパラメータの設定用に特定のベイの情報を提供するため、**linkA** または **linkB** キーワード シーケンスが追加されました。

使用上のガイドライン

オーバーサブスクリプションは、SIP（シリアル インターフェイス プロセッサ）レベルと ESP レベルで発生します。ESP レベルでオーバーサブスクリプションの問題を処理するには、**hw-module** スロット コマンドを使用します。ESI リンクを介して接続されている SIP に最小帯域幅が割り当てられます。また、重みが SIP に割り当てられ、利用可能な超過帯域幅を低プライオリティ パケット間で分割します。SIP の最小帯域幅サービスを設定するには、**hw-moduleslot***slot-number***qosinputlink***link-index***bandwidth***value_in_kbps* コマンドを実行します。

SIP と ESP を接続する ESI リンクに特定の重み値を割り当てるには、**hw-moduleslot***slot-number***qosinputlink***link-index***weight**weight-value* コマンドを実行します。

例

次の例は、最小帯域幅を ESI リンク A に割り当てる方法を示しています。

```
Router# config
Router(config)# hw-module slot 1 qos input link A bandwidth 512
```

次の例は、過剰な重み 150 をスロット 1 の SIP（シリアル インターフェイス プロセッサ）に割り当て、ESI リンク A を介して接続する方法を示しています。

```
Router# config
Router(config)# hw-module slot 1 qos input link A weight 150
```

次の例は、2 つのリンクが設定されている場合に、ESP40 および SIP40 カードの利用可能なリンク オプションを表示する方法を示しています。

```
Router(config)# hw-module slot 0 qos input link ?
 A  ESI Link A (Bay 0,2)
 B  ESI Link B (Bay 1,3)
```

次の例は、1 つのリンクが設定されている場合に、ESP40 および SIP10 カードの利用可能なリンク オプションを表示する方法を示しています。

```
Router(config)# hw-module slot 1 qos input link ?
 A  ESI Link A (All Bays)
```

関連コマンド

Command	Description
showplatformhardwareslot{f0|f1}serdesqos	ESP のための過剰な重みと認定帯域幅を表示します。

hw-module subslot（チャネライズド SPA スケジューリング）

チャネライズドSPAに対するSIP（シリアルインターフェイスプロセッサ）の入力側でパケットのオーバーサブスクリプションを処理するには、グローバル コンフィギュレーション モードで **hw-modulesubslot** コマンドを使用して、全体のチャネライズド SPA に過剰な重みを割り当てます。SIPに対して設定された過剰な重みを削除するには、このコマンドの **no** 形式を使用します。

hw-module subslot *slot/subslot* **qos** [**weight** *weightage_value*]
no hw-module subslot *slot/subslot* **qos** [**weight** *weightage_value*]

構文の説明

slot-subslot	過剰な重みを設定する必要がある SIP（シリアル インターフェイス プロセッサ）のスロット番号とチャネライズド SPA のサブスロット番号です。
qos	チャネライズド SPA 上の低プライオリティ パケットに対する過剰な重みの設定を有効にし、入力側のオーバーサブスクリプションの問題を解決します。
weight	チャネライズド SPA に過剰な重みを割り当てます。チャネライズド SPA に割り当てられる過剰な重みに基づいて、高プライオリティ パケットの処理後に利用できる残された帯域幅は、SPA 間で分割されます。
weightage_value	チャネライズド SPA 間の超過帯域幅を分割するため、チャネライズド SPA に割り当てられる重みの値です。重みの値の有効範囲は 5 ～ 100 です。

コマンド デフォルト

デフォルトでは、高プライオリティ パケットが最初に処理されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
3.1S	チャネライズドSPA の利用可能な帯域幅の分散時に重みを割り当てるため、このコマンドが導入されました。

使用上のガイドライン

SIP（シリアル インターフェイス プロセッサ）には、各スロットに異なるタイプの SPA が含まれます。低プライオリティ パケットのためにチャネライズド SPA に過剰な重みを割り当てるため、**hw-modulesubslot***slot-subslot***qosweight***weight-value* コマンドが導入されました。

（注） ポートレベル（インターフェイス レベル）で「絶対優先」キューの最小帯域幅を設定するためのこのオプションは、現在の操作モードに適用できないため廃止されました。既存の設定は、エラーが発生して拒否されます。

例

次の例では、スロット 1 およびサブスロット 0 にあるチャネライズド SPA に対して、過剰な重み 200 を割り当てる方法を示しています。

```
Router# config
Router(config)# hw-module subslot 1/0 qos weight 200
```

関連コマンド

Command	Description
showplatformhardware{slot *slotno* **|subslot** *slot/subslot* **}plimqosinputbandwidth**	SIP（シリアル インターフェイス プロセッサ）または SPA に設定された過剰な重みと認定帯域幅の設定をそれぞれ表示します。

identity policy（ポリシーマップ）から ip rsvp pq-profile

- identity policy（policy-map） （201 ページ）
- ingress-class-map （203 ページ）
- ip header-compression disable-feedback （205 ページ）
- ip header-compression max-header （207 ページ）
- ip header-compression max-period （209 ページ）
- ip header-compression max-time （211 ページ）
- ip header-compression recoverable-loss （213 ページ）
- ip header-compression old-iphc-comp （215 ページ）
- ip header-compression old-iphc-decomp （216 ページ）
- ip nbar attribute-map （217 ページ）
- ip nbar attribute-set （219 ページ）
- ip nbar classification auto-learn top-hosts （221 ページ）
- ip nbar classification granularity （222 ページ）
- ip nbar classification tunneled-traffic （224 ページ）
- ip nbar custom （225 ページ）
- ip nbar custom transport （230 ページ）
- ip nbar pdlm （233 ページ）
- ip nbar port-map （235 ページ）
- ip nbar protocol-discovery （237 ページ）
- ip nbar protocol-pack （239 ページ）
- ip nbar resources （241 ページ）
- ip nbar resources protocol （242 ページ）
- ip nbar resources system （244 ページ）
- ip options （246 ページ）
- ip rsvp admission-control compression predict （248 ページ）
- ip rsvp aggregation ip （250 ページ）
- ip rsvp aggregation ip map （252 ページ）
- ip rsvp aggregation ip reservation dscp （254 ページ）

- ip rsvp aggregation ip role interior （256 ページ）
- ip rsvp atm-peak-rate-limit （258 ページ）
- ip rsvp authentication （260 ページ）
- ip rsvp authentication challenge （262 ページ）
- ip rsvp authentication key （264 ページ）
- ip rsvp authentication key-chain （266 ページ）
- ip rsvp authentication lifetime （268 ページ）
- ip rsvp authentication neighbor （270 ページ）
- ip rsvp authentication type （274 ページ）
- ip rsvp authentication window-size （277 ページ）
- ip rsvp bandwidth （279 ページ）
- ip rsvp bandwidth ignore （283 ページ）
- ip rsvp bandwidth percent （284 ページ）
- ip rsvp burst policing （287 ページ）
- ip rsvp data-packet classification none （288 ページ）
- ip rsvp dsbm candidate （290 ページ）
- ip rsvp dsbm non-resv-send-limit （292 ページ）
- ip rsvp flow-assist （294 ページ）
- ip rsvp layer2 overhead （296 ページ）
- ip rsvp listener （300 ページ）
- ip rsvp listener outbound （303 ページ）
- ip rsvp msg-pacing （306 ページ）
- ip rsvp neighbor （308 ページ）
- ip rsvp policy cops minimal （310 ページ）
- ip rsvp policy cops report-all （311 ページ）
- ip rsvp policy cops servers （313 ページ）
- ip rsvp policy cops timeout （315 ページ）
- ip rsvp policy default-reject （316 ページ）
- ip rsvp policy identity （318 ページ）
- ip rsvp policy local （321 ページ）
- ip rsvp policy preempt （331 ページ）
- ip rsvp policy vrf （332 ページ）
- ip rsvp pq-profile （334 ページ）

identity policy（policy-map）

アイデンティティ ポリシーを作成するには、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、**identitypolicy** 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。

identity policy *policy-name*
no identity policy *policy-name*

構文の説明

policy-name	ポリシーの名前。

コマンド デフォルト

アイデンティティ ポリシーは作成されません。

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（config-pmap-class）

コマンド履歴

リリース	変更箇所
12.4(6)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

このコマンドは、適用するアクセスポリシーを含んだデバイス上に設定されているグローバル アイデンティティ ポリシーを参照します。ポリシー クラス コンフィギュレーション サブモードでは、単一のアイデンティティ ポリシーのみを設定できます。アイデンティティ ポリシーをデバイスに定義しなかった場合、ポリシーの適用時にエラーが生成されます。

例

次の例は、healthy_identity というアイデンティティ ポリシーを作成する方法を示しています。

```
Router(config)# policy-map type control tag healthy_pmap
Router(config-pmap)# class healthy_class
Router(config-pmap-class)# identity policy healthy_identity
Router(config-pmap-class)# end
```

次に、healthy_acl というアクセス グループを healthy_identity というアイデンティティ ポリシーに追加する例を示します。

```
Router(config)# identity policy healthy_identity
Router(config-identity-policy)# access-group healthy_acl
Router(config-identity-policy)# end
```

関連コマンド

コマンド	説明
classtypetag	クラス マップをポリシー マップに関連付けます。

コマンド	説明
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

ingress-class-map

IPv4、IPv6、および MPLS パケットを POS、チャネライズド、およびクリアチャネル SPA のために分類するには、まずグローバル コンフィギュレーション モードで **ingress-class-map** コマンドを使用し、入力分類テンプレートを定義します。入力分類テンプレートは、後からインターフェイスに適用されるインデックス ID で識別されます。テンプレートを削除するには、このコマンドの **no** 形式を入力します。

ingress-class-map *class-map index*
no ingress-class-map

構文の説明

class-map index	IPv4、IPv6、および MPLS 分類の組み合わせの入力分類テンプレートを識別するためのクラスマップインデックス ID。キャリア カード（CC）あたりのインデックス クラス マップの最大数の有効な範囲は、1 ～ 62 をキャリア カード スロットの最大数で掛けたものです。

コマンド デフォルト

入力クラス マップのインデックス ID 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（config）

コマンド履歴

リリース	変更箇所
Cisco IOS XE Release 3.1S	このコマンドが導入されました。

使用上のガイドライン

SIP（シリアル インターフェイス プロセッサ）または SPA で IPv4、IPv6、または MPLS などの高プライオリティ パケットを分類するには、**ingress-classmap***class-mapindex* コマンドを使用して分類テンプレートを定義します。分類テンプレート固有の詳細はテンプレートで定義されています。また、テンプレートは、**plimqosinputclass-map** コマンドを使用してインターフェイスにアタッチされます。分類テンプレートは、**no** コマンド形式を使用して削除できます各 SIP では、62 の入力分類テンプレートがサポートされています。Cisco ASR 1000 シリーズ ルータに適用できる入力分類テンプレートの合計数は、キャリア カードに 62 を掛けた数値に等しくなります。

（注） 分類テンプレートがインターフェイスによって使用されている場合、そのテンプレートを削除することはできません。

例

次の例は、**ingress-class-map** コマンドを使用して分類テンプレートを定義する方法を示しています。

```
Router# config
```

```
Router(config)# ingress-class-map 1
Router(config-ing-class-map)#
```

関連コマンド

Command	Description
plimqosinputclass-map	分類テンプレートをインターフェイスにアタッチします。

ip header-compression disable-feedback

インターフェイスまたはリンクからのコンテキスト ステータスのフィードバック メッセージを無効にするには、インターフェイス コンフィギュレーション モードで **ipheader-compressiondisable-feedback** コマンドを使用します。インターフェイスまたはリンクからのコンテキスト ステータスのフィードバック メッセージを有効にするには、このコマンドの **no** 形式を使用します。

ip header-compression disable-feedback
no ip header-compression disable-feedback

構文の説明

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

コンテキスト ステータスのフィードバック メッセージは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	変更箇所
12.3(2)T	このコマンドが導入されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。

使用上のガイドライン

ipheader-compressiondisable-feedback コマンドは、衛星リンクで使用するよう設計されています。衛星リンクでは、上方リンクへのパスは下方リンクへのパスと異なります。パスが異なる場合は、コンテキスト ステータス メッセージを活用できません。

ipheader-compressiondisable-feedback コマンドは、Real-time Transport Protocol（RTP）または TCP ヘッダー圧縮のいずれかとともに使用できます。

例

次の例では、シリアル インターフェイス 2/0 でコンテキスト ステータス メッセージを無効にしています。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
Router(config-if)# ip header-compression disable-feedback
Router(config-if)# end
```

関連コマンド

コマンド	説明
ipheader-compressionmax-header	圧縮された IP ヘッダーの最大サイズを指定します。

コマンド	説明
ipheader-compressionmax-period	フル ヘッダー間の圧縮されたパケットの最大数を指定します。
ipheader-compressionmax-time	圧縮された IP ヘッダーを更新する前に待機する最大時間を指定します。

ip header-compression max-header

圧縮された IP ヘッダーを更新する前に待機する最大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 **ipheader-compressionmax-header** コマンドを使用します。圧縮された IP ヘッダーを更新する前に待機する時間数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。

ip header-compression max-header *max-header-size*
no ip header-compression max-header *max-header-size*

構文の説明

max-header-size	IP ヘッダーのサイズ（バイト単位）。IP ヘッダーのサイズの範囲は 20 ～ 168 です。

コマンド デフォルト

168 バイト

コマンド 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	変更箇所
12.3(2)T	このコマンドが導入されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。

使用上のガイドライン

ipheader-compressionmax-header コマンドの *max-header-size* 引数は、圧縮するヘッダーのサイズを制限するために使用できます。

例

次の例では、**ipheader-compressionmax-header** コマンドを使用して、パケットの最大 IP ヘッダー サイズを 100 バイトに指定しています。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
Router(config-if)# ip header-compression max-header 100
Router(config-if)# end
```

関連コマンド

コマンド	説明
ipheader-compressiondisable-feedback	インターフェイスまたはリンクからのコンテキスト ステータスのフィードバック メッセージを無効にします。
ipheader-compressionmax-period	フル ヘッダー間の圧縮されたパケットの最大数を指定します。

コマンド	説明
ipheader-compressionmax-time	圧縮された IP ヘッダーを更新する前に待機する最大時間を指定します。

ip header-compression max-period

フルヘッダー間の圧縮パケットの最大数を指定するには、インターフェイス コンフィギュレーション モードで **ipheader-compressionmax-period** コマンドを使用します。圧縮パケットの数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。

ip header-compression max-period *number-of-packets*
no ip header-compression max-period *number-of-packets*

構文の説明

number-of-packets	フル ヘッダー間のパケットの数を指定します。指定できる値の範囲は 0 ～ 65535 です。

コマンド デフォルト

256 パケット

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.3(2)T	このコマンドが導入されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。

使用上のガイドライン

ipheader-compressionmax-period コマンドを使用すると、コンテキスト ステータスが変化した後、フル IP パケット ヘッダーが送信される期間が急激に長くなります。この急激な期間の増加により、ヘッダーの圧縮メカニズムとヘッダーの圧縮解除メカニズムとの間でメッセージ交換が必要になることを回避できます。

デフォルトでは、**ipheader-compressionmax-period** コマンドは User Datagram Protocol（UDP）トラフィックのみで動作します。ただし、**frame-relayiprtpheader-compression** コマンドまたは **frame-relaymapiprtpheader-compression** コマンドのいずれかで **periodicrefresh** キーワードが設定されている場合、**ipheader-compressionmax-period** コマンドは UDP トラフィックと Real-time Transport Protocol（RTP）トラフィックの両方で動作します。

例

次の例では、**ipheader-compressionmax-period** コマンドを設定し、フルヘッダー パケット間のパケット数を指定しています。この設定で、指定されているパケット数は 160 です。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
Router(config-if)# ip header-compression max-period 160
Router(config-if)# end
```

関連コマンド

コマンド	説明
frame-relayiprtpheader-compression	物理インターフェイス上のすべてのフレームリレーマップについて RTP ヘッダー圧縮をイネーブルにします。
frame-relaymapiprtpheader-compression	DLCI ごとに RTP ヘッダー圧縮を有効にします。
ipheader-compressiondisable-feedback	インターフェイスまたはリンクからのコンテキストステータスのフィードバック メッセージを無効にします。
ipheader-compressionmax-header	圧縮された IP ヘッダーの最大サイズを指定します。
ipheader-compressionmax-time	圧縮された IP ヘッダーを更新する前に待機する最大時間を指定します。

ip header-compression max-time

圧縮された IP ヘッダーを更新する前に待機する最大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 **ipheader-compressionmax-time** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ip header-compression max-time *length-of-time*
no ip header-compression max-time *length-of-time*

構文の説明

length-of-time	IP ヘッダーが更新されるまでに待機するための異なる長さの時間（デフォルト以外）を秒単位で指定します。指定できる範囲は 0 ～ 65535 です。

コマンド デフォルト

時間の長さが設定されていない場合、デフォルト値は 5 秒です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.3(2)T	このコマンドが導入されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。

使用上のガイドライン

ipheader-compressionmax-time コマンドは、受信者のコンテキスト ステータスが失われた場合に、多数のパケット損失を回避するように設計されています。

パケットを送信予定で、最後に IP ヘッダーを更新してから最大の時間数が経過した場合、フル ヘッダーが送信されます。

デフォルトでは、**ipheader-compressionmax-time** コマンドは User Datagram Protocol（UDP）トラフィックのみで動作します。ただし、**frame-relayiprtpheader-compression** コマンドまたは **frame-relaymapiprtpheader-compression** コマンドのいずれかで **periodicrefresh** キーワードが設定されている場合、**ipheader-compressionmax-time** コマンドは、UDP トラフィックと Real-time Transport Protocol（RTP）トラフィックの両方で動作します。

例

次の例では、圧縮された IP ヘッダーが更新されるまでに待機する時間の最大数を指定するために、**ipheader-compressionmax-time** コマンドが設定されています。この設定では、待機する時間の長さは 30 秒です。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
Router(config-if)# ip header-compression max-time 30
Router(config-if)# end
```

関連コマンド

コマンド	説明
frame-relayiprtpheader-compression	物理インターフェイス上のすべてのフレームリレーマップについて RTP ヘッダー圧縮をイネーブルにします。
frame-relaymapiprtpheader-compression	DLCI ごとに RTP ヘッダー圧縮を有効にします。
ipheader-compressiondisable-feedback	インターフェイスまたはリンクからのコンテキストステータスのフィードバック メッセージを無効にします。
ipheader-compressionmax-header	圧縮された IP ヘッダーの最大サイズを指定します。
ipheader-compressionmax-period	フル ヘッダー間の圧縮されたパケットの最大数を指定します。

ip header-compression recoverable-loss

インターフェイスで Enhanced Compressed Real-Time Transport Protocol（ECRTP）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 **ipheader-compressionrecoverable-loss** コマンドを使用します。インターフェイスで ECRTP 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 header-compression recoverable-loss {**dynamic***packet-drops*}
no ip header-compression recoverable-loss

構文の説明

dynamic	動的な回復可能な損失の計算です。
packet-drops	連続するパケット破棄の最大数です。範囲は 1 ～ 8 です。

コマンド デフォルト

dynamic キーワードを使用する場合、デフォルト値は 4 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	変更箇所
12.3(11)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

Enhanced CRTP は、コンプレッサがデコンプレッサでのコンテキストを更新する方法を変更することによって、破損を減らします。コンプレッサは、変更を複数回送信し、コンプレッサとデコンプレッサの同期を維持します。この方式は、ホスト間のリンク品質を表す *packet-drops* の数によって特徴付けられます。更新を繰り返すことで、パケット損失によるコンテキスト破損の確率が最小化されます。

packet-drops 引数の値は各コンテキストに依存せずに維持され、すべてのコンテキストで同一である必要はありません。

例

次の例は、Point-to-Point Protocol（PPP）カプセル化をシリアル インターフェイスに設定し、動的な損失回復を備えた ECRTP を有効にする方法を示しています。

```
Router(config)# interface serial 2/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression ietf-format
Router(config-if)# ip header-compression recoverable-loss dynamic
Router(config-if)# end
```

関連コマンド

コマンド	説明
debugiprtperror	RTP ヘッダー圧縮のエラーを表示します。

コマンド	説明
debugiprtpheader-compression	RTPヘッダー圧縮に固有のイベントを表示します。
iprtpheader-compression	RTP ヘッダー圧縮をイネーブルにします。
showiprtpheader-compression	RTP ヘッダー圧縮の統計情報を表示します。

ip header-compression old-iphc-comp

IP ヘッダー圧縮（IPHC）形式の圧縮を RFC 非準拠形式に戻すには、インターフェイス コンフィギュレーション モードで **ipheader-compressionold-iphc-comp** コマンドを使用します。IPHC 形式の圧縮を無効にするには、このコマンドの **no** 形式を使用します。

ip header-compression old-iphc-comp
no ip header-compression old-iphc-comp

構文の説明

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

IPHC 形式の圧縮は設定されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
15.1(3)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

ipheader-compressionold-iphc-comp コマンドは、IPHC 形式の圧縮またはサービス ポリシーベースの圧縮が設定されている場合にのみ設定する必要があります。

例

次の例は、IPHC 形式の圧縮を RFC 非準拠形式に戻す方法を示しています。

```
Router> enable

Router# configure terminal
Router(config)# interface serial 0/0
Router(config-if)# ip header-compression old-iphc-comp
```

関連コマンド

コマンド	説明
ipheader-compressionold-iphc-decomp	IPHC 形式の圧縮解除を RFC 非準拠形式に戻します。

ip header-compression old-iphc-decomp

IP ヘッダー圧縮（IPHC）形式の圧縮解除を RFC 非準拠形式に戻すには、インターフェイス コンフィギュレーション モードで **ipheader-compressionold-iphc-decomp** コマンドを使用します。IPHC 形式の圧縮解除の通常の形式を維持するには、このコマンドの **no** 形式を使用します。

ip header-compression old-iphc-decomp
no ip header-compression old-iphc-decomp

構文の説明

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

IPHC 形式の圧縮解除は設定されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
15.1(3)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

ipheader-compressionold-iphc-decomp コマンドは、IPHC 形式の圧縮またはサービス ポリシーベースの圧縮が設定されている場合にのみ設定する必要があります。

例

次の例は、IPHC 形式の圧縮解除を RFC 非準拠形式に戻す方法を示しています。

```
Router> enable

Router# configure terminal
Router(config)# interface serial 0/0
Router(config-if)# ip header-compression old-iphc-decomp
```

関連コマンド

コマンド	説明
ipheader-compressionold-iphc-comp	IPHC形式の圧縮をRFC非準拠形式に戻します。

ip nbar attribute-map

Network-Based Application Recognition（NBAR）属性プロファイルを作成するには、グローバル コンフィギュレーション モードで **ip nbar attribute-map** コマンドを使用します。NBAR 属性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 nbar attribute-map *profile-name*

no ip nbar attribute-map *profile-name*

構文の説明

profile-name	プロトコルの属性プロファイルの名前です。

コマンド デフォルト

新しい属性プロファイルは作成されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
15.2(4)M2	このコマンドが導入されました。
Cisco IOS XE Release 3.8S	このコマンドが、Cisco IOS XE リリース 3.8S に統合されました。

使用上のガイドライン

NBAR では、カスタム プロトコルを使用してカスタム アプリケーションを識別できます。カスタム プロトコルは、NBAR でサポートされないスタティック ポートベースのプロトコルとアプリケーションをサポートします。

NBAR を使用すると、プロトコルの属性プロファイルを設定し、プロファイルをプロトコルにアタッチできます。

ip nbar attribute-map コマンドを使用すると、NBAR 属性プロファイルを作成できます。このコマンドを使用すると、さまざまな属性をカスタムプロトコルに割り当てることができる属性マップ サブモードが開始されます。この属性プロファイルは、**ipnbarattribute-set** *protocol-name profile-name* コマンドを使用して、プロトコルにアタッチできます。

例

次に、Network News Transfer Protocol（NNTP）用に属性プロファイルを作成する例を示します。

```
Device# configure terminal
Device(config)# ip nbar attribute-map nntp-attrib
```

関連コマンド

コマンド	説明
attribute	属性を属性プロファイルに追加します。

コマンド	説明
ipnbarattribute-set	プロトコルに新しい属性プロファイルをアタッチします。

ip nbar attribute-set

特定のプロトコルに属性プロファイルを割り当てるには、グローバル コンフィギュレーション モードで **ip nbar attribute-set** コマンドを使用します。プロトコルに対する属性プロファイルのマッピングを削除するには、このコマンドの **no** 形式を使用します。

ip nbar attribute-set *protocol-name profile-name*
no ip nbar attribute-set *protocol-name profile-name*

構文の説明

protocol-name	属性プロファイルを割り当てるプロトコルです。
profile-name	属性プロファイルの名前です。

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	変更箇所
15.2(4)M2	このコマンドが導入されました。
Cisco IOS XE Release 3.8S	このコマンドが、Cisco IOS XE リリース 3.8S に統合されました。

使用上のガイドライン

Network-Based Application Recognition（NBAR）は、カスタム プロトコルを使用したカスタム アプリケーションの識別をサポートします。カスタム プロトコルは、NBAR でサポートされないスタティック ポートベースのプロトコルとアプリケーションをサポートします。

NBAR を使用すると、プロトコルの属性プロファイルを設定し、プロファイルをプロトコルにアタッチできます。

ip nbar attribute-set コマンドを使用し、属性プロファイルをプロトコルにアタッチできます。プロファイルをプロトコルにアタッチした後は、パラメータを追加または削除することでプロファイルを編集できます。アタッチされた属性プロファイルを、プロトコルから削除することもできます。

（注） 属性マップが定義されない場合、コマンド出力には「Unrecognized command」と表示されます。これは、コマンドを個別に実行した場合、コマンドラインに表示されること、またはバッチ コマンドの実行に対する出力ログ ファイルに表示されることがあります。

例

次に、属性プロファイルをアプリケーション通信プロトコル（ACP）にマップする例を示します。

```
Device# configure terminal
Device(config)# ip nbar attribute-set acp test-profile
```

関連コマンド

コマンド	説明
ipnbarattribute-map	属性プロファイルを作成します。

ip nbar classification auto-learn top-hosts

ジェネリックとして分類されたネットワーク トラフィックの上位ホストを示す Network Based Application Recognition（NBAR）の機能を有効にするには、**ip nbar classification auto-learn top-hosts** 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。

ip nbar custom auto-learn top-hosts sample-rate *sample-rate-number*

no ip nbar custom auto-learn top-hosts sample-rate *sample-rate-number*

構文の説明

sample-rate *sample-rate-number*	上位ホストを自動学習するサンプル レートを設定します。

コマンド デフォルト

ジェネリックとして分類されたネットワーク トラフィックの上位ホストを示す NBAR の機能を有効にします。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
15.5(2)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

ホスト名に基づくカスタム アプリケーションを作成するために、情報が使用されます。

例

次に、ジェネリックとして分類されたネットワーク トラフィックの上位ホストの名前を示す NBAR の機能を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip nbar classification auto-learn top-hosts
```

関連コマンド

コマンド	説明
clearipnbarclassificationauto-learntop-hosts	ジェネリックとして分類されたネットワーク トラフィックの上位ホストの統計情報およびデータベースの表示をクリアします。
showipnbarclassificationauto-learntop-hosts	ジェネリックとして分類されたネットワーク トラフィックの上位ホストの統計およびデータベースを表示します。

ip nbar classification granularity

Network Based Application Recognition（NBAR）のために分類モードを設定するには、細粒の場合も粗粒の場合も、グローバル コンフィギュレーション モードで **ipnbarclassificationgranularity** コマンドを使用します。粗粒分類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。

ip nbar classification granularity{**coarse-grain**|**fine-grain** ［**protocol** *protocol-name*］}
no ip nbar classification granularity{**coarse-grain**|**fine-grain** ［**protocol** *protocol-name*］}

構文の説明

coarse-grain	粗粒分類を指定します。
fine-grain	細粒分類を指定します。
protocol *protocol-name*	アプリケーションを示す指定されたプロトコルに対して、細粒分類を強制します。

コマンド デフォルト

NBAR のデフォルトの分類モードは細粒です。

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	変更箇所
Cisco IOS XE リリース 3.14S	このコマンドが導入されました。
15.5(1)T	このコマンドが Cisco IOS Release 15.5(1)T に統合されました。
15.5(2)T	このコマンドが、キーワードと引数のペア **protocol** *protocol-name* を含むように変更されました。
Cisco IOS XE Release 3.15S	このコマンドが、Cisco IOS XE Release 3.15S に統合されました。

使用上のガイドライン

細粒モードの分類は、細粒モードと粗粒モードが別々に導入される以前の NBAR の機能とパフォーマンスと等価です。細粒モードは、既存の設定に対して完全な後方互換性を提供します。

例

次の例は、NBAR に対して粗粒分類モードを設定しています。

```
Device# ip nbar classification granularity coarse-grain
```

次の例は、NBAR に対して細粒分類モードを設定し、特定のプロトコルを強制しています。

```
Device# Device# ip nbar classification granularity fine-grain protocol 3pc
```

関連コマンド

コマンド	説明
showipnbarclassificationgranularity	現在設定されているNBAR分類モードを表示します。

ip nbar classification tunneled-traffic

Network Based Application Recognition で、IPv4 トンネル（IPv4 および Teredo での IPv6）を介して伝送される IPv6 トラフィックのアプリケーション分類を有効にするには、グローバル コンフィギュレーション モードで **ipnbarclassificationtunneled-traffic** コマンドを使用します。アプリケーション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。

ip nbar classification tunneled-traffic{**ipv6inip**|**teredo**}
no ip nbar classification tunneled-traffic{**ipv6inip**|**teredo**}

構文の説明

ipv6inip	IPv4 トンネリング トラフィックの IPv6 を分類します。
teredo	Teredo トンネリング トラフィックを分類します。

コマンド デフォルト

IPv4 または Teredo トンネル内の IPv6 を介してトンネリングされた IPv6 トラフィックに対するアプリケーション分類は、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	変更箇所
15.2(2)T	このコマンドが導入されました。
Cisco IOS XE リリース 3.5S	このコマンドが、Cisco IOS XE Release 3.5S に統合されました。
15.2(1)S	このコマンドが、Cisco IOS Release 15.2(1)S に統合されました。

使用上のガイドライン

ipv6inip キーワードは、プロトコル 41 を経由し、IPv4 トンネルを介して伝送される IPv6 トラフィックのアプリケーション分類を有効にします。プロトコル 41 には、ISATAP、6to4、6rd などのトンネル タイプが含まれています。

teredo キーワードは、Teredo トンネルを介して伝送される IPv6 トラフィックのアプリケーション分類を有効にします。Teredo トンネルは、UDP 経由のポート 3544 と ポート 3545 という 2 つの共通するデフォルト ポートで識別され、IPv4 トンネル エンドポイントに存在します。

例

次の例は、Teredo トンネルを介して伝送される IPv6 トラフィックのアプリケーション分類を有効にする方法を示しています。

```
Router(config)# ip nbar classification tunneled-traffic teredo
```

ip nbar custom

このコマンドはすでに廃止されています。**ip nbar custom transport** を使用してください。「ip nbar custom transport （230 ページ）」を参照してください。

Network-Based Application Recognition（NBAR）Protocol Discovery 機能を拡張するには、グローバル コンフィギュレーション モードで **ip nbar custom** コマンドを使用します。NBAR が追加のスタティック ポート アプリケーションを分類および監視するのを停止したり、サポートしていないスタティック ポート トラフィックの分類を停止するには、このコマンドの **no** 形式を使用します。

ip nbar custom *custom-name* {[*field-offset* {**ascii** *ascii-value* | **decimal** *decimal-value* | **hex** *hex-value* | **variable** *variable-name*}] [**destination** | **source**] [プロトコル] | **ssl unique-name** *unique-name-string* [**id** *selector-id*] | **dns domain-name** *domain-name-string* [**id** *selector-id*] | **http** {**host** *host-name* [**id** *selector-id*] | **url** *url-name* [**host** *host-name*] [**id** *selector-id*]}}

no ip nbar custom *custom-name*

構文の説明

custom-name	カスタム プロトコルの名前。 名前は、4 文字以上 24 文字以下でなくてはなりません。名前には、小文字の英字（a ～ z）、数字（0 ～ 9）、およびアンダースコア（_）文字を含めることができます。
field-offset	（任意）フィールドに関するペイロード検査のバイト位置を表す数字です。
ascii *ascii-value*	ASCII として検査値の形式を設定し、値の長さを定義します。最大で 16 文字を検索できます。正規表現はサポートされません。
decimal *decimal-value*	10 進数で検査値の形式を設定し、値の長さを定義します。最大 4 バイトがサポートされます。
hex *hex-value*	16 進数で検査値の形式を設定し、値の長さを定義します。最大 4 バイトがサポートされます。
variable *variable-name*	**variable** キーワードを入力すると、カスタム プロトコルの特定部分を NBAR がサポートするプロトコルとして処理できます（たとえば、class-map 統計を使用してカスタム プロトコルの特定部分を追跡し、**class-map** コマンドを使用して照合できます）。*variable-name* 引数は、ペイロードを検索するフィールドの名前を指定します。
destination	（任意）パケットの宛先の方向を指定します。宛先の方向を指定しない場合は、両方向に転送されるすべてのパケットが NBAR によって監視されます。

source	（任意）パケットの送信元の方向を指定します。送信元の方向を指定しない場合は、両方向に転送されるすべてのパケットが NBAR によって監視されます。
プロトコル	（任意）アプリケーションによって実装されるプロトコルが TCP か UDP かを指定し、次の値を定義します。 • *port-number*：カスタム アプリケーション モニタによって監視されるポート。最大 16 個の個別ポートを指定できます。 • **id** *selector-id*：（任意）カスタム プロトコルのアプリケーション ID を指定します。範囲：1 ～ 65535。 • **range** *start-value end-value*：監視するカスタム アプリケーションのポート範囲を指定します。*start-value* 変数は範囲の最初のポートを表し、*end-value* 変数は範囲の最後のポートを表します。カスタム プロトコルごとに最大 1000 ポートの範囲を指定できます。
http	カスタム HTTP 文字列の名前を指定します。
ssl	カスタム SSL 文字列の名前を指定します。
unique-name *unique-name-string*	クライアントの Hello メッセージの SSL サーバ名指定（SNI）フィールドまたは証明書の共通名（CN）フィールドのホスト名を指定します。*unique-name-string* 引数の長さは、30 文字以下である必要があります。
dns	カスタム DNS 文字列の名前を指定します。
domain-name *domain-name-string*	DNS ドメイン名を指定します。完全なドメイン名またはその一部を正規表現で指定できます。*domain-name-string* 引数の長さは、30 文字以下である必要があります。
host *host-name*	HTTP ヘッダー文字列のホスト名を指定します。
url *url-name*	HTTP ヘッダー文字列の URL を指定します。
id *selector-id*	（任意）カスタム プロトコルのアプリケーション ID を指定します。範囲：1 ～ 65535。

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	変更箇所
12.3(4)T	このコマンドが導入されました。
12.3(11)T	**variable** *field-name field-length* キーワードと引数のペアが導入されました。

リリース	変更箇所
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
15.2(4)M2	このコマンドが、Cisco IOS Release 15.2(4)M2 に統合されました。**http** キーワード、**host** *host-name* と **url** *url-name* キーワードと引数のペアが導入されました。
Cisco IOS XE Release 3.8S	このコマンドが、Cisco IOS XE リリース 3.8S に統合されました。
Cisco IOS XE Release 3.15S	このコマンドが変更されました。**ssl** キーワード、**unique-name** *unique-name-string* キーワードと引数のペア、**dns** キーワード、および **domain-name** *domain-name-string* キーワードと引数のペアが導入されました。
Cisco IOS XE Denali 16.2.1	このコマンドはすでに廃止されています。**ip nbar custom transport** を使用してください。「ip nbar custom transport （230 ページ）」を参照してください。

使用上のガイドライン

追加のスタティック ポート アプリケーションを分類および監視するか、NBAR がサポートしていないスタティック ポート トラフィックを分類できるようにするには、グローバル コンフィギュレーション モードで、**ip nbar custom** コマンドを使用します。

カスタム プロトコルの最初の 3 文字は、すべての定義済みプロトコルに対して一意でなければなりません。一意でない場合、あいまいなコマンドであることを示すエラー メッセージが表示されます。

NBAR は、最大 128 のプロトコルをサポートできます。

カスタム プロトコルの設定時に **variable** キーワードを入力すると、一部の NBAR クラス マップの **show** 出力に変数のトラフィック統計情報が表示されます。

protocol 引数は、アプリケーションによって実装されたプロトコルを表します。次に記載されている要素のセットに進む前に、プロトコルを TCP または UDP として指定します。

{*port-number* ［**id** *selector-id*］ | **range** *start-value end-value*}

カスタム プロトコルごとに最大 24 個の変数値をクラス マップで設定できます。たとえば、次の設定では、4 つの変数が使用されます。

```
Device(config)# ip nbar custom ftdd 23 variable scid 1 tcp range 5001 5005
Device(config)# class-map match-any active-craft
Device(config-cmap)# match protocol ftdd scid 0x15
Device(config-cmap)# match protocol ftdd scid 0x21
Device(config-cmap)# exit
Device(config)# class-map match-any passive-craft
Device(config-cmap)# match protocol ftdd scid 0x11
Device(config-cmap)# match protocol ftdd scid 0x22
```

例

次の例は、0 文字以上の文字の後に文字列「whatsnew/latest」が続く任意の URL に基づいて、HTTP パケットを分類する方法を示しています。

```
Device(config)# ip nbar custom my_http http url "*whatsnew/latest"
```

次の例は、「sell」または「dell」の文字列の後に 0 文字以上の文字が続く任意のホスト名に基づいて、パケットを分類する方法を示しています。

```
Device(config)# ip nbar custom my_http http host "*(s|d)ell"
```

次の例は、カスタム プロトコル「app_sales1」を設定し、4567 の発信元ポートを持つ TCP パケット、およびペイロードの第 5 バイトに SALES という用語を含む TCP パケットを識別する方法を示しています。

```
Device(config)# ip nbar custom app_sales1 5 ascii SALES source tcp 4567
```

次の例は、カスタム プロトコル「virus_home」を設定し、3000 の宛先ポートを持ち、ペイロードの第 7 バイトに「0x56」を含む UDP パケットを識別する方法を示しています。

```
Device(config)# ip nbar custom virus_home 7 hex 0x56 destination udp 3000
```

次の例は、カスタム プロトコル「media_new」を設定し、4500 の宛先ポートまたは送信元ポートを持つ TCP パケット、およびペイロードの第 6 バイトの値が 90 の TCP パケットを識別する方法を示しています。

```
Device(config)# ip nbar custom media_new 6 decimal 90 tcp 4500
```

次の例は、カスタム プロトコル msn1 を設定し、6700 の宛先ポートまたは送信元ポートを持つ TCP パケットを検索する方法を示しています。

```
Device(config)# ip nbar custom msn1 tcp 6700
```

次の例は、カスタム プロトコル mail_x を設定し、宛先ポート 8202 を持つ UDP パケットを検索する方法を示しています。

```
Device(config)# ip nbar custom mail_x destination udp 8202
```

次の例は、カスタム プロトコル mail_y を設定し、3000 以上 4000 以下の宛先ポートを持つ UDP パケットを検索する方法を示しています。

```
Device(config)# ip nbar custom mail_y destination udp range 3000 4000
```

次の例は、変数を使用して、カスタム プロトコル ftdd を作成する方法を示しています。変数に基づいて、このカスタムプロトコルを照合するクラスマップも作成されます。この例では、TCP ポート 5001 ～ 5005 で送受信され、バイト 23 に値 804 を持つすべてのトラフィックに対し、クラス マップ matchscidinftdd が一致します。変数 scid の長さは 2 バイトです。

```
Device(config)# ip nbar custom ftdd 23 variable scid 2 tcp range 5001 5005
```

```
Device(config)# class-map matchscidinftdd
Device(config-cmap)# match protocol ftdd scid 804
```

上記の同じ例は、クラス マップに 16 進数の値を使用して次のように行うこともできます。

```
Device(config)# ip nbar custom ftdd 23 variable scid 2 tcp range 5001 5005
Device(config)# class-map matchscidinftdd
Device(config-cmap)# match protocol ftdd scid 0x324
```

次の例は、**variable** キーワードを使用してカスタム プロトコルを作成し、変数フィールドから異なるトラフィック クラスへと異なる値を分類するためのクラス マップを設定する方法を示しています。次の例では、変数 scid 値 0x15、0x21、および 0x27 は、クラス マップ active-craft に分類され、scid 値 0x11、0x22、および 0x25 はクラス マップ passive-craft に分類されます。

```
Device(config)# ip nbar custom ftdd 23 variable scid 1 tcp range 5001 5005
Device(config)# class-map match-any active-craft
Device(config-cmap)# match protocol ftdd scid 0x15
Device(config-cmap)# match protocol ftdd scid 0x21
Device(config-cmap)# match protocol ftdd scid 0x27
Device(config-cmap)# exit
Device(config)# class-map match-any passive-craft
Device(config-cmap)# match protocol ftdd scid 0x11
Device(config-cmap)# match protocol ftdd scid 0x22
Device(config-cmap)# match protocol ftdd scid 0x25
```

次の例は、SSL カスタム アプリケーション機能を設定し、サーバ名（Client Hello 拡張内に存在する場合）またはサーバからクライアントに送信された証明書内の共通名を使用して、HTTP over Secure Socket Layer（HTTPS）などのセキュア ソケット レイヤ（SSL）経由の任意のプロトコルに対して動作するアプリケーションをカスタマイズすることができる方法を示しています。

```
Device(config)# ip nbar custom name ssl unique-name www.example.com id 11
```

次の例は、DNS 名機能に基づいて NBAR カスタム アプリケーションを設定する方法を示しています。完全なドメイン名またはその一部を正規表現で指定できます。

```
Device(config)#  ip nbar custom name dns dns-name *example.com id 11
```

ip nbar custom transport

Network-Based Application Recognition（NBAR）を有効にし、IPアドレスに基づいてトラフィックを認識し、アプリケーション ID を指定の IP アドレスのトラフィックに関連付けるには、グローバル コンフィギュレーション モードで **ip nbar custom transport** コマンドを使用します。トラフィック認識を無効にするには、このコマンドの **no** 形式を使用します。

ip nbar custom 名前 **transport** {**tcp**|**udp**} **id** *id* {**ip** {**address** *ip-address*|**subnet** *subnet-ip subnet-mask*}|**ipv6 address** {*ipv6-address*|**subnet** *subnet-ipv6 ipv6-prefix*}|**port** {*port-number*|**range** *start-range end-range*}|**direction** {**any**|**destination**|**source**}}

no ip nbar custom *custom-name*

構文の説明

名前	カスタム プロトコルの名前。 名前は 24 文字以内である必要があります。また、小文字の英字（a ～ z）、数字（0 ～ 9）、およびアンダースコア（_）文字を含めることができます。
tcp	トランスポート プロトコルとして TCP を指定します。
udp	トランスポート プロトコルとして UDP を指定します。
id *id*	アプリケーション ID（セレクタ ID）を指定します。
ip address *ip-address*	空白で区切られた最大 8 つの IP アドレスを指定します。
ip subnet *subnet-ip*	TCP または UDP 転送を使用するサブネット IP アドレスを指定します。
subnet-mask	サブネット マスクの長さ。範囲は 0 ～ 32 です。
ipv6 address *ipv6-address*	空白で区切られた最大 8 つの IPv6 アドレスを指定します。
ip subnet *subnet-ipv6*	TCP または UDP 転送を使用する IPv6 サブネット IP アドレスを指定します。
ipv6-prefix	IPv6 のプレフィックスの数字。範囲は 0 ～ 128 です。
port *port-number*	空白で区切られた最大 8 つのポート番号を指定します。ポート番号の範囲は 1 ～ 65535 です。
range	最大で 1000 ポートの範囲を指定します。IP オプションを使用する場合、最大範囲は 8 を使用します。
start-range	範囲の開始ポート番号。指定できる範囲は 1 ～ 65535 です。
end-range	範囲の終了ポート番号。指定できる範囲は 1 ～ 65535 です。

direction	フローの方向を指定します。
any	パケットの任意の方向を指定します。
destination	パケットの宛先の方向を指定します。
source	パケットの送信元の方向を指定します。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
Cisco IOS XE Release 3.12S	このコマンドが導入されました。
15.4(2)T	このコマンドが Cisco IOS 15.4(2)T に統合されました。

使用上のガイドライン

IP アドレスとポートベースの設定を使用してカスタム プロトコルを設定するには、グローバル コンフィギュレーション モードで、**ip nbar custom transport** コマンドを使用します。

NBAR は、すべてのカスタム アプリケーションを含む、最大 110 のユーザ定義カスタム プロトコルをサポートできます。

カスタム IP アドレスとポート設定の場合、IP アドレスとポート番号は 8 個までに制限されます。

ip nbar custom transport コマンドをサポートするため、カスタム コンフィギュレーション モード（config-custom）が導入されます。

例

次に、カスタム 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)# ip nbar custom mycustom transport tcp id 100
Device(config-custom)#
```

次の例は、サブネットを 10.1.1.1 に、サブネット マスク長を 22 に指定する方法を示しています。

```
Device(config-custom)# ip subnet 10.1.1.1 22
```

次の例は、空白で区切った IP アドレスを指定する方法を示しています。

```
Device(config-custom)# ip address 10.1.1.2 10.1.1.3 10.1.1.4
```

次の例は、345 として開始ポート範囲を、また、350 として終了ポート範囲を設定する方法を示しています。

```
Device(config-custom)# port range 345 350
```

次に、グローバル コンフィギュレーション モードからカスタム コンフィギュレーション モードを開始し、サブネット IP アドレスおよびそのマスク長を設定する例を示します。

```
Device(config)#  ip nbar custom mycustom transport tcp id 100
Device(config-custom)# ip subnet 10.1.2.3 22
```

ip nbar pdlm

シスコが提供する Packet Description Language Module（PDLM）を使用し、Network-Based Application Recognition（NBAR）によって認識されるプロトコルのリストを拡張または強化するには、**ipnbarpdlmcommandinglobalconfiguration** モードを使用します。以前にロードした PDLM をアンロードするには、このコマンドの **no** 形式を使用します。

ip nbar pdlm *pdlm-name*
no ip nbar pdlm *pdlm-name*

構文の説明

pdlm-name	フラッシュ カードに PDLM がある URL です。

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（config）

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.1(13)E	このコマンドが、FlexWAN モジュールを備えていない Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
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。

使用上のガイドライン

ipnbarpdlm コマンドは、特定のバージョンの NBAR によって認識されるプロトコルのリストを拡張したり、既存のプロトコルの認識能力を強化するために使用します。NBAR には、実行時に外部の PDLM が提供される場合があります。ほとんどの場合、PDLM は NBAR を有効にし、新しい Cisco IOS イメージやルータのリロードなしで新しいプロトコルを認識できるようにします。新しい PDLM を提供できるのはシスコのみです。

利用可能な PDLM のリストは、Cisco.com でオンラインで表示できます。

例

次の例では、ルータのフラッシュ メモリから citrix.pdlm PDLM をロードするように NBAR を設定しています。

```
ip nbar pdlm flash://citrix.pdlm
```

関連コマンド

コマンド	説明
showipnbarpdlm	NBAR で使用されている現在の PDLM を表示します。

ip nbar port-map

このコマンドは廃止されました。

ウェルノウン ポート以外のポート番号を使用し、Network-Based Application Recognition（NBAR）を設定して、プロトコルまたはプロトコル名を検索するには、グローバル コンフィギュレーション モードで **ipnbarport-map** コマンドを使用します。ウェルノウン ポート番号のみを使用してプロトコル名を検索するには、このコマンドの **no** 形式を使用します。

ip nbar port-map *protocol-name* [{**tcp**|**udp**}] *port-number*
no ip nbar port-map *protocol-name* [{**tcp**|**udp**}] *port-number*

構文の説明

protocol-name	NBAR によって認識されるプロトコル名です。
tcp	（任意）指定した *protocol-name* 引数を、TCP ポートで検索するように指定します。
udp	（任意）指定した *protocol-name* 引数を、User Datagram Protocol（UDP）ポートで検索するように指定します。
port-number	名前付きプロトコルに割り当てられたポート。*port-number* 引数は、UDP ポート番号か TCP ポート番号であり、このコマンドラインで指定されるプロトコルによって決まります。1 つのコマンド ラインで最大 16 個の *port-number* 引数を指定できます。ポート番号の値は 0 ～ 65535 の範囲で指定します。

コマンド デフォルト

プロトコルは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.1(13)E	このコマンドが、FlexWAN モジュールを備えていない Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
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。

リリース	変更箇所
Cisco IOS XE Release 3.10S	このコマンドは廃止されました。

使用上のガイドライン

ipnbarport-map コマンドにより、Internet Assigned Numbers Authority（IANA）によって割り当てられたウェルノウン ポート以外のポート番号を使用し、NBAR で検索するプロトコルまたはプロトコル名を指定します。たとえば、このコマンドを使用して、23 以外のポートで Telnet を検索するように NBAR を設定します。このコマンドを使用すると、最大 16 ポートを指定できます。

NBAR プロトコルの一部は、ポートを確認する以外にも、トラフィック分類のためにヒューリスティックなアプローチに従います。**ipnbarport-map** コマンドを使用し、異なるポートをプロトコルに適用する場合、プロトコルのヒューリスティックな特性は変更されません。ポート番号を追加するメリットは、パフォーマンスが向上することです。

既存のポート マップに属さないポートに対して定義済みポート マップを最初に設定した場合にのみ、定義済みポート マップからウェルノウン ポートを削除できます。たとえば、カスタム ポート マップ X を定義し、ポート 20 と関連付けたい場合は、それができないことを示すエラーが表示されます。ただし、最初にポート マップ A を別のポート（ポート 100 など）に関連付けてからポート 20 との関連付けを削除した場合、カスタム ポート マップ X をポート 20 に関連付けることができます。

（注） 最善の結果を得るには、Citrix または BitTorrent プロトコルを設定しないでください。

例

次の例では、ウェルノウン ポート番号ではなく、ポート番号 63000 および 63001 でプロトコル Structured Query Language（SQL）*NET を検索するように、NBAR を設定しています。

```
Router(config)# ip nbar port-map sqlnet tcp 63000 63001
```

関連コマンド

コマンド	説明
showipnbarport-map	NBAR に現在使用されているプロトコルからポートへのマッピングを表示します。

ip nbar protocol-discovery

特定のインターフェイスで NBAR によって認識されるすべてのプロトコルのトラフィックを検出するように Network-Based Application Recognition（NBAR）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 モードまたは VLAN コンフィギュレーション モードで、**ipnbarprotocol-discovery** コマンドを使用します。トラフィック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。

ip nbar protocol-discovery [{**ipv4**|**ipv6**}]
no ip nbar protocol-discovery

構文の説明

ipv4	（任意）インターフェイスの IPv4 パケットに対してのみプロトコルディスカバリを指定します。
ipv6	（任意）インターフェイスの IPv6 パケットに対してのみプロトコルディスカバリを指定します。

コマンド デフォルト

トラフィック検出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）
VLAN コンフィギュレーション（config-vlan）-- Catalyst スイッチのみ

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.1(13)E	このコマンドが、FlexWAN モジュールを備えていない Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
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。
12.2(18)ZYA	このコマンドが、Cisco IOS Release 12.2(18)ZYA に統合されました。レイヤ 2 Etherchannel、レイヤ 3 Etherchannel、および VLAN コンフィギュレーション モードのサポートが提供されました（Catalyst スイッチのみ）。

リリース	変更箇所
Cisco IOS XE リリース 3.3S	このコマンドが、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータで Cisco IOS XE Release 3.3S に統合されました。**ipv6** キーワードが追加されました。

使用上のガイドライン

NBARで認識されるすべてのプロトコルに対してトラフィック統計情報を維持するようにNBARを設定するには、**ipnbarprotocol-discovery** コマンドを使用します。プロトコル ディスカバリは、QoS ポリシーを開発および適用できるように、インターフェイスを通過するアプリケーション プロトコルを検出するための容易な方法を提供します。プロトコル ディスカバリ機能は、NBAR でサポートされているすべてのプロトコル トラフィックを検出します。プロトコル ディスカバリは、入力トラフィックと出力トラフィックの両方をモニタするために使用でき、有効なサービス ポリシーがあってもなくても適用できます。

Cisco IOS XE Release 3.3S、L3、および L4 では、Internet Assigned Numbers Authority（IANA）プロトコルは IPv4 および IPv6 パケットに対してサポートされています。

ipv4 キーワードを入力して IPv4 パケットのプロトコル ディスカバリ統計情報収集を有効にするか、**ipv6** キーワードを入力して IPv6 パケットのプロトコル ディスカバリ統計情報収集を有効にします。次のいずれかのキーワードを指定すると、指定した IP バージョンのみの Protocol Discovery 統計情報収集が可能になります。どちらのキーワードも指定しなかった場合は、IPv4 と IPv6 の両方の統計情報収集が有効になります。指定したキーワードのみの統計情報収集が有効になるため、このコマンドの **no** 形式を使用してキーワードを無効にする必要はありません。

レイヤ 2/3 Etherchannel サポート

Cisco IOS Release 12.2(18)ZYA は、Supervisor 32/PISA を搭載した Catalyst 6500 シリーズ スイッチ用に設計されているため、**ipnbarprotocol-discovery** コマンドは、レイヤ 2 およびレイヤ 3 Etherchannel の両方でサポートされます。

例

次の例は、イーサネット インターフェイスで IPv4 と IPv6 の両方のプロトコル ディスカバリを設定する方法を示しています。

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 2/4
Router(config-if)# ip nbar protocol-discovery
Router(config-if)# end
```

関連コマンド

コマンド	説明
showipnbarprotocol-discovery	NBAR Protocol Discovery 機能によって収集された統計情報を表示します。

ip nbar protocol-pack

Network Based Application Recognition（NBAR）プロトコル パックをロードするには、グローバル コンフィギュレーション モードで **ip nbar protocol-pack** コマンドを使用します。ロード済みのプロトコル パックを削除するには、このコマンドの **no** 形式を使用します。

ip nbar protocol-pack *protocol-pack* **[force]**
no ip nbar protocol-pack *protocol-pack*

構文の説明

protocol-pack	プロトコル パック ファイルのパスおよび名前です。
force	（任意）デフォルトのプロトコル パック バージョンよりも低いバージョンのプロトコル パックをロードします。

コマンド デフォルト

デフォルトのプロトコル パックがロードされます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.3S	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

ip nbar protocol-pack コマンドを使用すると、複数のプロトコル記述言語（PDL）ファイルとマニフェスト ファイルを 1 つの圧縮ファイルにまとめたプロトコル パックを簡単にロードできます。このコマンドが導入される前は、PDL を個別にロードする必要がありました。このコマンドを使用すると、プロトコルのセットをロードできます。このプロトコルは、ネットワーク上での分類のために、NBAR が追加のプロトコルを認識するのに役立ちます。

次の状況では、**force** キーワードを使用します。

- Cisco IOS イメージに存在するデフォルトのプロトコル パック バージョンよりも低いバージョンの特定のプロトコル パックをロードする場合。
- 新しいバージョンにアップグレードすることになるか、低いバージョンのプロトコル パックに戻すことになるかに関わらず、既存のプロトコル パック バージョンを維持する場合。
- アクティブなプロトコル チェックを上書きする場合。

例

次の例は、ハードディスクから defProtoPack という名前のプロトコル パックをロードする方法を示しています。

```
Router# configure terminal
Router(config)# ip nbar protocol-pack harddisk:defProtoPack
```

次の例は、**force** キーワードを使用して、低いバージョンのプロトコル パックをロードする方法を示しています。

```
Router# configure terminal
Router(config)# ip nbar protocol-pack harddisk:olddefProtoPack force
```

関連コマンド

コマンド	説明
defaultipnbarprotocol-pack	プロトコル パックのベース バージョンをロードし、ロード済みのその他のすべてのプロトコル パックを削除します。
showipnbarprotocol-pack	プロトコル パック情報を表示します。

ip nbar resources

ipnbarresources コマンドは、**ipnbarresourcesprotocol** コマンドおよび **ipnbarresourcessystem** コマンドによって置き換えられます。詳細については、**ipnbarresourcesprotocol** コマンドおよび **ipnbarresourcessystem** コマンドを参照してください。

ip nbar resources protocol

プロトコル ベースの Network-Based Application Recognition（NBAR）フローリンク テーブルの有効期限を設定するには、グローバル コンフィギュレーション モードで **ip nbar resources protocol** コマンドを使用します。有効期限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 nbar resources protocol *link-age* [*protocol-name*]
no ip nbar resources protocol *link-age* [*protocol-name*]

構文の説明

link-age	プロトコルのリンクの有効期限が切れる時間（秒）。範囲は 1 ～ 1000000000 です。デフォルトは 120 です。
protocol-name	（任意）ロード済みのプロトコル記述言語（PDL）モジュールに登録されているプロトコルの名前です。

コマンド デフォルト

このリンク期間経過は、すべてのプロトコルに対して 120 秒です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.4(6)T	このコマンドが導入されました。
Cisco IOS XE Release 3.2S	このコマンドが、Cisco ASR 1000 シリーズ ルータで実装されました。

使用上のガイドライン

サポートされているプロトコルのリストを表示するには、**match protocol ?** または **show ip nbar port-map** コマンドを入力します。

特定のプロトコルのリンク期間経過を設定するには、**ip nbar resources protocol** コマンドに、*protocol-name* 引数を含める必要があります。*protocol-name* 引数を含めないと、すべてのプロトコルのリンク期間経過タイマーは、指定されたリンク期間経過値に設定されます。

特定のプロトコルのリンク期間経過をリセットするには、**no ip nbar resources protocol** コマンドに、*protocol-name* 引数を含める必要があります。*protocol-name* 引数を含めないと、すべてのプロトコルのリンク期間経過タイマーは 120 に設定されます。

存在しないプロトコル名を入力すると、次のエラー メッセージが表示されます。

```
%NBAR ERROR: <entered string> is not a valid protocol
```

指定したプロトコルに関連付けられたすべての状態のノードのリンク期間経過をリセットすることに加え、プロトコル名とそのリンク期間経過は、デバイスのリセットが発生する可能性に備えて NVRAM に保存されます。

例

次に、すべてのプロトコルに対してリンク期間経過を360秒に設定する例を示します。

```
Device# configure terminal
Device(config)# ip nbar resources protocol 360
```

次に、kazaa2 プロトコルに対してリンク期間経過を 180 秒に設定する例を示します。

```
Device# configure terminal
Device(config)# ip nbar resources protocol 180 kazaa2
```

関連コマンド

コマンド	説明
ipnbarresourcessystem	システム全体で、NBAR フローリンク テーブルの有効期限とメモリ要件を設定します。

ip nbar resources system

このコマンドは廃止されました。

システム全体の Network-Based Application Recognition（NBAR）フローリンク テーブルの有効期限およびメモリ要件を設定するには、グローバル コンフィギュレーション モードで **ipnbarresourcessystem** コマンドを使用します。アクティブなリンクを削除するには、このコマンドの **no** 形式を使用します。

ip nbar resources system *system-link-age initial-memory exp-memory*
no ip nbar resources system

構文の説明

system-link-age	システムのリンクが期間経過（期限切れ）になる時間（秒）。範囲は 10 ～ 86400 です。デフォルトは 30 です。
initial-memory	初期化時にリンクに割り当てられたメモリのサイズ（キロバイト）。範囲は 1 ～ 30000 です。デフォルトは、システム初期化時の空きメモリの合計値の 10% であり、プラットフォームごとに異なります。
exp-memory	より大きい領域がリンクに必要であることを NBAR が検出した場合に、拡張できるメモリ サイズ（キロバイト）。範囲は 0 ～ 112 です。デフォルトは 112 です。 （注） デフォルトは、NBAR の内部構造のサイズに基づいており、将来のリリースで変更される場合があります。

コマンド デフォルト

デフォルトのシステム リンクの期間経過は、NBAR の有効化時に 30 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	変更箇所
12.4(6)T	このコマンドが導入されました。
Cisco IOS 15.4(3)M および IOS XE 3.13S	このコマンドは廃止されました。

使用上のガイドライン

ipnbarresourcessystem コマンドは NBAR に対してシステム全体で影響するため、パラメータを任意に変更しないでください。パラメータを任意に変更すると、NBAR の非効率な動作や正しくない動作につながる可能性があります。デフォルト値は、ほとんどのインスタンスで有効です。

例

次の例では、システム リンクの期間経過が 30 秒、初期メモリが 200 キロバイト、および拡張メモリが 112 キロバイトになっています。

```
Router# configure terminal
Router(config)# ip nbar resources system 30 200 112
```

関連コマンド

コマンド	説明
ipnbarresourcesprotocol	プロトコル ベースで、NBAR フロー リンク テーブルの有効期限を設定します。

ip options

ルータに送信される IP オプション パケットを破棄または無視するには、グローバル コンフィギュレーション モードで **ip options** コマンドを使用します。この機能を無効にし、すべての IP オプション パケットをルータに送信できるようにするには、このコマンドの **no** 形式を使用します。

ip options {**drop**|**ignore**}
no ip options {**drop**|**ignore**}

構文の説明

drop	ルータは受信したすべての IP オプション パケットを破棄します。
ignore	ルータは、すべてのオプションを無視し、IP オプションがないかのようにパケットを処理します。（オプションはパケットから削除されるわけではなく、単に無視されます。） （注） このオプションは、Cisco 10000 シリーズ ルータで使用できません。

コマンド デフォルト

このコマンドはディセーブルになります。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.0(23)S	このコマンドが導入されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
12.2(27)SBC	このコマンドが、Cisco IOS Release 12.2(27)SBC に統合されました。
12.3(19)	このコマンドが Cisco IOS Release 12.3(19) に統合されました。
12.2(31)SB2	このコマンドが PRE3 用の Cisco IOS Release 12.2(31)SB2 に統合されました。

使用上のガイドライン

ip options コマンドを使用すると、IP オプション パケットをフィルタ処理し、ルータ、およびダウンストリームのルータとホストの IP オプションの効果を軽減できます。

破棄モードと無視モードは相互に排他的です。つまり、破棄モードが設定されている場合に無視モードを設定すると、無視モードによって破棄モードが上書きされます。

Cisco 10720 インターネット ルータ

ip options ignore コマンドはサポートされていません。破棄モード（**ip options drop** コマンド）のみがサポートされています。

Cisco 10000 シリーズ ルータ

このコマンドは、PRE3 でのみ利用できます。PRE2 はこのコマンドをサポートしません。

ip options ignoreコマンドはサポートされていません。ルータは、**ip options drop** コマンドのみをサポートします。

例

次に、ネットワークに入ったすべてのオプション パケットをドロップするように、ルータ（およびダウンストリーム ルータ）を設定する例を示します。

```
ip options drop
% Warning:RSVP and other protocols that use IP Options packets may not function in drop
 or ignore modes.
end
```

ip rsvp admission-control compression predict

リソース予約プロトコル（RSVP）アドミッション コントロール圧縮予測を設定するには、インターフェイス コンフィギュレーション モードで **iprsvpadmission-controlcompressionpredict** コマンドを使用します。圧縮予測を無効にするには、このコマンドの **no** 形式を使用します。

ip rsvp admission-control compression predict [**method** {**rtp**|**udp**} [**bytes-saved** *N*]]
no ip rsvp admission-control compression predict [**method** {**rtp**|**udp**} [**bytes-saved** *N*]]

構文の説明

method	（オプション）使用される圧縮の種類です。
rtp udp	Real-time Transport Protocol（RTP）または User Datagram Protocol（UDP）圧縮方式。
bytes-saved *N*	（オプション）指定された方式で圧縮が実行されると RSVP によって予測された場合に、パケットごとに保存される予測バイト数。RTP の場合、N の値は 1 ～ 38、UDP の場合は 1 ～ 26 です。

コマンド デフォルト

このコマンドはデフォルトでイネーブルになっています。RTP の場合、保存されるデフォルトのバイト数は 36、UDP の場合は 20 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	変更箇所
12.2(15)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

rtp と **udp** のいずれも選択しない場合、指定した方式またはすべての方式に対して RSVP 圧縮予測を有効または無効にするには、**iprsvpadmission-controlcompressionpredict** コマンドを使用します。フローごとに圧縮率を計算するために RSVP が使用する、デフォルトの圧縮パラメータを調整できます。

iprsvpadmission-controlcompressionpredict コマンドを使用して圧縮方式またはパケットごとに保存されるバイト数を変更した場合、これらの値は新しいフローにのみ影響し、既存のフローには影響を及ぼしません。

圧縮には、アグレッシブとコンサーバティブという 2 つのアプローチがあります。コンサーバティブで圧縮を予測する場合、パケットごとの保存バイト数を少なく想定しますが、保証される Quality of Service（QoS）は高くなる可能性があります。呼び出しごとに許可される帯域幅はより大きくなりますが、各リンクが対応できる呼び出しの数は少なくなります。アグレッシブで圧縮を予測する場合、パケットごとの保存バイト数を多く想定しますが、保証される Quality of Service（QoS）は低くなる可能性があります。呼び出しごとに許可される帯域幅はより小さくなりますが、各リンクが対応できる呼び出しの数は大きくなります。

例

次の例は、パケットごとに30バイト保存されるRTPを使用したフローの圧縮パラメータを設定する方法を示しています。

```
Router(config-if)# ip rsvp admission-control compression predict method rtp bytes-saved
 30
```

次の例は、パケットごとに20バイト保存されるUDPを使用したフローの圧縮パラメータを設定する方法を示しています。

```
Router(config-if)# ip rsvp admission-control compression predict method udp bytes-saved
 20
```

次の例は、RTP ヘッダー圧縮予測を無効にする方法を示しています。

```
Router(config-if)# no ip rsvp admission-control compression predict method rtp
```

UDP ヘッダー圧縮予測を無効にする方法を、次に示します。

```
Router(config-if)# no ip rsvp admission-control compression predict method udp
```

（注） 圧縮パラメータを無効にすると、指定した方式を使用するフローのみにパラメータが影響します。

関連コマンド

コマンド	説明
showiprtpheader-compression	RTPヘッダー圧縮についての統計を表示します。

ip rsvp aggregation ip

リソース予約プロトコル（RSVP）集約をルータで有効にするには、グローバル コンフィギュレーション モードで **iprsvpaggregationip** コマンドを使用します。RSVP 集約を無効にするには、このコマンドの **no** 形式を使用します。

ip rsvp aggregation ip
no ip rsvp aggregation 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

RSVP アグリゲーション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	変更箇所
12.2(33)SRC	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

ルータで集約を有効にすると、ルータはアグリゲータ、デアグリゲータ、または内部ルータとして機能します。アグリゲータおよびデアグリゲータの機能を実行するには、RSVP プロセスが、ルータ上で RSVP-E2E-IGNORE プロトコル タイプ（134）を認識する必要があります。そうしないと、メッセージはルータのデータ プレーンによってデータとして転送されます。**iprsvpaggregationip** コマンドは、RSVP で RSVP-E2E-IGNORE プロトコルを使用したメッセージの識別を有効にします。その後、エンドツーエンド（E2E）予約の集約とデアグリゲーション動作を指定する追加のコマンドを設定します。

iprsvpaggregationip コマンドは、ルータが RSVP-E2E-IGNORE メッセージを受信するように登録します。内部ルータでは、RSVP 集約予約のみを処理するため、このコマンドを発行する必要はありません。この手順を実行すると、内部ルータが無駄にすべての RSVP-E2E-IGNORE メッセージを処理するため、パフォーマンスが低下することがあります。

（注） RSVP 集約を内部ルータでグローバルにイネーブルにする場合は、すべてのインターフェイスを内部として設定する必要があります。設定しないと、インターフェイスは外部に戻され、RSVP-E2E-IGNORE パケットは破棄されます。

例

次の例は、ルータで RSVP 集約を有効にする方法を示しています。

```
Router(config)# ip rsvp aggregation ip
```

関連コマンド

コマンド	説明
showiprsvpaggregationip	RSVP 要約集約情報を表示します。

ip rsvp aggregation ip map

リソース予約プロトコル（RSVP）集約ルールを設定し、エンドツーエンド（E2E）予約を集約予約にマップする方法をルータに通知するには、グローバル コンフィギュレーション モードで **iprsvpaggregationipmap** コマンドを使用します。RSVP 集約キューを無効にするには、このコマンドの **no** 形式を使用します。

ip rsvp aggregation ip map {**access-list** *acl-number*|**any**} **dscp** *value*
no ip rsvp aggregation ip map {**access-list** *acl-number*|**any**}

構文の説明

access-list	アクセス コントロール リスト（ACL）を指定します。
acl-number	ACL の番号。値は 1 ～ 199 です。
any	アグリゲータとデアグリゲータの間のすべての予約が 1 つの DSCP に集約される場合に、使用する一致基準を示します。
dscp *value*	Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を指定します。有効な値は次のとおりです。 • 0 ～ 63：DSCP の数値。デフォルト値は 0 です。 • af1 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）プレシデンス値。 • default：デフォルト DSCP 値。 • ef：Expedited Forwarding（EF; 完全優先転送）DSCP 値。

コマンド デフォルト

集約マッピング ルールは設定されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.2(33)SRC	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

E2E 予約が集約にマッピングされるように単一のグローバル ルールを設定するには、**iprsvpaggregationipmap** コマンドを使用します。

iprsvpaggregationipmap コマンドを使用する前に、RSVP エンドポイントのグループを定義し、グループの予約が単一の DSCP に集約されるように ACL を設定する必要があります。ACL は、標準 ACL にすることも拡張 ACL にすることもできます。

標準 ACL

- IP アドレスは、RSVP PATH メッセージの送信者テンプレートまたは RSVP RESV メッセージ フィルタ指定に一致します。これは、IP 送信元アドレスまたは RSVP 送信側です。

拡張 ACL の有無

iprsvpaggregationipmap コマンド内で使用される ACL は、RSVP メッセージ オブジェクトに対して、拡張 ACL を次のように照合します。

- 送信元 IP アドレスとポートは、RSVP PATH メッセージの送信者テンプレートまたは RSVP RESV メッセージ フィルタ指定に一致します。これは、IP 送信元または RSVP 送信元です。
- 宛先 IP アドレスとポートは、RSVP PATH/RESV メッセージ セッション オブジェクトの IP アドレスに一致します。これは、IP 宛先アドレスまたは RSVP 受信者です。
- プロトコルは、RSVP PATH/RESV メッセージ セッション オブジェクト プロトコルを照合します。プロトコルが IP の場合、上記のように送信元または宛先アドレスを照合します。

（注） 従来の（集約されない）RSVP では、セッションは、予約メッセージ セッション オブジェクト中で、宛先 IP アドレスとプロトコル情報によって識別されます。RSVP 集約では、セッションは集約 RSVP メッセージのセッション オブジェクト内で宛先 IP アドレスと DSCP によって識別されます。E2E 予約は、E2E 予約セッション オブジェクトのみ、あるいは、セッション オブジェクトと送信者テンプレートまたはフィルタ指定の組み合わせによって識別される特定の集約 RSVP セッションにマッピングされます。

例

次の例では、RSVP PATH メッセージのセッション オブジェクト宛先アドレスがサブネット 10.1.0.0 内にあるすべての RSVP メッセージについて、アクセス リスト 1 を定義しています。これにより、デアグリゲータがこれらの予約を AF41 Per-Hop Behavior に関連付けられている DSCP の集約予約にマッピングできるようになります。

```
Router(config)# access-list 1 permit host 10.1.0.0 0.0.255.255
Router(config)# ip rsvp aggregation ip map access-list 1 dscp af41
```

次の例では、アグリゲータとデアグリゲータの間のすべての予約が 1 つの DSCP に集約されます。

```
Router(config)# ip rsvp aggregation ip map any dscp af41
```

関連コマンド

コマンド	説明
iprsvpaggregationip	ルータで RSVP 集約を有効にします。
showiprsvpaggregationip	RSVP 要約集約情報を表示します。

ip rsvp aggregation ip reservation dscp

Differentiated Services Code Point（DSCP; DiffServ コード ポイント）ベースでリソース予約プロトコル（RSVP）集約予約属性（トークン バケット パラメータとも呼ばれる）を使用するには、グローバル コンフィギュレーション モードで **iprsvpaggregationipreservationdscp** コマンドを使用します。集約予約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。

ip rsvp aggregation ip reservation dscp *value* [**aggregator** *agg-ip-address*] **traffic-params static rate** *data-rate* [**burst** *burst-size*] [**peak** *peak-rate*]
no ip rsvp aggregation ip reservation dscp *value* [**aggregator** *agg-ip-address*] **traffic-params static rate** *data-rate* [**burst** *burst-size*] [**peak** *peak-rate*]

構文の説明

value	集約予約の DSCP 値。値は、次のいずれかにすることができます。 • 0 ～ 63：DSCP の数値。デフォルト値は 0 です。 • af11 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）プレシデンス値。 • default：デフォルト DSCP 値。 • ef：Expedited Forwarding（EF; 完全優先転送）DSCP 値。
aggregator *agg-ip-address*	（オプション）data-rate、burst-size、および peak-rate トラフィック パラメータが適用されるアグリゲータの IP アドレスを指定します。 （注） 省略した場合、デアグリゲータに対するすべての集約予約で同一のトークン バケット パラメータが使用されます。
traffic-params	トラフィック パラメータ属性を指定します。
static	静的なトラフィック パラメータ属性を指定します。
rate *data-rate*	平均データ レート（キロビット/秒）を指定します。範囲は 1 ～ 10000000 です。
burst *burst-size*	（オプション）最大データ バースト サイズ（キロバイト）を指定します。範囲は 1 ～ 8192 です。 （注） 省略した場合、この値は集約レート値に等しくなります。
peak *peak-rate*	（オプション）ピーク データ レート（キロビット/秒）を指定します。範囲は 1 ～ 10000000 です。 （注） 省略した場合、この値は集約レート値に等しくなります。

コマンド デフォルト

集計予約属性（トークン バケット パラメータ）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（config）

コマンド履歴

リリース	変更箇所
12.2(33)SRC	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

iprsvpaggregationipreservationdscp コマンドを使用して、トークンバケットパラメータを静的に設定できます。

デアグリゲータで収集 RESV メッセージ用に flowspec オブジェクトを構成しやすくするには、*data-rate*、*burst-size*、および *peak-rate* 引数が必要です。既存の RSVP プロシージャは、フローに対して確立された予約のサイズが PATH sender_tspec と RESV flowspec の最小値に設定されるように指定します。そのため、集約 PATH の sender_tspec *data-rate*、*burst-size*、または *peak-rate* 引数が、デアグリゲータで設定されている *data-rate*、*burst-size*、または *peak-rate* 引数よりも大きい場合、集約 RESV flowspec オブジェクトは PATH メッセージおよび設定された値から *data-rate*、*burst-size*、および *peak-rate* の最小値を含むことになります。

集約にマップされているエンドツーエンド（E2E）予約の合計帯域幅よりも厳格さが低い値へと集約予約サイズが変更された場合、プリエンプションが発生することがあります。

集約帯域幅が小さくなった場合に、プリエンプションが必要かつ**iprsvppolicypreempt** コマンドの発行によって有効になっていない場合、変更は拒否され、次のメッセージが表示される可能性があります。

```
RSVP:AGG: Command not accepted.
RSVP-AGG: This change requires some E2E reservations to be removed and
RSVP:AGG: preemption is not enabled. Issue 'ip rsvp policy preempt'
RSVP:AGG: in order to make this change.
```

例

次の例は、DSCP が AF11 の場合に、アグリゲータ 10.10.10.10 を使用して確立された集約予約に対する集約 RESV メッセージの設定方法を示しています。これには、10 kbps の平均レートおよびピーク レートと、8 KB のバーストサイズを要求する flowspec が含まれています。

```
Router(config)# ip rsvp aggregation ip reservation dscp af11 aggregator 10.10.10.10
traffic-params static rate 10 burst 8 peak 10
```

関連コマンド

コマンド	説明
iprsvpaggregationip	ルータで RSVP 集約を有効にします。
iprsvppolicypreempt	プライオリティの低い予約からプライオリティの高い予約へと、帯域幅を再分配します。
showiprsvpaggregationip	RSVP 要約集約情報を表示します。

ip rsvp aggregation ip role interior

集約領域側のアグリゲータおよびデアグリゲータの内部ルータでリソース予約プロトコル（RSVP）集約を設定するには、インターフェイス コンフィギュレーション モードで **iprsvpaggregationiproleinterior** コマンドを使用します。アグリゲータおよびデアグリゲータルータで RSVP 集約を無効にするには、このコマンドの **no** 形式を使用します。

ip rsvp aggregation ip role interior
no ip rsvp aggregation ip role interior

構文の説明

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

RSVP 集約は、アグリゲータおよびデアグリゲータの内部ルータでは設定されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.2(33)SRC	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

このコマンドは、エンドツーエンド（E2E）メッセージがインターフェイスに到達するまで、ルータに影響はありません。

ルータが E2E のすべてのフローの内部ノードである場合は、集約コマンドを設定する必要はありません。RSVP は、IP データグラムとして転送される RSVP-E2E-IGNORE メッセージの通知を取得することはありません。ただし、ルータには集約をサポートするイメージがロードされているため、ルータは集約シグナリング メッセージを正しく処理します。

内部ノードで集約を有効にした場合は、そのすべてのインターフェイスを内部として設定する必要があります。そうしないと、すべてのインターフェイスの役割が外部となり、ルータに到着するすべての E2E Path（E2E-IGNORE）メッセージが廃棄されます。

つまり、内部ルータについては次の 2 つの選択肢があります。

- RSVP 集約コンフィギュレーション コマンドを入力しない。
- 集約を有効にし、すべてのインターフェイスを内部として設定する。

インターフェイスの内部の役割が設定されていない場合、そのインターフェイスにインストールされているすべての集約および E2E 予約は停止します。

追加の必要な設定コマンド

アグリゲータまたはデアグリゲータの RSVP インターフェイス、および内部ルータのインターフェイスで集約を有効にする場合は、次のコマンドも設定する必要があります。

- **iprsvpresource-providernone**
- **iprsvpdata-packetclassificationnone**

これらのコマンドを設定する理由は、Cisco IOS Release 12.2(33)SRC と Cisco IOS XE Release 2.6 がコントロール プレーンの集約のみをサポートするためです。RSVP データ パケット分類子は、集約をサポートしていません。データ プレーン集計は、RSVP スケーラビリティ拡張機能を使用して実行する必要があります。

例

次の例は、アグリゲータまたはデアグリゲータの内部ルータのイーサネット 0/0 インターフェイスを設定する方法を示しています。

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip rsvp aggregation ip role interior
```

関連コマンド

コマンド	説明
iprsvpaggregationip	ルータで RSVP 集約を有効にします。
iprsvpdata-packetclassificationnone	RSVP データ パケット分類を無効にします。
iprsvpresource-providernone	集約フローのリソース プロバイダーを設定します。
showiprsvpaggregationip	RSVP 要約集約情報を表示します。

ip rsvp atm-peak-rate-limit

現在のインターフェイスまたはそのサブインターフェイスのいずれかに確立された、すべての新規作成されたリソース予約プロトコル（RSVP）相手先選択接続（SVC）に対して予約のピーク セル レート（PCR）に制限を設定するには、インターフェイス コンフィギュレーション モードで **iprsvpatm-peak-rate-limit** コマンドを使用します。予約レートがライン レートによって制限される、現在のピーク レー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。

ip rsvp atm-peak-rate-limit *limit*
no ip rsvp atm-peak-rate-limit

構文の説明

limit	指定された予約のピーク レート制限（KB）。許容される最小値は 1 KB であり、許容される最大値は 2 GB です。

コマンド デフォルト

予約のピーク レートのデフォルトは、ライン レートです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
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。

使用上のガイドライン

各 RSVP 予約は、特定のピーク セル レート（PCR）、平均セル レート（SCR）、および最大バースト サイズを備えた ATM SVC に対応します。PCR は、ピーク レートとも呼ばれ、ユーザが設定することも、デフォルトのライン レートにすることもできます。

RSVP によって制御される負荷予約は、データのピーク レートを定義しません。慣例により、このような予約の許容ピーク レートは無限大とされ、通常非常に大きい数によって表されます。これらの状況下では、制御される負荷予約が ATM SVC に変換され、SVC の PCR はこれに対応して大きくなり、スイッチの範囲外となる可能性があります。**iprsvpatm-peak-rate-limit** コマンドを使用して、ピーク レートを制限できます。

RSVP SVC のピーク レート制限は、次の条件により決定されます。

- ピーク レートのデフォルトが、ライン レートになっている。
- 設定されたピーク レート リミッタよりもピーク レートが大きい場合、ピーク レートはピーク レート リミッタよりも小さくされる。

- ピーク レートを予約帯域幅よりも小さくすることはできません。これが該当する場合、ピーク レートは予約帯域幅まで引き上げられます。

（注） RSVP スペースから ATM スペースに適用される帯域幅変換は、ピーク レートにも適用されます。

ピーク レート制限は、ルータにローカルなものであり、RSVP の通常のメッセージングには影響しません。SVC セットアップのみが影響を受けます。大きなピーク レートは、変更されずに次のホストに送信されます。

サブインターフェイスに確立された RSVP SVC の場合、サブインターフェイスに適用されるピーク レート制限は、そのサブインターフェイスに作成されたすべての SVC に影響します。ピーク レート制限がメイン インターフェイスに適用される場合、そのメイン インターフェイスの制限値がサブインターフェイスに適用される制限よりも低かったとしても、メイン インターフェイスのサブインターフェイスに作成された SVC に影響することはありません。

特定のインターフェイスまたはサブインターフェイスに対して、そのインターフェイスに適用されたピーク レート制限は、インターフェイスに作成された新しい SVC にのみ影響し、既存の SVC には影響しません。

（注） このコマンドは、**iprsvpsvc-required** コマンドをサポートするインターフェイス上でのみ利用可能です。

インターフェイスまたはサブインターフェイスに設定されたピーク レート制限を特定するには（存在する場合）、**showiprsvpatm-peak-rate-limit** コマンドを使用します。

例

次の設定サンプルは、ATM インターフェイス 2/0/0.1 のピーク レート制限を 100 KB に設定しています。

```
interface atm2/0/0.1
 ip rsvp atm-peak-rate-limit 100
```

関連コマンド

Command	Description
iprsvpsvc-required	インターフェイスまたはサブインターフェイスで行われる新しい RSVP 予約にサービスを提供するため、SVC の作成を有効にします。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。

ip rsvp authentication

リソース予約プロトコル（RSVP）暗号化認証を有効にするには、インターフェイス コンフィギュレーション モードで **iprsvpauthentication** コマンドを使用します。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。

ip rsvp authentication
no ip rsvp authentication

構文の説明

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

RSVP 暗号化認証は、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	変更箇所
12.2(15)T	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

他の RSVP 認証設定コマンドを再入力することなく RSVP 認証を無効にしてから再有効化するには、**iprsvpauthentication** コマンドを使用します。以前にキーを設定していない限り、認証を有効にしないでください。**iprsvpauthenticationkey** コマンドの前にこのコマンドを発行すると、キーを指定するまで RSVP がすべてのメッセージを破棄することを示す警告メッセージが表示されます。**noiprsvpauthentication** コマンドは、RSVP 暗号化認証を無効にします。ただし、このコマンドが、他の設定済みの認証パラメータを自動的に削除することはありません。設定から削除する場合は、特定の **noiprsvpauthentication** コマンドを発行する必要があります。たとえば、**noiprsvpauthenticationkey**、**noiprsvpauthenticationtype**、または **noiprsvpauthenticationwindow-size** などです。

iprsvpauthentication コマンドは、**iprsvpneighbor** コマンドと類似しています。ただし、**iprsvpauthentication** コマンドは、より優れた認証を提供し、システム ロギングを実行します。

例

次のコマンドは、インターフェイスで認証を有効にします。

```
Router(config-if)# ip rsvp authentication
```

次のコマンドは、インターフェイスで認証を無効にします。

```
Router(config-if)# no ip rsvp authentication
```

関連コマンド

コマンド	説明
iprsvpauthenticationkey	RSVP 認証アルゴリズムのキー（文字列）を指定します。
iprsvpauthenticationtype	RSVP メッセージに暗号化署名を生成するために使用するアルゴリズムを指定します。
iprsvpauthenticationwindow-size	順序どおりでなくても受信できる RSVP 認証済みメッセージの最大数を指定します。
iprsvpneighbor	ネイバーによる予約の要求を有効にします。

ip rsvp authentication challenge

リソース予約プロトコル（RSVP）によって、ネットワークの任意の新規ネイバーとチャレンジレスポンス ハンドシェイクを実行するには、インターフェイス コンフィギュレーション モードで **iprsvpauthenticationchallenge** コマンドを使用します。チャレンジレスポンス ハンドシェイ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。

ip rsvp authentication challenge
no ip rsvp authentication challenge

構文の説明

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

このコマンドによって開始されるチャレンジレスポンス ハンドシェイク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	変更箇所
12.2(15)T	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

i**prsvpauthenticationchallenge** コマンドでは、ネットワーク上で新しい RSVP が検出された場合、RSVP でチャレンジレスポンス ハンドシェイクを実行する必要があります。このハンドシェイクを実行することで、ルータは再起動後に、信頼されている RSVP ネイバーによる起動時の RSVP メッセージ リプレイ アタックを阻止することができます（特に、長期間動作していない場合）。ルータの再起動後、信頼されている RSVP ネイバーからメッセージが非常に早く到着した場合、信頼されていないノードがリプレイ アタックを試みる前に、ルータは信頼されているノードとのセキュリティ アソシエーションを再確立するため、チャレンジは必要ない可能性があります。

マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）が移動するインターフェイスで RSVP 認証を有効にし、その認証でルータのステートフル スイッチオーバー（SSO）が有効になっている場合、次のことが発生します。

- チャレンジが無効になっている（**iprsvpauthenticationchallenge** コマンドを指定しなかった）場合、LSP が適切に回復します。
- チャレンジが有効になっている（**iprsvpauthenticationchallenge** コマンドを指定した）場合、さらに RSVP シグナリング メッセージが必要であり、LSP が回復するのにより長い時間がかかります。または、フォワーディング ステートがタイムアウトし、回復しない可能

性があります。タイムアウトが発生すると、ヘッドエンド ルータが新しい LSP にシグナルを送信し、データ パケットの転送が中断されます。

RSVP 認証チャレンジを有効にした場合、**iprsvpsignallingrefreshreduction** コマンドを使用した RSVP リフレッシュ削減の有効化を検討してください。チャレンジ ハンドシェイクの進行中は、ハンドシェイクを開始したルータがチャレンジに対する有効なレスポンスを受信するまで、ハンドシェイクを開始した受信側のルータではチャレンジの対象となっているノードからのすべての RSVP メッセージが破棄されます。

（注） ネイバーが最初のチャレンジ メッセージに応答しない場合、Cisco IOS ソフトウェアは 1 秒後に別のチャレンジ メッセージを送信し、2 秒間待機します。2 回目のチャレンジに対するレスポンスを受信しなかった場合、Cisco IOS ソフトウェアはさらにチャレンジを送信し、4 秒間待機します。3 回目のチャレンジに対するレスポンスを受信しなかった場合、Cisco IOS ソフトウェアは 4 回目のチャレンジを送信し、8 秒間待機します。4 回目のチャレンジに対するレスポンスがない場合、Cisco IOS ソフトウェアはそのネイバーへの現在のチャレンジを停止し、システム エラー メッセージをログに記録し、ネイバーとのセキュリティ アソシエーションを作成しません。このような Exponential Backoff は、ネットワークまたはビジー状態のネイバーによって破棄されたチャレンジから回復するために使用されます。

リフレッシュ削減を有効にすると、チャレンジの対象となっているノードは、破棄されたメッセージをハンドシェイクの完了後により迅速に再送信できます。これにより、ルータの再起動時に、迅速に予約状態が再確立されます。

リプレイ アタックに対するルータの脆弱性を可能な限り低減するため、認証チャレンジを有効にしてください。

例

次の例は、RSVP を有効にし、チャレンジレスポンス ハンドシェイクを実行する方法を示しています。

```
Router(config-if)# ip rsvp authentication challenge
```

関連コマンド

コマンド	説明
iprsvpsignallingrefreshreduction	リフレッシュ削減を有効にします。

ip rsvp authentication key

リソース予約プロトコル（RSVP）認証アルゴリズムのキー（文字列）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 **iprsvpauthenticationkey** コマンドを使用します。キーをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip rsvp authentication key *pass-phrase*
no ip rsvp authentication key

構文の説明

pass-phrase	8 ～ 40 文字の範囲のフレーズ。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

キーは指定されていません。

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	変更箇所
12.2(15)T	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

認証アルゴリズムのキーを選択するには、**iprsvpauthenticationkey** コマンドを選択します。このキーは、8～40 文字のパスフレーズです。これには、スペースを含めることができます。スペースを使用する場合、引用符は必要ありません。キーは、複数の単語で構成できます。可能な限り長いパスフレーズを作成することをお勧めします。このキーは、このインターフェイスのすべての RSVP ネイバーに対して同じである必要があります。すべてのパスワードと同様に、攻撃者が簡単に推測できないように、パスワードは慎重に選択する必要があります。

いくつかのガイドラインを、次に示します。

- 大文字と小文字、数字、および記号を含めます。
- 1 単語だけを使用する場合、どの言語のどのような辞書、スペルのリスト、その他の単語の一覧にも含まれていない単語を使用します。
- 書き留めておく必要がないように、覚えやすいものを使用します。
- ファイルやスクリプト内のクリアテキスト、または端末に貼り付けた紙でパスワードが知られることがないようにします。

デフォルトでは、RSVP 認証キーはルータ設定ファイル内にクリア テキストで保存されますが、必要に応じて設定ファイル内に暗号化されたテキストとして保存できます。キーの暗号化を有効にするには、グローバル設定の **keyconfig-key1***string* コマンドを使用します。このコマ

ンドの入力後、各 **iprsvpauthenticationkey** コマンドのパスフレーズパラメータは、設定ファイルの保存時に Data Encryption Standard（DES; データ暗号規格）によって暗号化されます。後から **nokeyconfig-key** 1 *string* コマンドを発行する場合、RSVP 認証キーは設定の保存時にクリアテキストで再度保存されます。

string 引数は設定ファイルに保存されません。ルータのプライベート NVRAM にのみ保存され、**showrunning-config** コマンドまたは **showconfig** コマンドの出力に表示されません。したがって、別のルータに設定ファイルをコピーする場合、ルータが起動して RSVP 認証が正しく動作していないと、そのファイル内の暗号化された RSVP キーは RSVP で正しく復号できません。この状態から回復するには、新しいルータで次の手順を実行します。

1. 認証キーを持つ各 RSVP インターフェイスに対して、古いキーをクリアするため、**noiprsvpauthenticationkey** コマンドを発行します。
2. RSVP インターフェイスの同じセットに対して、**iprsvpauthenticationkey** コマンドを発行し、正しいクリア テキスト キーを再構成します。
3. グローバルな **keyconfig-key** 1 *string* コマンドを発行し、新しいルータに対して RSVP キーを再度暗号化します。
4. 設定を保存します。

例

次のコマンドは、クリア テキストでパスフレーズを 11223344 に設定する方法を示しています。

```
Router(config-if)# ip rsvp authentication key 11223344
```

次のコマンドは、認証キーを暗号化する方法を示しています。

```
Router# configure terminal
Router(config)# key config-key 1 11223344
Router(config)# end
```

関連コマンド

コマンド	説明
keyconfig-key	ルータのプライベート DEF キーを定義します。

ip rsvp authentication key-chain

リソース予約プロトコル（RSVP）ネイバーのキーの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 **iprsvpauthenticationkey-chain** コマンドを使用します。キー チェー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。キー チェーンをデフォルトに設定するには、このコマンドの **no** 形式を使用します。

ip rsvp authentication key-chain *string*
no ip rsvp authentication key-chain

構文の説明

string	キー チェーンの名前。範囲は 1 ～ 2147483647 個のキーです。

コマンド デフォルト

キー チェーン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	変更箇所
12.0(29)S	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
15.0(1)M	このコマンドが、Cisco IOS Release 15.0(1)M よりも前のリリースに統合されました。

使用上のガイドライン

キー チェーンを選択するには、**iprsvpauthenticationkey-chain** コマンドを使用します。

（注） 同じルータ インターフェイスで **iprsvpauthenticationkey** コマンドと **iprsvpauthenticationkey-chain** コマンドを使用することはできません。これらのコマンドは相互排他的ですが、エラー メッセージは表示されません。

例

次の例は、RSVPkey にグローバルなデフォルト キー チェーンを設定する方法を示しています。

```
Router(config)# ip rsvp authentication key-chain RSVPkey
```

関連コマンド

コマンド	説明
iprsvpauthenticationkey	RSVP認証アルゴリズムのインターフェイス キー（文字列）を指定します。
showkeychain	認証キーの情報を表示します。

ip rsvp authentication lifetime

リソース予約プロトコル（RSVP）が他の RSVP ネイバーとセキュリティ アソシエーションを維持する時間を制御するには、インターフェイス コンフィギュレーション モードで **iprsvpauthenticationlifetime** コマンドを使用します。ライフタイム設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip rsvp authentication lifetime *hh* **:** *mm* **:** *ss*
no ip rsvp authentication lifetime *hh* **:** *mm* **:** *ss*

構文の説明

hh **:** *mm* **:** *ss*	信頼できる他の RSVP ネイバーとのセキュリティ アソシエーションを RSVP が維持する時間：分：秒。指定できる範囲は 1 秒～ 24 時間です。デフォルトは 30 分です。この構文にはコロンが必要です。

コマンド デフォルト

セキュリティ アソシエーションのライフタイムを指定しない場合は、30 分になります。

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	変更箇所
12.2(15)T	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

RSVP で信頼されたネイバーとのセキュリティアソシエーションを終了するタイミングを示すには、**iprsvpauthenticationlifetime** コマンドを使用します。アソシエーションのライフタイムが期限切れになっても、1 つ以上のライフタイムが有効であれば、その期間中に RSVP による認証メッセージは受信され、セキュリティアソシエーションのライフタイムが RSVP によって設定された値にリセットされます。ネイバーが RSVP シグナリング メッセージの送信を停止した（つまり最後の予約が解除された）場合、アソシエーションのライフタイム期間終了時と同様に、セキュリティ アソシエーションに使用されていたメモリが開放されます。RSVP ネイバーがシグナリングを再開した場合、アソシエーションを再作成できます。ライフタイムを短い期間に設定すると、有効期間が短い予約をルータが多数処理する場合に、メモリの回復が早くなります。ライフタイムを長い期間に設定すると、新しい認証予約を確立するときにルータのワークロードが低減されます。

ライフタイムの期限が切れる前にセキュリティ アソシエーションを開放するには、**cleariprsvpauthentication** コマンドを使用します。

例

次のコマンドは、ライフタイム期間を 30 分 5 秒に設定します。

```
Router(config-if)# ip rsvp authentication lifetime 00:30:05
```

関連コマンド

コマンド	説明
cleariprsvpauthentication	ライフタイムの期限が切れる前に RSVP セキュリティ アソシエーションを削除します。

ip rsvp authentication neighbor

ネイバーに対するリソース予約プロトコル（RSVP）暗号化認証を有効にするには、グローバル コンフィギュレーション モードで **iprsvpauthenticationneighbor** コマンドを使用します。ネイバーの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。

ip rsvp authentication neighbor {**access-list** *acl-name-or-number*|**address** *address*} **[challenge]** [**key-chain** *name*] [**type** {**md5**|**sha-1**}] [**window-size** *number-of-messages*]
no ip rsvp authentication neighbor {**access-list** *acl-name-or-number*|**address** *address*} **[challenge]** [**key-chain** *name*] [**type** {**md5**|**sha-1**}] [**window-size** *number-of-messages*]

構文の説明

access-list *acl-name-or-number*	このキーを共有するネイバーの IP アドレスが記述された標準の番号付きまたは名前付き IP アクセス リストを指定します。
address *address*	特定のネイバーの単一 IP アドレスを指定します。通常は、ネイバーの物理インターフェイスまたは論理（ループバック）インターフェイスのいずれかです。
challenge	（オプション）RSVP が既存のセキュリティ アソシエーションをメモリ内に持っていない RSVP ネイバーとのチャレンジレスポンス ハンドシェイクを RSVP で実行するよう要求します。
key-chain *name*	（オプション）ネイバーとの通信に使用されるキーのセットを含むキー チェーンの名前を指定します。
type	（オプション）RSVP メッセージに暗号化署名を生成するためのアルゴリズムを指定します。
md5	（オプション）RSA Message Digest 5（MD5）アルゴリズムを指定します。
sha-1	（オプション）米国国立標準技術研究所（NIST）の Secure Hash Algorithm-1 を指定します。これは、**md5** よりも新しく安全です。
window-size *number-of-messages*	（オプション）順序どおりでなくても受信できる認証済みメッセージの最大数を指定します。範囲は 1 ～ 64 です。デフォルト値は 1 です。

コマンド デフォルト

ネイバーの暗号化認証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	変更箇所
12.0(29)S	このコマンドが導入されました。
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。

リリース	変更箇所
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
15.0(1)M	このコマンドが、Cisco IOS Release 15.0(1)M よりも前のリリースに統合されました。

使用上のガイドライン

オプションのキーワードを省略すると、**iprsvpauthenticationneighbor** コマンドは、ネイバーの RSVP 暗号化認証を有効にします。オプションのキーワードを使用すると、グローバルデフォルトが継承されます。

ネイバーごとの認証を有効にするには、**iprsvpauthenticationneighbor** コマンド（または、認証を無効にするには、**noiprsvpauthenticationneighbor** コマンド）を発行する必要があります。**iprsvpauthentication** コマンドを、**neighbor** なしで発行する場合、このコマンドは、ネイバーごと、またはインターフェイスごとに定義されたキーの有無に関わらずすべてのネイバーおよびインターフェイスに対する認証を有効にします。**iprsvpauthenticationneighbor** コマンドを発行すると、認証はそのネイバーに対してのみ有効になります。

アクセス コントロール リスト

1 つの ACL で、特定のネイバーが RSVP メッセージをルータから受信するために使用する、すべての物理および論理インターフェイスを記述できます。これは、2 つのネイバー間に複数のルートが存在する場合に便利です。1 つの ACL で、自身のルータとともに多数の異なるネイバーを指定できます。ただし、これは一般的には、ネットワークのセキュリティ プラクティスとして優れているとは見なされません。

番号付きの場合、ACL は 1 ～ 99 の範囲内または 1300 ～ 1999 の範囲内になっている必要があり、合計 798 の番号付き ACL がネイバー キーを設定するために使用されます（一部は他の目的に使用されないことを想定）。標準の名前付き IP ACL の数に制限はありません。ACL で使用する IP アドレスには、少なくともネイバーの物理インターフェイス アドレスが含まれている必要があります。マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）を使用している場合などは、必要に応じて、ルータ ID アドレスを追加できます。

標準 ACL は送信元または宛先アドレスのみを処理しますが、拡張 ACL は 5 タプルを処理し、設定がより複雑なため、RSVP ネイバー用の名前付きまたは番号付き標準 IP ACL を作成するには、既存の **ipaccess-liststandard** コマンドを使用する必要があります。RSVP CLI は、標準以外の ACL を指定した場合にエラー メッセージを返します。

```
Router(config)# ip rsvp authentication neighbor access-list 10 key-chain wednesday
% Invalid access list name.
RSVP error: unable to find/create ACL
```

また、名前付き標準 IP ACL も推奨されます。ネイバー ルータのホスト名を ACL 名の一部として含めることができ、ルータ設定内でネイバーごとの ACL を識別しやすくなるためです。

有効な名前付きまたは番号付き ACL が指定されていても、存在しないか、または有効でないキー チェーンがその ACL に関連付けられている場合、RSVP CLI はエラー メッセージを表示します。キー チェーンがないと、そのネイバーが送受信する RSVP メッセージが破棄される可能性があるためです。

```
Router(config)# ip rsvp authentication neighbor access-list myneighbor key-chain xyz
RSVP error: Invalid argument(s)
```

キー チェーン

key-chainパラメータでは、キーは有効期限の昇順で使用されます。名前に関する唯一の制限として、スペースを含めることはできません。key-chainパラメータはオプションです。つまり、RSVP ネイバーに対する他のオプションの認証パラメータを変更しようとする場合には省略できます。ただし、キーを探す場合、期限切れでないキーを少なくとも 1 つ持つ、有効なキーチェーンを参照する key-chain パラメータが含まれていないと、RSVP は **iprsvpauthenticationneighboraccess-list** コマンドを無視します。

エラー状態と警告状態

RSVP CLI は、RSVP にすでに割り当てられた他のチェーン内のキー ID と重複するチェーン内のキー ID があった場合、次の例のようにエラーを返します。

```
Router(config)# ip rsvp authentication neighbor access-list myneighbor key-chain abc
RSVP error: key chains abc and xyz contain duplicate key ID 1
RSVP error: Invalid argument(s)
```

指定されたキーチェーンが存在しないか、少なくとも1つの期限切れでないキーが含まれていない場合、RSVP CLI は、エラーを返します。

キーチェーンが適切に定義され、RSVPが後からそのネイバーにメッセージを送信しようとしても、有効かつ期限切れでないネイバーごとまたはインターフェイスごとのキーを見つけられない場合、RSVP は RSVP_AUTH_NO_KEYS_LEFT システム メッセージを生成し、そのネイバーのキーが取得できなかったことを示します。

キー チェーンが有限の期限切れ時間を持つキーを含んでいる場合、RSVP は RSVP_AUTH_ONE_KEY_EXPIREDメッセージを生成して各キーが期限切れになったタイミングを示します。

RSVP が誤ったダイジェスト タイプを持つネイバーからメッセージを受信した場合、RSVP は RSVP_MSG_AUTH_TYPE_MISMATCH システム メッセージを生成し、そのネイバーと不一致のダイジェスト タイプがあることを示します。

すでにウィンドウ内にあるか、またはウィンドウ外にある重複メッセージをRSVPが受信した場合、RSVP は BAD_RSVP_MSG_RCVD_AUTH_DUP または BAD_RSVP_MSG_RCVD_AUTH_WIN エラー メッセージをログに記録し、メッセージのシーケンス番号が無効であることを示します。

ネイバーのチャレンジが失敗したか、またはタイムアウトになった場合、RSVP は BAD_RSVP_MSG_RCVD_AUTH_COOKIE システムメッセージ、または RSVP_MSG_AUTH_CHALLENGE_TIMEOUTメッセージを生成し、指定されたネイバーがチャレンジに対して正しく応答することに失敗したことを示します。

例

次の例は、ネイバー V、Y、および Z に対するアクセス リストとキー チェーンを作成し、他のすべての認証パラメータに対して継承を使用して認証をグローバルに有効にする方法を示しています。

```
Router# configure terminal
Router(config)# ip access-list standard neighbor_V
Router(config-std-nacl)# permit 10.0.0.2
Router(config-std-nacl)#
permit 10.1.16.1
Router(config-std-nacl)# exit
Router(config)# ip access-list standard neighbor_Y
Router(config-std-nacl)# permit 10.0.1.2
Router(config-std-nacl)# permit 10.16.0.1
Router(config-std-nacl)# exit
Router(config)# ip access-list standard neighbor_Z
Router(config-std-nacl)# permit 10.16.0.2
Router(config-std-nacl)# permit 10.1.0.2
Router(config-std-nacl)# permit 10.0.1.2
Router(config-std-nacl)#
exit
Router(config)# ip rsvp authentication neighbor access-list neighbor_V key-chain neighbor_V
Router(config)# ip rsvp authentication neighbor access-list neighbor_Y key-chain neighbor_Y
Router(config)# ip rsvp authentication neighbor access-list neighbor_Z key-chain neighbor_Z
Router(config)# ip rsvp authentication
Router(config)# end
```

次の例は、ネイバー V、Y、および Z に対するアクセス リストとキー チェーンを作成し、各ネイバーに対して明示的に認証を有効にする方法を示しています。

```
Router(config)# ip rsvp authentication neighbor access-list neighbor_V key-chain neighbor_V
Router(config)# ip rsvp authentication neighbor access-list neighbor_V
Router(config)# ip rsvp authentication neighbor access-list neighbor_Y key-chain neighbor_Y
Router(config)# ip rsvp authentication neighbor access-list neighbor_Y
Router(config)# ip rsvp authentication neighbor access-list neighbor_Z key-chain neighbor_Z
Router(config)# ip rsvp authentication neighbor access-list neighbor_Z
Router(config)#
end
```

関連コマンド

コマンド	説明
iprsvpauthentication	RSVP暗号化認証を有効にします。

ip rsvp authentication type

リソース予約プロトコル（RSVP）メッセージで暗号化署名を生成するために使用するアルゴリズムのタイプを指定するには、インターフェイス コンフィギュレーション モードまたはグローバル コンフィギュレーション モードで **iprsvpauthenticationtype** コマンドを使用します。どのようなタイプのアルゴリズムも使用しないよう指定するには、このコマンドの **no** 形式を使用します。設定からタイプを削除するには、このコマンドの **default** 形式を使用します。

（注） **noiprsvpauthenticationtype** コマンドを使用する前に、詳細については、「使用上のガイドライン」のセクションを参照してください。

T リリースの構文
ip rsvp authentication type {md5|sha-1}
no ip rsvp authentication type
default ip rsvp authentication type

12.0S および 12.2S リリースの構文
ip rsvp authentication type {md5|sha-1}
default ip rsvp authentication type

構文の説明

md5	RSA Message Digest 5 アルゴリズム。
sha-1	米国国立標準技術研究所（NIST）の Secure Hash Algorithm-1。これは、MD5 よりも新しく安全です。

コマンド デフォルト

アルゴリズムが指定されない場合、**md5** が使用されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）
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	変更箇所
12.2(15)T	このコマンドが導入されました。
12.0(29)S	このコマンドが、すべてのネイバーのグローバル コンフィギュレーション モードで導入されました。このコマンドの **default** 形式が追加されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

アルゴリズムを指定してRSVPメッセージの暗号化署名を生成するには、**iprsvpauthenticationtype** コマンドを使用します。アルゴリズムを指定しない場合は、**md5** が使用されます。

iprsvpauthenticationneighbortype コマンドではなく **iprsvpauthenticationtype** コマンドを使用する場合、タイプのグローバル デフォルトが変更されます。

事前定義済みの

Cisco IOS T リリースでは、**noiprsvpauthenticationtype** コマンドがサポートされますが、**defaultiprsvpauthenticationtype** コマンドをお勧めします。**toremovetheauthenticationtypefromaconfigurationandforcethetypetoitsdefault.**

例

T リリースの例

次の例は、interf**aceauthentication** に対してタイプを sha-1 に設定する方法を示しています。

```
Router(config-if)# ip rsvp authentication type sha-1
```

12.0S および 12.2S リリースの例

次の例は、ネイバーの認証に対してタイプを sha-1 に設定する方法を示しています。**ghborauthentication:**

```
Router(config)# ip rsvp authentication neighbor address 10.1.1.1 type sha-1
```

または

```
Router(config)# ip rsvp authentication neighbor access-list 1 type sha-1
```

次の例は、グローバルデフォルト タイプを**sha-1forauthentication** に設定する方法を示しています。

```
Router(config)# ip rsvp authentication type sha-1
```

default コマンドの例

次の例は、設定からタイプを削除し、タイプをデフォルトに強制する方法を示しています。

```
Router(config)# default ip rsvp authentication type
```

関連コマンド

コマンド	説明
iprsvpauthenticationkey	RSVP認証アルゴリズムのキー（文字列）を指定します。

コマンド	説明
iprsvpauthenticationneighbortype	特定のネイバーのタイプを設定します。

ip rsvp authentication window-size

順序どおりでなくても受信できるリソース予約プロトコル（RSVP）認証済みメッセージの最大数を指定するには、インターフェイス コンフィギュレーション モードで **iprsvpauthenticationwindow-size** コマンドを使用します。ウィンドウ サイズを無効にする（またはデフォルト値の 1 を使用する）場合は、このコマンドの **no** 形式を使用します。

ip rsvp authentication window-size [*number-of-messages*]
no ip rsvp authentication window-size

構文の説明

number-of-messages	（オプション）順序どおりでなくても受信できる認証済みメッセージの最大数。指定できる範囲は 1 ～ 64 で、デフォルト値は 1 です。

コマンド デフォルト

ウィンドウ サイズが指定されない場合は、値 1 が使用されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.2(15)T	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

順序どおりでなくても受信できる RSVP 認証済みメッセージの最大数を指定するには、**iprsvpauthenticationwindow-size** コマンドを使用します。すべての RSVP 認証済みメッセージには、RSVP メッセージの再送を防止するためのシーケンス番号が付けられています。

1 つのメッセージに設定されたデフォルト ウィンドウ サイズの場合、重複する認証済みメッセージはリプレイ アタックと見なされるため、このようなメッセージは拒否されます。ただし、場合によっては、RSVP メッセージのバーストが RSVP ネイバー間で並べ替えられることがあります。この事象が定期的に発生し、メッセージのバーストを送信しているノードの信頼性を確認できる場合は、**iprsvpauthenticationwindow-size** コマンド オプションを使用して、再編成されたバーストが RSVP によって廃棄されないようにバースト サイズを変更してください。RSVP は、これらのバースト内の重複メッセージもチェックします。

例

次の例は、ウィンドウ サイズを 2 に設定する方法を示しています。

```
Router(config-if)# ip rsvp authentication window-size 2
```

関連コマンド

コマンド	説明
iprsvpauthentication	RSVP暗号化認証を有効にします。

ip rsvp bandwidth

IPに対するリソース予約プロトコル（RSVP）をインターフェイスで有効にするには、インターフェイス コンフィギュレーション モードで **ip rsvp bandwidth** コマンドを使用します。RSVPを完全に無効にするには、このコマンドの **no** 形式を使用します。

Cisco IOS Release 15.1(2)T 以降のリリース用の構文

ip rsvp bandwidth [*interface-bandwidth* [{**percent** *percent-bandwidth*|[*single-flow-bandwidth*] [**sub-pool** *bandwidth*]}] [**ingress** [{*ingress-bandwidth*|**percent** *percent-bandwidth* [{*maximum-ingress-bandwidth*|**percent** *percent-bandwidth*}]}]]]
no ip rsvp bandwidth

Cisco IOS Release 12.0S および 12.2S、Cisco IOS XE Release 2.6、および以降のリリースの構文

{**ip rsvp bandwidth** [**rdm** [**bc0** *interface-bandwidth*]] [*single-flow-bandwidth* [{**bc1** *bandwidth*|**sub-pool** *bandwidth*}]] [*interface-bandwidth* [*single-flow-bandwidth* [{**bc1** *bandwidth*|**sub-pool** *bandwidth*}]]]|**mam max-reservable-bw** [*interface-bandwidth* [*single-flow-bandwidth*] [**bc0** *interface-bandwidth* [**bc1** *bandwidth*]]]|**percent** *percent-bandwidth* [*single-flow-bandwidth*]}
{**no ip rsvp bandwidth** [**rdm** [**bc0** *interface-bandwidth*]] [*single-flow-bandwidth* [{**bc1** *bandwidth*|**sub-pool** *bandwidth*}]] [*interface-bandwidth* [*single-flow-bandwidth* [{**bc1** *bandwidth*|**sub-pool** *bandwidth*}]]]|**mam max-reservable-bw** [*interface-bandwidth* [*single-flow-bandwidth*] [**bc0** *bc0-pool* [**bc1** *bandwidth*]]]|**percent** *percent-bandwidth* [*single-flow-bandwidth*]}

構文の説明

interface-bandwidth	（オプション）RSVPフローが割り当て可能な帯域幅の最大量（kbps単位）。範囲は 1 ～ 10000000 です。
percent *percent-bandwidth*	（オプション）インターフェイス帯域幅のパーセンテージを指定します。範囲は 1 ～ 1000 です。 • **ingress** キーワードとともに使用すると、**percent** キーワードはRSVP入力帯域幅として設定されるインターフェイスの帯域幅のパーセンテージを指定します。
single-flow-bandwidth	（オプション）1つのフローで割り当てることができる帯域幅の最大量（kbps）。範囲は 1 ～ 10000000 です。 （注） この値は、DiffServ 認識型マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング機能によって無視されます。

sub-pool *bandwidth*	（オプション）インターフェイスで全体の一部として予約される帯域幅の量（kbps）を指定します。範囲は、1 から *interface-bandwidth* 引数と **rdm** *bandwidth* 引数のどちらか小さい方の値までです。このキーワードと引数のペアは、Diffserv 認識型トラフィック エンジニアリング（DS-TE）の従来（IETF 標準以前）の実装で使用されています。
ingress	（任意）RSVP 入力予約可能帯域幅を設定します。
ingress-bandwidth	（オプション）入力予約可能帯域幅（kbps）。範囲は 1 ～ 10000000 です。
maximum-ingress-bandwidth	（オプション）1 つのフローで割り当てることができる入力帯域幅の最大量（kbps）。範囲は 1 ～ 10000000 です。ただし、設定できる値は、プールに残っている帯域幅の量によって決まります。
rdm	（オプション）DS-TE に Russian Doll Model（RDM）を指定します。
bc0 *interface-bandwidth*	（オプション）全体（以前の「グローバル プール」）に対してインターフェイスで予約される帯域幅の量（kbps）。範囲は、1 から **max-reservable-bw***interface-bandwidth* キーワードと引数のペアの値。
bc1 *bandwidth*	（オプション）**bc0** *interface-bandwidth* と同じ帯域幅の部分を指定します。つまり、インターフェイスで全体の一部に対して予約される帯域幅の量（kbps）です。
mam	（オプション）DS-TE に Maximum Allocation Model（MAM）を指定します。
max-reservable-bw	（オプション）最大予約帯域幅を指定し、合計プールのサイズに制限を設定します。
bc1 *bandwidth*	（オプション）インターフェイスで全体の一部として予約される帯域幅の量（kbps）を指定します。（以前、この部分は「サブプール」と呼ばれていました。）範囲は、1 から **max-reservable-bw***interface-bandwidth* キーワードと引数の値。

コマンド デフォルト

RSVP はデフォルトで無効になっています。帯域幅値を入力せずに **ip rsvp bandwidth** コマンドを入力した（たとえば、**ip rsvp bandwidth** の後に Enter キーを押した）場合、デフォルトの帯域幅値（つまり、リンク帯域幅の 75 %）が *interface-bandwidth* 引数と *single-flow-bandwidth* 引数に想定されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
12.0(11)ST	このコマンドが Cisco IOS Release 12.0(11)ST に統合されました。**sub-pool** キーワードが追加されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(18)SXD	このコマンドが、Cisco IOS リリース 12.2(18)SXD に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
12.2(33)SRB	このコマンドが変更されました。DS-TE 用 IETF 標準が、**rdm** および **mam** キーワード、および補助引数を介して追加されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。
15.1(2)T	このコマンドが変更されました。**percent***percent-bandwidth* キーワードと引数の組み合わせが追加されました。
15.(1)3T	このコマンドが変更されました。**ingress** キーワード、*ingress-bandwidth* 引数、および *maximum-ingress-bandwidth* 引数が追加されました。
15.2(3)T	このコマンドが変更されました。IPv6 のサポートが追加されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

RSVP は、distributed Cisco Express Forwarding（dCEF; 分散型シスコ エクスプレス フォワーディング）で設定できません。

RSVP は、RSVP を実装しないシステムとの後方互換性を提供できるように無効になっています。

重み付けランダム早期検出（WRED）または均等化キューイングを最初に有効にします。

このコマンドを DS-TE の IETF 標準モードで使用する場合、**rdm** およびその引数または **mam** およびその引数のいずれかを使用する必要があり、両方は使用できません。各選択肢の詳細については、『*Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*』（F. Le Faucheur 著）（RFC 4127）および『*Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*』（F. Le Faucheur and W. Lai 著）（RFC 4125）を参照してください。

帯域幅のサブプール部分のみを削除するには、このコマンドの **no** 形式を、**sub-pool** キーワードとともに使用します。

入力コール アドミッション制御（CAC）を有効にするには、**ip rsvp bandwidth ingress** コマンドを使用します。インターフェイスの入力 CAC 機能を無効にするには、**no ip rsvp bandwidth**

コマンドを使用します。ただし、このコマンドはまた、インターフェイスのRSVPを無効にします。インターフェイスの入力機能のみを無効にするには、**ip rsvp bandwidth** *interface-bandwidth single-flow-bandwidth* コマンドを使用します。

ip rsvp bandwidth コマンドに関連するすべての設定は、IPv4 セッションと IPv6 セッションの両方に適用可能です。IPv4 セッションと IPv6 セッションは、共通の帯域幅プールに十分な帯域幅がある場合にのみ許可されます。IPv4 予約と IPv6 予約に、別々の帯域幅制限を適用することはできません。

例

次の例は、シリアル インターフェイス 0 で、最大 1158 kbps の RSVP 予約を許可するが、どのようなフローに対しても 100 kbps 未満しか許可しないように設定された T1（1536 kb/秒）リンクを示します。均等化キューイングは 15 の予約可能なキューを使用して設定し、予約されたフローをサポートします（必要な場合）。

```
Device(config)# interface serial 0
Device(config-if)# fair-queue 64 256 15
Device(config-if)# ip rsvp bandwidth 1158 100
```

関連コマンド

Command	Description
fair-queue(WFQ)	インターフェイスに対する WFQ を有効にします。
iprsvpneighbor	ネイバーによる予約の要求を有効にします。
iprsvpreservation	RSVP RESV メッセージを受信および転送しているようにデバイスの動作を設定します。
iprsvpsender	RSVP PATH メッセージを受信および転送しているようにデバイスの動作を設定します。
iprsvpudp-multicasts	デバイスが IP カプセル化マルチキャスト パケットを生成するときはいつでも、UDP カプセル化済み RSVP マルチキャストを生成するようにルータに指示します。
random-detect(interface)	WRED または DWRED をイネーブルにします。
showiprsvpinstalled	RSVP 関連のインストールされているフィルタと対応する帯域幅情報を表示します。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。
showiprsvpneighbor	現在の RSVP ネイバーを表示します。
showiprsvpreservation	現在データベースに格納されている RSVP 関連の受信側情報を表示します。
showiprsvpsender	現在データベース上に存在する RSVP PATH 関連の送信側情報を表示します。

ip rsvp bandwidth ignore

リソース予約プロトコル（RSVP）トンネル帯域幅設定を無視するには、インターフェイス コンフィギュレーション モードで **iprsvpbandwidthignore** コマンドを使用します。

ip rsvp bandwidth ignore

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

RSVP トンネル帯域幅設定が使用されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
15.1(2)T	このコマンドが導入されました。
15.1(1)S	このコマンドが、Cisco IOS Release 15.1(1)S に統合されました。

使用上のガイドライン

iprsvpbandwidthignore コマンドを使用して、トンネルの任意の RSVP 帯域幅設定を無視できます。RSVP 帯域幅を再設定する必要がある場合、**iprsvpbandwidth** または **iprsvpbandwidthpercent** コマンドを使用します。

例

次の例は、トンネル インターフェイスで RSVP 帯域幅設定を無視する方法を示しています。

```
Router(config)# interface tunnel 1
Router(config-if)# ip rsvp bandwidth ignore
```

関連コマンド

コマンド	説明
iprsvpbandwidth	インターフェイスで IP 用 RSVP をイネーブルにします。
iprsvpbandwidthpercent	インターフェイスで IP 用の RSVP をイネーブルにし、RSVP 帯域幅プールで使用できるインターフェイスの合計帯域幅の割合を指定します。
showiprsvpinterfacedetail	すべてのインターフェイスの hello 設定を表示します。

ip rsvp bandwidth percent

インターフェイスの IP に対してリソース予約プロトコル（RSVP）を有効にし、RSVP の利用可能な帯域幅のパーセンテージと 1 つのフローの帯域幅プールを設定するには、インターフェイス コンフィギュレーション モードで **iprsvpbandwidthpercent** コマンドを使用します。インターフェイスで RSVP 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 rsvp bandwidth percent *interface-bandwidth* [{*max-flow-bw*|**percent** *flow-bandwidth*}]
no ip rsvp bandwidth

構文の説明

interface-bandwidth	RSVPに対して設定されたインターフェイス帯域幅のパーセンテージ。範囲は 1 ～ 1000 です。
max-flow-bw	（オプション）1 つのフローに対する最大帯域幅（kb/秒）。範囲は 1 ～ 10000000 です。ただし、設定できる値は、プールに残っている帯域幅の量によって決まります。
percent *flow-bandwidth*	（オプション）フローの帯域幅として使用する帯域幅のパーセンテージを指定します。範囲は 1 ～ 1000 です。

コマンド デフォルト

RSVP は、デフォルトで無効になっています。したがって、帯域幅のパーセンテージは設定されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。
15.1(2)T	このコマンドが変更されました。**percent** および *flow-bandwidth* キーワードと引数の組み合わせが追加されました。

使用上のガイドライン

RSVP は、distributed Cisco Express Forwarding（dCEF; 分散型シスコ エクスプレス フォワーディング）で設定できません。

RSVP は、RSVP を実装しないシステムとの後方互換性を提供できるように無効になっています。

重み付けランダム早期検出（WRED）または均等化キューイングを最初に有効にします。

RSVP 帯域幅プールを、インターフェイスの帯域幅の指定されたパーセンテージに設定するには、**iprsvpbandwidthpercent** コマンドを使用します。**iprsvpbandwidthpercent** コマンドを発行すると、インターフェイスの帯域幅の変化に応じて、RSVP 帯域幅プールは動的に調整されます。

インターフェイスの帯域幅のあるパーセンテージを RSVP 帯域幅として設定するには、**iprsvpbandwidthpercent***percent-bandwidth***percent***flow-bandwidth* コマンドを使用できます。RSVP 帯域幅は、RSVP コネクション アドミッション制御（CAC）に使用されます。このコマンドは、オーバーサブスクリプションを許可します。つまり、100% を超えるインターフェイスの帯域幅が RSVP 帯域幅として、およびフローごとの帯域幅として使用されるように設定できます。

バンドルのメンバー リンクで **iprsvpbandwidth***rsvp-bandwidth* コマンドを使用し、RSVP に使用される帯域幅の量として絶対値を設定するように選択できます。**iprsvpbandwidthpercent***rsvp-bandwidth* コマンドを使用すると、RSVP 帯域幅は、インターフェイスの帯域幅の変化と並行して変化するようになります。バンドルの RSVP 帯域幅は、バンドル インターフェイスの帯域幅にのみ依存します。このバンドル インターフェイスはさらに、メンバー リンクの RSVP 帯域幅ではなく、インターフェイス帯域幅に依存します。

iprsvpbandwidthpercent コマンドは、RSVP 帯域幅の動的更新がサポートされていないインターフェイスではブロックされます。サポートされていないインターフェイスで RSVP クライアントが **iprsvpbandwidthpercent** コマンドを設定しようとすると、デバッグ メッセージが表示されます。

Cisco IOS Release 15.1(2)T では、**iprsvpbandwidthpercent** コマンドは、Multilevel Precedence and Preemption（MLPP）およびマルチリンク フレーム リレー（MFR）インターフェイスでサポートされています。

例

次の例は、シリアル インターフェイス 0 で、インターフェイスの帯域幅の 90% まで RSVP 予約を許容するが、どのようなフローに対しても 1000 kb/秒までしか許可しないように設定されたシリアル リンクを示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface serial 0
Router(config-if)# ip rsvp bandwidth percent 90 1000
```

次の例は、マルチリンク インターフェイス 2 で、インターフェイスの帯域幅の 50% まで RSVP 帯域幅として許容し、どのようなフロー帯域幅に対しても 10% までしか許可しないように設定されたマルチリンクを示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface multilink 2
Router(config-if)# ip rsvp bandwidth percent 50 percent 10
Router(config-if)#
exit
```

関連コマンド

Command	Description
fair-queue(WFQ)	インターフェイスに対する WFQ を有効にします。
iprsvpbandwidth	インターフェイスで IP 用 RSVP をイネーブルにします。
iprsvpneighbor	ネイバーによる予約の要求を有効にします。

Command	Description
iprsvpreservation	RSVP RESV メッセージを受信および転送しているようにルータの動作を設定します。
iprsvpsender	RSVP PATH メッセージを受信および転送しているようにルータの動作を設定します。
iprsvpudp-multicasts	ルータが IP カプセル化マルチキャスト パケットを生成するときはいつでも、UDP カプセル化済み RSVP マルチキャストを生成するようにルータに指示します。
random-detect(interface)	WRED または DWRED をイネーブルにします。
showiprsvpinstalled	RSVP 関連のインストールされているフィルタと対応する帯域幅情報を表示します。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。
showiprsvpneighbor	現在の RSVP ネイバーを表示します。
showiprsvpreservation	現在データベースに格納されている RSVP 関連の受信側情報を表示します。
showiprsvpsender	現在データベース上に存在する RSVP PATH 関連の送信側情報を表示します。

ip rsvp burst policing

インターフェイスごとでリソース予約プロトコル（RSVP）トークンバケットポリシング機能内のバースト係数を設定するには、インターフェイス コンフィギュレーション モードで、**iprsvpburstpolicing** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ip rsvp burst policing [*factor*]
no ip rsvp burst policing

構文の説明

factor	（オプション）受信者の要求されたバーストのパーセンテージとしてバースト係数値を示します。

コマンド デフォルト

デフォルト値は 200、最小値は 100、最大値は 700 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(3)T	このコマンドが導入されました。
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。

使用上のガイドライン

フローごとではなくインターフェイスごとのバーストポリシング係数を設定します。バースト係数は、バーストに関して、送信者のトラフィックをどれくらい厳しくまたは緩くポリシングするかを制御します。

バースト係数は、特定のインターフェイスにインストールされているすべての RSVP フローに適用されます。バーストのポリシング用に各インターフェイスを個別に設定できます。

例

次の例は、バースト係数 200 の **iprsvpburstpolicing** コマンドを示しています。

```
ip rsvp burst policing 200
```

ip rsvp data-packet classification none

リソース予約プロトコル（RSVP）データ パケット分類をオフ（無効）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 **iprsvpdata-packetclassificationnone** コマンドを使用する必要があります。データ パケット分類をオン（有効）にするには、このコマンドの **no** 形式を使用します。

ip rsvp data-packet classification none
no ip rsvp data-packet classification none

構文の説明

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

RSVP データ パケット分類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	変更箇所
12.2(2)T	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(18)SXF2	このコマンドが、Cisco IOS Release 12.2(18)SXF2 に統合されました。
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。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

RSVP がすべてのパケットを処理しないようにするには、**iprsvpdata-packetclassificationnone** コマンドを使用します。すべてのパケットが処理されないように RSVP を設定すると、オーバーヘッドがなくなり、ネットワークのパフォーマンスとスケーラビリティが向上します。

例

このセクションには、**iprsvpdata-packetclassificationnone** コマンドの 2 つの例が記載されています。最初の例は、データ パケット分類をオフ（無効）にする方法を示します。

```
Router# configure terminal
Router(config)# interface atm 6/0
Router(config-if)# ip rsvp data-packet classification none
```

次の例は、データ パケット分類をオン（有効）にする方法を示します。

```
Router# configure terminal
Router(config)# interface atm 6/0
Router(config-if)# no ip rsvp data-packet classification none
```

関連コマンド

コマンド	説明
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。

ip rsvp dsbm candidate

インターフェイスを Designated Subnetwork Bandwidth Manager（DSBM）候補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 **iprsvpdsbmcandidate** コマンドを使用します。インターフェイスで DSBM を無効にして、インターフェイスを DSBM 候補から除外するには、このコマンドの **no** 形式を使用します。

ip rsvp dsbm candidate [*priority*]
no ip rsvp dsbm candidate

構文の説明

priority	（任意）64 ～ 128 の範囲の値です。DSBM 候補者の中で、最も優先順位の高い番号のインターフェイスが DSBM 選択プロセスで選ばれます。

コマンド デフォルト

インターフェイスは、デフォルトでは DSBM 候補として設定されていません。このコマンドを使用してインターフェイスを DSBM 候補として有効にし、優先順位を指定しない場合は、デフォルトの優先順位である 64 と見なされます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.1(1)T	このコマンドが Cisco IOS Release 12.1(1)T に統合されました。
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。

使用上のガイドライン

セグメントのリソースを管理できる SBM プロトコル エンティティは、レイヤ 2 またはレイヤ 3 のデバイスに置くことができます。多くの SBM 対応デバイスは、共有レイヤ 2 セグメントにアタッチできます。指定されたセグメント上に複数の SBM が存在する場合は、いずれかの SBM が DSBM に選ばれます。選ばれた DSBM は、プロセスで管理対象セグメントとなるセグメントでのリソース予約の要求に対して、アドミッション コントロールを実行する役割を担います。管理対象セグメントには、DSBM によって分離されない共有 LAN の相互接続部分が含まれます。どのような場合でも、各レイヤ 2 セグメントに存在する DSBM は 1 つだけです（存在する場合）。

DSBM 優先順位が 64 ～ 128 の範囲になるようにインターフェイスを設定できます。セグメントでの DSBM 選択に参加しないようにインターフェイスを除外できますが、そのセグメントに DSBM が存在する場合、システムは DSBM と対話できます。つまり、DSBM 選択プロセスに候補として参加するようにインターフェイスを設定していない場合でも、管理対象セグメン

トに接続されたルータのリソース予約プロトコル（RSVP）対応インターフェイスを DSBM で管理できます。インターフェイスを DSBM 候補から除外するには、そのインターフェイスで **iprsvpdsbmcandidate** コマンドを発行しないようにします。

RSVP は、Versatile Interface Processor（VIP）分散型シスコ エクスプレス フォワーディング（dCEF）で設定できません。

例

次に、イーサネット インターフェイス 2 を優先順位 100 で DSBM 候補として設定する例を示します。

```
interface Ethernet2
 ip rsvp dsbm candidate 100
```

関連コマンド

コマンド	説明
debugiprsvp	SBM メッセージ処理、DSBM 選択プロセス、および標準 RSVP 対応メッセージ処理情報に関する情報を表示します。
debugiprsvpdetail	RSVP と SBM に関する詳細情報を表示します。
debugiprsvpdetailsbm	SBM メッセージのみに関する詳細情報と、SBM と DSBM の状態遷移を表示します。
iprsvpdsbmnon-resv-send-limit	NonResvSendLimit オブジェクト パラメータを設定します。
showiprsvpsbm	ルータ上の特定の RSVP 対応インターフェイスまたはすべての RSVP 対応インターフェイス用に設定された SBM に関する情報を表示します。

ip rsvp dsbm non-resv-send-limit

NonResvSendLimit オブジェクト 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 **iprsvpdsbmnon-resv-send-limit** コマンドを使用します。デフォルトの NonResvSendLimit オブジェクト パラメータを使用するには、このコマンドの **no** 形式を使用します。

ip rsvp dsbm non-resv-send-limit {**rate** *kbps*|**burst** *kilobytes*|**peak** *kbps*|**min-unit** *bytes*|**max-unit** *bytes*}
no ip rsvp dsbm non-resv-send-limit {**rate** *kbps*|**burst** *kilobytes*|**peak** *kbps*|**min-unit** *bytes*|**max-unit** *bytes*}

構文の説明

rate *kbps*	Designated Subnetwork Bandwidth Manager（DSBM）候補の平均レート（kbps 単位）。平均レートは、1 ～ 2147483 までの番号です。
burst *kilobytes*	DSBM 候補の最大バースト サイズ（kb 単位）。最大バースト サイズは、1 ～ 2147483 までの番号です。
peak *kbps*	DSBM 候補のピーク レート（kBps 単位）。ピーク レートは、1 ～ 2147483 までの番号です。
min-unit *bytes*	DSBM候補の最小ポリシング済みユニット（バイト単位）。最小ポリシング済みユニットは、1 ～ 2147483647 までの番号です。
max-unit *bytes*	DSBM 候補の最大パケット サイズ（バイト単位）。最大パケット サイズは、1 ～ 2147483647 までの番号です。

コマンド デフォルト

rate、**burst**、**peak**、**min-unit**、および **max-unit** キーワードのデフォルトは無制限です。有効なリソース予約プロトコル（RSVP）予約なしに、すべてのトラフィックを送信できます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.1(1)T	このコマンドが導入されました。
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。

使用上のガイドライン

有効なRSVP予約なしで送信できるトラフィックの量に対してフロー単位の制限を設定するには、**rate**、**burst**、**peak**、**min-unit**、および **max-unit** の値を 0 よりも大きい有限値に設定します。

有効な RSVP 予約なしですべてのトラフィックが送信されるようにするには、**rate**、**burst**、**peak**、**min-unit**、および **max-unit** の値を無制限のトラフィック用に設定します。無制限のトラフィック用にパラメータを設定するには、コマンドを省略するか、コマンドの **no** 形式を入力します（**noiprsvpdsbmnon-resv-send-limitrate** など）。デフォルト値は無制限です。

NonResvSendLimit オブジェクトがない場合、有効な RSVP 予約がない状態で、任意の量のトラフィックを送信できます。

RSVP は、VIP 分散型シスコ エクスプレス フォワーディング（dCEF）で設定できません。

例

次の例では、優先順位 100、平均レート 500 kBps、最大バースト サイズ 1000 KB、ピーク レート 500 kBps、最小および最大パケット サイズ無制限の DSBM 候補として、イーサネット インターフェイス 2 を設定します。

```
interface Ethernet2
 ip rsvp dsbm candidate 100
 ip rsvp dsbm non-resv-send-limit rate 500
 ip rsvp dsbm non-resv-send-limit burst 1000
 ip rsvp dsbm non-resv-send-limit peak 500
```

関連コマンド

Command	Description
iprsvpdsbmcandidate	インターフェイスを DSBM 候補として設定します。
showiprsvpsbm	ルータ上の特定の RSVP 対応インターフェイスまたはすべての RSVP 対応インターフェイス用に設定された SBM に関する情報を表示します。

ip rsvp flow-assist

リソース予約プロトコル（RSVP）を有効にして、フロー分類、ポリシング、およびマーキングのために Cisco Express Forwarding（CEF）パスと統合するには、インターフェイス コンフィギュレーション モードで **iprsvpflow-assist** コマンドを使用します。この目的のための RSVP と CEF の統合を無効にするには、**iprsvpdata-packetclassificationnone** コマンドを使用します。

ip rsvp flow-assist

構文の説明

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

このコマンドはデフォルトでオンになっており、データ パケットの分類、ポリシング、およびマーキングのために RSVP が CEF と統合されます。

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	変更箇所
12.0(3)T	このコマンドが導入されました。
12.4	このコマンドの動作が変更されました。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。
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。

使用上のガイドライン

予約済みフローのデータ パケットをポリシングおよびマーキングするために、RSVP は基礎となるパケット転送メカニズム（CEF）と対話する必要があります。

Cisco IOS リリース 12.4 で、**iprsvpflow-assist** コマンドの **no** 形式がサポートされなくなりました。既存の **iprsvpdata-packetclassificationnone** コマンドを使用して、データ パケットを処理するためのメカニズムとの RSVP の統合を無効にできるためです。

例

次に、ATM インターフェイス 2/0/0 で RSVP を有効にする例を示します。

```
interface atm2/0/0
 ip rsvp flow-assist
```

関連コマンド

Command	Description
iprsvpdata-packetclassificationnone	RSVP とデータ プレーンを統合しないようにします。

Command	Description
iprsvpprecedence	RSVP フロースペックに適合するパケットまたは RSVP フロースペックを超過するパケットに適用する IP プレシデンス値を設定できます。
iprsvpsvc-required	インターフェイスまたはサブインターフェイスで行われる新しいRSVP予約にサービスを提供するため、SVCの作成を有効にします。
iprsvptos	RSVP フロースペックに適合するパケットまたは RSVP フロースペックを超過するパケットに適用するToS値を設定できます。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。

ip rsvp layer2 overhead

フローがATM相手先固定接続（PVC）で許可されたときにリソース予約プロトコル（RSVP）/重み付け均等化キューイング（WFQ）によって実行されるオーバーヘッドアカウンティングを制御するには、インターフェイス コンフィギュレーション モードで **iprsvplayer2overhead** コマンドを使用します。オーバーヘッド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。

ip rsvp layer2 overhead [*h c n*]
default ip rsvp layer2 overhead
no ip rsvp layer2 overhead [*h c n*]

構文の説明

h	（任意）各レイヤ 3 パケットに適用されるレイヤ 2 カプセル化ヘッダーとトレーラ サイズ（バイト単位）です。有効なサイズは、0 ～ 65535 までの番号です。
c	（任意）各レイヤ2セルに適用されるレイヤ2セルヘッダーのサイズ（バイト単位）です。有効なサイズは、0 ～ 65535 までの番号です。
n	（任意）レイヤ 2 ペイロード サイズ（バイト単位）です。有効なサイズは、0 ～ 65534 までの番号です。

コマンド デフォルト

このコマンドは、RSVP および WFQ を実行している ATM インターフェイスでは、デフォルトで有効になっています。非 ATM インターフェイスでもこのコマンドを使用できます。

このコマンドのデフォルト バージョンである **defaultiprsvplayer2overhead**、またはパラメータ（*h*、*c*、および *n*）を省略した **iprsvplayer2overhead** コマンドを入力すると、RSVP によりインターフェイス/PVC カプセル化に基づいてオーバーヘッド値が自動的に決定されます。（現在、RSVP は ATM アダプテーション層 5（AAL5）サブネットワーク アクセス プロトコル（SNAP）と MUX（マルチプレクサ）のカプセル化を認識します）。

非 ATM/PVC インターフェイスでは、設定された *h*、*c*、および *n* パラメータによって、RSVP によりオーバーヘッドに使用される値が決定されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.2(2)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

IP フローがリンクを通過すると、レイヤ2カプセル化のオーバーヘッドにより、フローがアドバタイズされた（レイヤ 3）レートを超えるために必要な帯域幅の量が増える可能性があります。

多くの場合、レイヤ2オーバーヘッドのためにフローに必要となる追加の帯域幅は無視でき、リンクの 25 パーセントの一部として送信できるため、この帯域幅は予約できず、ルーティングの更新とレイヤ2オーバーヘッドのために保持されます。この状況は、通常、IP フローで大きなパケット サイズが使用されている場合、またはレイヤ2カプセル化で可変サイズのフレームが許可されている場合（イーサネットおよびフレーム リレーのカプセル化など）に発生します。

ただし、フローのパケット サイズが小さく、基礎となるレイヤ2カプセル化が固定サイズのフレームを使用する場合は、Voice over IP（VoIP）フローが ATM リンクを通過する場合と同様に、レイヤ 2 カプセル化オーバーヘッドが重要になる可能性があります。

AAL5 SNAP または AAL5 MUX のカプセル化を使用する ATM PVC のオーバーサブスクライブを避けるために、RSVP はフローを許可するときに自動的にレイヤ 2 オーバーヘッドを考慮します。フローごとに、RSVP が、レイヤ 2 オーバーヘッドを含む、必要な帯域幅の総容量を決定し、その値を WFQ 帯域幅マネージャによるアドミッション コントロールで使用します。

（注） **iprsvplayer2overhead** コマンドは、ATM 相手先選択接続（SVC）での RSVP フローの帯域幅要件には影響しません。

例

次の例では、WFQ で予約されている帯域幅の総量が表示されます。

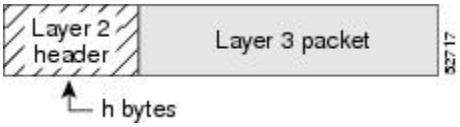
```
Router# show ip rsvp installed detail
RSVP:ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.1, Source is 10.1.1.1,
  Protocol is UDP, Destination port is 1000, Source port is 1000
  Reserved bandwidth:50K bits/sec, Maximum burst:1K bytes, Peak rate:50K bits/sec
  Min Policed Unit:60 bytes, Max Pkt Size:60 bytes
  Resource provider for this flow:
    WFQ on ATM PVC 100/101 on AT6/0: PRIORITY queue 40.  Weight:0, BW 89 kbps
  Conversation supports 1 reservations
  Data given reserved service:0 packets (0M bytes)
  Data given best-effort service:0 packets (0 bytes)
  Reserved traffic classified for 9 seconds
  Long-term average bitrate (bits/sec):0M reserved, 0M best-effort
```

上記の例では、フローのアドバタイズされたレイヤ 3 レートは 50 kbps です。この値が、**iprsvpbandwidth** 値によるアドミッション コントロールに使用されます。レイヤ 2 オーバーヘッドを含む実際に必要な帯域幅は、89 kbps です。WFQ はこの値をアドミッション コントロールに使用します。

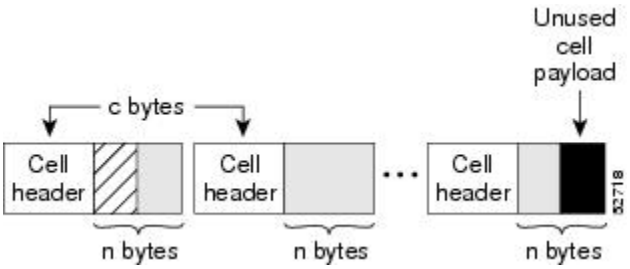
通常、レイヤ2オーバーヘッド アカウンティングの設定や無効化は必要ありません。RSVP は、アドバタイズされたレイヤ3フロー レート、最小パケット サイズ、および最大ユニット サイズと ATM PVC のレイヤ 2 カプセル化の特性を組み合わせて、アドミッション コントロールに必要な帯域幅を計算します。ただし、**iprsvplayer2overhead** コマンドを使用して、（任意のリンク タイプについて）レイヤ2オーバーヘッド アカウンティングを無効にすることや、カスタマイズすることができます。このコマンドのパラメータは、レイヤ3パケットがレイヤ2伝送用にどのようにフラグメント化およびカプセル化されるかを示す次の手順に基づいています。

1. 図 1 で示されているように、IP ヘッダーとペイロードを含むレイヤ 3 パケットから始めます。

2. 図 2 で示されているように、サイズ *h* のカプセル化ヘッダーまたはトレーラを追加します。



3. 図 3 で示されているように、セル ヘッダーが c バイト、セル ペイロードが n バイトの固定サイズのセルに結果のパケットを分割します。



4. 結果のレイヤ 2 セルを送信します。

その他の設定例

次の例では、インターフェイスとその PVC のすべての予約でレイヤ 2 オーバーヘッド アカウンティングが無効になっています。

```
Router(config-if)# no ip rsvp layer2 overhead
```

次の例では、ATM AAL5 SNAP カプセル化を使用してレイヤ 2 オーバーヘッド アカウンティングが設定されています。

```
Router(config-if)# no ip rsvp layer2 overhead 8 5 48
```

次の例では、ATM AAL5 MUX カプセル化を使用してレイヤ 2 オーバーヘッド アカウンティングが設定されています。

```
Router(config-if)# ip rsvp layer2 overhead 0 5 48
```

次の例では、イーサネット V2.0 カプセル化（8 バイトのプリアンブル、6 バイトの Source-Active（SA）メッセージ、6 バイトの Destination-Active（DA）メッセージ、2 バイトのタイプ、および 4 バイトのフレーム チェック シーケンス（FCS）トレーラ）を使用してレイヤ 2 オーバーヘッド アカウンティングが設定されています。

```
Router(config-if)# ip rsvp layer2 overhead 26 0 1500
```

関連コマンド

コマンド	説明
showiprsvpinstalled	RSVP 関連のインストールされているフィルタと対応する帯域幅情報を表示します。

ip rsvp listener

PATH メッセージをリッスンするようにリソース予約プロトコル（RSVP）ル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 **iprsvplistener** コマンドを使用します。リスニ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 rsvp listener [**vrf** *vrf-name*] *destination-ip* {**udp**|**tcp**|**any***number*} {**any***destination-port*} {**announce**|**reply**|**reject**}
no ip rsvp listener [**vrf** *vrf-name*] *destination-ip* {**udp**|**tcp**|**any***number*} {**any***destination-port*} {**announce**|**reply**|**reject**}

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）インスタンス名を指定します。
destination-ip	受信インターフェイスの IP アドレスです。
udp	受信インターフェイスの UDP を指定します。
tcp	受信インターフェイスの TCP を指定します。
any	受信インターフェイスに任意のプロトコルを使用できることを指定します。
number	0 ～ 255 の送信元ポート番号です。プロトコルは IP です。
any	受信インターフェイスに任意の宛先ポートを使用できることを指定します。
destination-port	受信インターフェイスのポート番号です。範囲は 0 ～ 65535 です。
announce	宛先へのフローの到着を受信側が通知しますが、それに応答して RESV メッセージは送信しません。
reply	フローが受信されたときに送信者が応答を要求し、一致する PATH メッセージが着信したときに RESV メッセージを送信します。
reject	指定されたリスナーパラメータと一致する着信 PATH メッセージに応答して、ルータが PATHERROR（拒否）メッセージを送信します。

コマンド デフォルト

このコマンドは、デフォルトでは無効になっています。そのため、リスナ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（config）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。
12.4(6)T	このコマンドが変更されました。RSVP アプリケーション ID のサポートが追加されました。

リリース	変更箇所
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。
15.0(1)M	このコマンドが変更されました。オプションの **vrf***vrf-name* キーワードと引数の組み合わせが追加されました。
Cisco IOS XE Release 2.6	このコマンドが、Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

（注） コマンドの構文は、プラットフォームとリリースによって異なります。**vrf***vrf-name* キーワードと引数の組み合わせは、ASR 1000 シリーズ アグリゲーション サービス ルータではサポートされていません。

iprsvplistener コマンドを使用して、PATH メッセージが目的の宛先アドレス、ポート、およびプロトコルに着信したときに、ルータが一致する RESV メッセージを送信できるようにします。このコマンドは、PATH メッセージからアプリケーション ID とプリエンプション優先順位値（存在する場合）をコピーし、RESV メッセージに含めます。

iprsvplistenervrf*vrf-name* コマンドを使用して、VRF によって定義されたルーティング ドメインのコンテキストでリスナーを作成します。リスナーの設定の階層を認識しておく必要があります。IP アドレスやその他のフィールドを指定せずに VRF のリスナーを設定すると、VRF、IP アドレス、およびポートによる後続のより具体的なリスナー設定が受け付けられません。

このコマンドは、**iprsvpreservation** コマンドおよび **iprsvpreservation-host** コマンドと似ています。ただし、これらのコマンドでは、1 つのコマンドで複数のポートまたはプロトコルを指定することはできません。そのため、場合によっては、ポートとプロトコルのセットを指定するために、多数のコマンドをプロキシに入力する必要があります。その一方で、**iprsvplistener** コマンドでは、1 つのコマンドだけを使用し、ポートとプロトコルのセットを指定するためにワイルドカードを使用することができます。

debugiprsvpapi コマンドを使用して一致する PATH メッセージを検索できますが、RESV メッセージは送信されません。

例

次の例では、PATH メッセージの宛先が 192.168.2.1 の場合、受信側がフローの RESV メッセージで応答するように送信者が要求しています。

```
Router# configure terminal
Router(config)# ip rsvp listener 192.168.2.1 any any reply
```

次の例では、VRF ルーティング ドメインにリスナーを作成します。

```
Router# configure terminal
Router(config)# ip rsvp listener vrf vpn1 10.10.10.10 any any reply
```

関連コマンド

コマンド	説明
iprsvpreservation	ルータが RSVP RESV メッセージの受信と転送をシミュレートできるようにします。
iprsvpreservation-host	RSVP RESV メッセージを生成するホストをシミュレートするようにルータをイネーブルにします。
showiprsvplisteners	設定されている RSVP リスナーを表示します。

ip rsvp listener outbound

指定されたインターフェイス経由で送信された PATH メッセージをリッスンするようにリソース予約プロトコル（RSVP）デバイスを設定するには、インターフェイス コンフィギュレーション モードで **ip rsvp listener outbound** コマンドを使用します。PATH メッセージのリスニ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 rsvp listener outbound{**reply**|**reject**}
no ip rsvp listener outbound {**reply**|**reject**}

構文の説明

reply	指定されたインターフェイスから送信される PATH メッセージについて、デバイスは次の処理を行います。
	• メッセージのローカル PATH 状態をインストールします。
	• PATH メッセージを終了し、ダウンストリームに転送しません。
	• PATH メッセージの代わりに、以下を使用して RESV（応答）メッセージを生成し、アップストリームに送信します。
	  • RESV メッセージ内のオブジェクトは、PATH メッセージ内のオブジェクトと同じです。
	  • プリエンプションやアプリケーション ID などのポリシー オブジェクトはエコー バックされます。
	  • 共有明示スタイルが使用されます。

reject	指定されたインターフェイスから送信される PATH メッセージについて、デバイスは次の処理を行います。 • PATH メッセージを終了し、ダウンストリームに転送しません。 • PATHERROR（拒否）メッセージを生成してアップストリームに送信します。 • ローカル PATH 状態をインストールせず、PATH メッセージを廃棄します。

コマンド デフォルト

リスナーは設定されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.2(18)SFX5	このコマンドが導入されました。
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。

リリース	変更箇所
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。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。
15.2(3)T	このコマンドが変更されました。IPv6 のサポートが追加されました。

使用上のガイドライン

ip rsvp listener outbound コマンドを使用して、指定されたインターフェイスから送信されるすべての PATH メッセージを照合します。

インターフェイスベースの受信側プロキシを応答するように設定すると、RSVP はフローのアウトバウンド（または出力）インターフェイスでコール アドミッション制御（CAC）を実行します。CAC が失敗すると、予約は作成されません。これは、グローバル RSVP 受信側プロキシ コマンドの場合と同じ動作です。

フローが使用するアウトバウンドインターフェイスはフローのセットアップ時に決定され、インターフェイスベースの受信側プロキシが参照されます。既存のフローのルーティングが変更されている場合は、インターフェイスベースの受信側プロキシは参照されません。

インターフェイスベースの受信側プロキシが、アドミッション コントロール エラーまたはポリシー拒否エラーによる RESVERR メッセージを受信した場合、インターフェイスベースの受信側プロキシは同じエラーで PATHERR メッセージを生成して、予約エラーの送信者に明示的な通知を提供します。

ip rsvp listener outbound 設定は、指定されたインターフェイス経由で送信された IPv4 と IPv6 両方の PATH メッセージに適用されます。

例

次の例では、イーサネット インターフェイス 3/0 経由で送信された PATH メッセージが拒否され、PATHERROR メッセージが生成されます。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface Ethernet3/0
Device(config-if)# ip rsvp listener outbound reject
```

関連コマンド

コマンド	説明
iprsvplistener	PATH メッセージをリッスンする RSVP デバイスを設定します。
ipv6rsvpreservation	ネットワーク デバイスが IPv6 RSVP RESV メッセージの受信と転送をシミュレートできるようにします。
iprsvpreservation-host	ネットワーク デバイスが IPv6 RSVP RESV メッセージを生成するホストをシミュレートできるようにします。

コマンド	説明
showipv6rsvplisteners	設定されている IPv6 RSVP リスナーを表示します。

ip rsvp msg-pacing

（注） Cisco IOS リリース 12.2(13)T 以降では、**ip rsvp msg-pacing** コマンドは、**ip rsvp signalling rate-limit** コマンドによって置き換えられました。詳細については、**ip rsvp signalling rate-limit** コマンドを参照してください。

リソース予約プロトコル（RSVP）メッセージの転送速度を設定するには、グローバル コンフィギュレーション モードで **ip rsvp msg-pacing** 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 rsvp msg-pacing [**period** *ms* [**burst** *msgs* [**maxsize** *qsize*]]]
no rsvp msg-pacing

構文の説明

period *ms*	（任意）**burst** キーワードで指定された RSVP メッセージの数をルータが送信できる間隔の長さ（ミリ秒単位）です。値は、1 ～ 1000 ミリ秒の範囲で指定します。
burst *msgs*	（任意）*period* キーワードで指定された各間隔でルータが出力インターフェイスに送信できる RSVP メッセージの最大数です。指定できる値は 1 ～ 2000 です。
maxsize *qsize*	（任意）送信ルータのインターフェイスごとの出力キューのサイズです。有効な値は 1 ～ 2000 です。

コマンド デフォルト

RSVP メッセージはペーシングされません。オプションの **burst** キーワードなしでコマンドを入力した場合、RSVP メッセージの転送速度は、発信インターフェイスごとに 200 メッセージ/秒に制限されます。**maxsize** キーワードで指定されるデフォルトの出力キュー サイズは 500 です。

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	変更箇所
12.0(14)ST	このコマンドが導入されました。
12.2(11)S	このコマンドが、Cisco IOS Release 12.2(11)S に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。

リリース	変更箇所
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。
12.2(13)T	このコマンドは、**ip rsvp signalling rate-limit** コマンドによって置き換えられました。

使用上のガイドライン

このコマンドを使用して、RSVP トラフィック エンジニアリングのシグナリング メッセージのバーストが、受信ルータのインプット キューをオーバーフローさせることを防ぐことができます。シグナリング メッセージでインプット キューがオーバーフローすると、ルータが一部のメッセージをドロップします。ドロップされたメッセージにより、メッセージがドロップされた LSP のシグナリングの完了が大幅に遅延します。

オプションの **burst** キーワードなしで **ip rsvp msg-pacing** コマンドを入力した場合、RSVP メッセージの転送速度は、発信インターフェイスごとに 200 メッセージ/秒に制限されます。**maxsize** キーワードで指定されるデフォルトの出力キュー サイズは 500 です。

例

次に、ネイバーに対して 1 秒間に最大で 150 の RSVP トラフィック エンジニアリングのシグナリング メッセージを送信するようにルータを設定し、出力キューのサイズを 750 にする例を示します。

```
Router(config)# ip rsvp msg-pacing period 1 burst 150 maxsize 750
```

関連コマンド

コマンド	説明
clear ip rsvp msg-pacing	**show ip rsvp neighbor** コマンドから、RSVP メッセージ ペーシング出力をクリアします。

ip rsvp neighbor

ネイバーが予約を要求できるようにするには、インターフェイス コンフィギュレーション モードで **iprsvpneighbor** 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。

ip rsvp neighbor *access-list-number*
no ip rsvp neighbor *access-list-number*

構文の説明

access-list-number	標準または拡張 IP アクセス リストの番号です。番号の範囲は 1 ～ 199 です。

コマンド デフォルト

ルータはすべてのネイバーからのメッセージを受け入れます。

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	変更箇所
11.2	このコマンドが導入されました。
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。

使用上のガイドライン

このコマンドを使用すると、特定のリソース予約プロトコル（RSVP）ネイバーのみが予約を行うことができます。制限が指定されていない場合は、すべてのネイバーが予約を要求できます。アクセス リストが指定されている場合は、指定されたアクセス リストの要件を満たすネイバーのみが予約を行うことができます。

RSVP は、Versatile Interface Processor（VIP）分散型シスコ エクスプレス フォワーディング（dCEF）で設定できません。

例

次に、アクセス リスト 1 の要件を満たすネイバーに予約の要求を許可する例を示します。

```
interface ethernet 0
 ip rsvp neighbor 1
```

関連コマンド

Command	Description
fair-queue(WFQ)	インターフェイスに対する WFQ を有効にします。

Command	Description
iprsvpbandwidth	インターフェイスで IP 用 RSVP をイネーブルにします。
iprsvpreservation	ルータが RSVP RESV メッセージの受信と転送をシミュレートできるようにします。
iprsvpsender	ルータが RSVP PATH メッセージの受信と転送をシミュレートできるようにします。
iprsvpudp-multicasts	ルータが IP カプセル化マルチキャスト パケットを生成するときはいつでも、UDP カプセル化済み RSVP マルチキャストを生成するようにルータに指示します。
random-detect(interface)	WRED または DWRED をイネーブルにします。
showiprsvpinstalled	RSVP 関連のインストールされているフィルタと対応する帯域幅情報を表示します。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。
showiprsvpneighbor	現在の RSVP ネイバーを表示します。
showiprsvpreservation	現在データベースに格納されている RSVP 関連の受信側情報を表示します。
showiprsvpsender	現在データベース上に存在する RSVP PATH 関連の送信側情報を表示します。

ip rsvp policy cops minimal

Common Open Policy Service（COPS）サーバの負荷を軽減し、管理対象ルータでのメッセージの遅延時間を改善するには、グローバル コンフィギュレーション モードで **iprsvppolicycopsminimal** コマンドを使用して COPS RSVP ポリシーを制限し、PATH および RESV メッセージのみを判定するようにします。制限をオフにするには、このコマンドの **no** 形式を使用します。

ip rsvp policy cops minimal
no ip rsvp policy cops minimal

構文の説明

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

デフォルトの状態はオフで、設定された COPS ポリシーにより、判定可能なすべての RSVP メッセージが処理されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.1(1)T	このコマンドが導入されました。
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。

使用上のガイドライン

このコマンドを使用した場合、COPS は PATHERROR および RESVERROR メッセージの判定を試みません。代わりに、これらのメッセージはすべて受け入れられ、転送されます。

例

次に、COPS 認証が PATH および RESV メッセージに限定される例を示します。

```
ip rsvp policy cops minimal
```

次に、この制限を削除する例を示します。

```
no ip rsvp policy cops minimal
```

ip rsvp policy cops report-all

アウトソースの決定でルータが成功と失敗をレポートできるようにするには、グローバル コンフィギュレーション モードで **iprsvppolicycopsreport-all** コマンドを使用します。ルータをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip rsvp policy cops report-all
no ip rsvp policy cops report-all

構文の説明

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

このコマンドのデフォルトの状態では、設定の決定に関するポリシー決定ポイント（PDP）にのみレポートを送信します。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.1(1)T	このコマンドが導入されました。
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。

使用上のガイドライン

デフォルトの状態では、ルータがリソース予約プロトコル（RSVP）の設定の決定の導入に成功または失敗したときに PDP にレポートします。

設定の決定には、少なくとも次のいずれかが含まれます。

- （追加のコンテキストの有無にかかわらず）RESV ALLOC コンテキスト
- ステートレスまたは名前付きの決定オブジェクト

これらの要素の少なくとも 1 つを含まない決定は、アウトソースの決定です。

ポリシー サーバの一部のブランドは、RSVP メッセージングに関するレポートを予期している場合があります。このレポートは、デフォルトの状態の RSVP 用 Cisco Common Open Policy Service（COPS）では発行されません。このような場合は、**iprsvppolicycopsreport-all** コマンドを使用してルータとポリシー サーバの間の相互運用性を確保します。これによりルータのポリシー処理に悪影響が及ぶことはありません。

ユニキャスト FF 予約要求には（IN CONTEXT および OUT CONTEXT と組み合わせて）RESV ALLOC コンテキストが含まれているため、ルータから PDP へのレポートを常にスティミュレートします。

例

ポリシー適用ポイント（PEP）から PDP へのレポート プロセスを示すために、次の例では新しい PATH メッセージがルータに到着すると **debugcops** コマンドが常に有効になります。

```
Router(config)# ip rsvp policy cops report-all
00:02:48:COPS:** SENDING MESSAGE **
Contents of router's request to PDP:
 COPS HEADER:Version 1, Flags 0, Opcode 1 (REQ), Client-type:1, Length:216
 HANDLE (1/1) object. Length:8.    00 00 02 01
 CONTEXT (2/1) object. Length:8.   R-type:5.     M-type:1
 IN_IF (3/1) object. Length:12.   Address:10.1.2.1.    If_index:4
 OUT_IF (4/1) object. Length:12.   Address:10.33.0.1.    If_index:3 CLIENT SI (9/1)
object. Length:168.   CSI data:
 [A 27-line Path message omitted here]
00:02:48:COPS:Sent 216 bytes on socket,
00:02:48:COPS:Message event!
00:02:48:COPS:State of TCP is 4
00:02:48:In read function
00:02:48:COPS:Read block of 96 bytes, num=104 (len=104)
00:02:48:COPS:** RECEIVED MESSAGE **
Contents of PDP's decision received by router:
 COPS HEADER:Version 1, Flags 1, Opcode 2 (DEC), Client-type:1, Length:104
 HANDLE (1/1) object. Length:8.    00 00 02 01
 CONTEXT (2/1) object. Length:8.   R-type:1.     M-type:1
 DECISION (6/1) object. Length:8.   COMMAND cmd:1, flags:0
 DECISION (6/3) object. Length:56.   REPLACEMENT
 [A 52-byte replacement object omitted here]
 CONTEXT (2/1) object. Length:8.   R-type:4.     M-type:1
 DECISION (6/1) object. Length:8.   COMMAND cmd:1, flags:0
00:02:48:Notifying client (callback code 2)
00:02:48:COPS:** SENDING MESSAGE **
Contents of router's report to PDP:
 COPS HEADER:Version 1, Flags 1, Opcode 3 (RPT), Client-type:1, Length:24
 HANDLE (1/1) object. Length:8.    00 00 02 01
 REPORT (12/1) object. Length:8.   REPORT type COMMIT (1)
00:02:48:COPS:Sent 24 bytes on socket,
```

ip rsvp policy cops servers

リソース予約プロトコル（RSVP）がリモート判定に Common Open Policy Service（COPS）ポリシーを使用するように指定するには、グローバル コンフィギュレーション モードで **iprsvppolicycopsservers** コマンドを使用します。RSVP 用 COPS の使用をオフにするには、このコマンドの **no** 形式を使用します。

ip rsvp policy cops [*acl*] **servers** *server-ip* [*server-ip*]
no ip rsvp policy cops [*acl*] **servers**

構文の説明

acl	（任意）セッションが COPS ポリシーによって管理されるアクセス コントロール リスト（ACL）を指定します。
server-ip	（任意）COPS ポリシーを管理するサーバの IP アドレスを指定します。最大で 8 台のサーバを指定でき、最初のサーバがプライマリ サーバとして扱われます。

コマンド デフォルト

ACL を指定しない場合、デフォルトの動作ではすべての予約が指定したポリシー サーバにより管理されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.1(1)T	このコマンドが導入されました。
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。

使用上のガイドライン

複数のサーバを指定した場合、最初のサーバは RSVP によりプライマリ サーバとして扱われ、指定したすべての ACL に対して同様に機能します。

リスト内のすべてのサーバは、同じポリシー設定を持つ必要があります。

ルータとサーバの接続が切断された場合、ルータは同じサーバに再接続を試みます。再接続に失敗した場合、ルータは次のアルゴリズムに従います。

（ポリシー決定ポイント（PDP）が接続を閉じたか、TCP/IP エラーが発生したか、またはキープアライブに失敗したために）PDP への接続が閉じられた場合、ポリシー適用ポイント（PEP）が CLIENT-CLOSE メッセージを発行し、同じ PDP に再接続を試みます。PEP が PDP リダイレクト アドレスを含む CLIENT-CLOSE メッセージを受信した場合、PEP はリダイレクトされた PDP への接続を試みます。

次の点に注意してください。

- いずれかの試みに失敗すると、PEP は **iprsvppolicycopsservers** コンフィギュレーション コマンドで以前に指定された PDP への接続を試みます。接続順はこのコマンドで指定されているサーバの順序に従い、常にリスト内の最初のサーバから始まります。
- PEP が接続に成功せずにサーバのリストの最後に到達した場合、PEP はリスト内の最初のサーバへの接続を再度試みる前に、一定の時間（再接続遅延と呼ばれます）待機します。この再接続遅延の初期値は 30 秒で、PEP が接続できないままリストの最後に到達するたびに 2 倍されます。最大値は 30 分です。接続が確立されると直ちに、遅延が 30 秒にリセットされます。

このコマンドの **no** 形式には、サーバ IP アドレスを含める必要はありません。ただし、以前に指定したすべてのアクセス リストを含める必要があります（次のセクションの最後の例を参照）。

例

この最初の例では、ルータ 9 を通過するすべての予約にサーバ 172.27.224.117 にある COPS ポリシーを適用します。また、このルータのバックアップ COPS サーバを、アドレス 172.27.229.130 のサーバとして識別します。

```
Router(config)# ip rsvp policy cops servers 172.27.224.117 172.27.229.130
```

次の例では、アクセス リスト 40 および 160 に一致する場合に限り、ルータ 9 を通過する予約にサーバ 172.27.224.117 にある COPS ポリシーを適用します。このルータを通過するその他の予約は、このサーバによって管理されません。また、このコマンド ステートメントはこのルータのバックアップ COPS サーバを、アドレス 172.27.229.130 のサーバとして識別します。

```
Router(config)# ip rsvp policy cops 40 160 servers 172.27.224.117 172.27.229.130
```

次の例では、以前に指定したアクセス リスト 40 および 160 の COPS をオフにします（以前に指定したリストの 1 つだけをオフにすることはできません）。

```
Router(config)# no ip rsvp policy cops 40 160 servers
```

ip rsvp policy cops timeout

Common Open Policy Service（COPS）サーバとの接続が失われた後にポリシー適用ポイント（PEP）ルータがポリシー情報を保持する時間の長さを設定するには、グローバル コンフィギュレーション モードで **iprsvppolicycopstimeout** コマンドを使用します。ルータをデフォルト値（5 分）に戻すには、このコマンドの **no** 形式を使用します。

ip rsvp policy cops timeout *policy-timeout*
no ip rsvp policy cops timeout

構文の説明

policy-timeout	タイムアウトの期間は 1 ～ 10,000 秒です。

コマンド デフォルト

タイムアウトのデフォルトは 300 秒（5 分）です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.1(1)T	このコマンドが導入されました。
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。

例

次に、失われたサーバに関連するすべてのポリシー情報を 10 分間でタイムアウトするようにルータを設定する例を示します。

```
ip rsvp policy cops timeout 600
```

次に、タイムアウトをデフォルト値にリセットする例を示します。

```
no ip rsvp policy cops timeout
```

ip rsvp policy default-reject

ポリシー アクセス コントロール リスト（ACL）と一致しないすべてのメッセージを拒否するには、グローバル コンフィギュレーション モードで **iprsvppolicydefault-reject** コマンドを使用します。ACL と一致しないすべてのメッセージを伝えるデフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

ip rsvp policy default-reject
no ip rsvp policy default-reject

構文の説明

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

このコマンドを使用しない場合、リソース予約プロトコル（RSVP）のデフォルトの動作では、一致しないすべての RSVP メッセージが受け入れられるか、インストールされるか、転送されます。このコマンドが呼び出されると、一致しないすべての RSVP メッセージが拒否されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.1(1)T	このコマンドが導入されました。
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。

使用上のガイドライン

ACL を使用せずに COPS が設定されている場合、またはいずれかのポリシー ACL が **permitipanyany** コマンドを使用するように設定されている場合は、ACL の動作が優先され、セッションは不一致になりません。

（注） このコマンドは、一致しないメッセージのブロッキングに対して 1 つの例外を作成します。これにより、RESV および PATH メッセージの拒否によって生成された RESVERROR および PATHERROR メッセージが転送されます。これは、デフォルトの拒否操作がネットワーク マネージャから完全に隠されないようにするために行われます。

注意 このコマンドには十分に注意してください。アクセス リストの範囲が狭すぎる場合、または Common Open Policy Service（COPS）サーバが指定されていない場合は、ルータ上のすべての RSVP 処理がシャットダウンされます。（COPS サーバを指定するには、**iprsvppolicycopsservers** コマンドを使用します）。

例

次に、一致しないすべての予約を拒否するように RSVP を設定する例を示します。

```
ip rsvp policy default-reject
```

次に、一致しないすべての予約を受け入れるように RSVP を設定する例を示します。

```
no ip rsvp policy default-reject
```

ip rsvp policy identity

リソース予約プロトコル（RSVP）アプリケーションID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 **iprsvppolicyidentity** コマンドを使用します。RSVP アプリケーション ID を削除するには、このコマンドの **no** 形式を使用します。

ip rsvp policy identity *alias* **policy-locator** *locator*
no ip rsvp policy identity *alias* [**policy-locator** *locator*]

構文の説明

alias	RSVP コンフィギュレーション コマンドと **show** 表示で ID を参照するためにルータ内で使用される文字列です。文字列には、印刷可能文字（0x20 ～ 0x7E の範囲）を 64 文字まで使用できます。 （注） 空白文字または疑問符（?）を、別名の一部またはロケータ文字列自体として使用する場合、空白文字または疑問符を入力する前に、CTRL-V キー シーケンスを入力する必要があります。エイリアスが他のルータに送信されることはありません。
policy-locator *locator*	RSVP メッセージで伝えられ、X.500 識別名（DN）形式のアプリケーション ID を含む文字列を指定します。（詳細については、「**UsageGuidelines"** セクションを参照してください）。

コマンド デフォルト

このコマンドは、デフォルトでは無効になっています。そのため、RSVPアプリケーションID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（config）

コマンド履歴

リリース	変更箇所
12.4(6)T	このコマンドが導入されました。
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。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

RSVP PATH および RESV メッセージをローカル ポリシーに一致させる基準として、RSVP ID を使用できます。また、IDを使用して静的な送信者と受信者を設定することもできます。ローカル ポリシーの一致基準として RSVP ID を使用する場合、RSVP は *policylocator* 文字列を、正規表現と呼ばれるパターン一致文字列の一種として扱います。正規表現では、複数のX.500 DN に一致できるローカル ポリシーで使用する、単一 ID を設定できます。デフォルトでは、正規表現は式に適切な制御文字を追加して完全一致を適用しない限り、完全一致ではありません。

Cisco IOS および Cisco IOX XE ソフトウェアでは、*locator* は、ルータがアプリケーション ID を含む RSVP メッセージに適用する正しいポリシーを見つけるために使用する主要な情報で

す。この文字列は X.500 DN 形式を前提としており、RFC 2872 で推奨されている次の属性を含みます。

- APP = アプリケーション識別子（必須属性）。
- VER = アプリケーションのバージョン番号（必須属性）。
- SAPP=サブアプリケーション識別子（オプション属性）。任意の数のサブアプリケーション要素を含めることができます。
- GUID = グローバル固有識別子（オプション属性）。

次に例を示します。

- APP = CCM、VER = 1.1、SAPP = Voice
- GUID = http://www.cisco.com/apps、APP = VideoConference、VER = 1.2.3

1 つのルータ上に最大で 100 個の ID を作成できます。それ以上の ID を作成しようとすると、コマンドは失敗し、「RSVP エラー：最大数の ID がすでに作成されています（RSVP error: maximum number of identities already created）」というエラー メッセージが生成されます。

iprsvppolicyidentity コマンドを使用する場合は、次の動作に注意してください。

- *alias* または *locator* に空の文字列や無効な文字列を指定すると、コマンドは拒否され、エラー メッセージが生成されます。
- 設定の *alias* または *locator* の文字列に引用符が必要な場合は、Cisco IOS ソフトウェアにより自動的に引用符が追加されます。
- オプションの **policy-locator** キーワードをこのコマンドの **no** 形式で指定し、削除される *alias* の設定された *locator* 文字列に *locator* が一致しない場合は、コマンドが拒否されます。
- 見つからない、空の、または無効な文字を含む *alias* を指定した場合は、コマンドが拒否され、エラー メッセージが生成されます。
- RSVP は、有効な X.500 DN の *locator* 文字列をチェックしません。そのため、*locator* 文字列は希望の文字列にすることができます。

コマンドの制限

- ユーザ ID は、Cisco IOS リリース 12.4(6)T ではサポートされていません。
- 100 個を超える ID がある単一のルータを一度に設定することはできません。

例

アプリケーション ID の完全一致

次の例は、コンテンツが正確な文字列「APP=Voice」であるロケータ文字列を含む RSVP メッセージのアプリケーション ID を示しています。

```
Router# configure terminal
Router(config)# ip rsvp policy identity "rsvp-voice" policy-locator "^APP=Voice$"
Router(config-rsvp-id)# end
```

アプリケーション ID のワイルドカード（または部分）一致

次の例は、伝えられるアプリケーション ID のいずれかの場所に文字列の一部「APP=Voice」があるロケータ文字列を含む RSVP メッセージの部分一致であるアプリケーション ID を示しています。

```
Router# configure terminal
Router(config)# ip rsvp policy identity "rsvp-voice" policy-locator ".*APP=Voice.*"
Router(config-rsvp-id)# end
```

関連コマンド

コマンド	説明
iprsvppolicylocal	ネットワーク内の RSVP リソースの使用を決定するローカルプロシージャを作成します。
showiprsvppolicyidentity	ルータ設定で選択された RSVP ID を表示します。
showiprsvppolicylocal	設定されている選択されたローカル ポリシーを表示します。

ip rsvp policy local

リソース予約プロトコル（RSVP）要求に対する認証の実行方法を決定し、ローカル ポリシー コンフィギュレーション モードにするには、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 **iprsvppolicylocal** 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。

ip rsvp policy local {**acl** *acl1* [*acl2...acl8*]|**dscp-ip** *value1* [*value2....value8*]|**default**|**identity** *alias1* [*alias2* **...** *alias4*]|**origin-as** *as1* [*as2...as8*]}
no ip rsvp policy local {**acl** *acl1* [*acl2...acl8*]|**dscp-ip** *value1* [*value2...value8*]|**default**|**identity** *alias1* [*alias2...alias4*]|**origin-as** *as1* [*as2...as8*]}

構文の説明

acl *acl1* [*acl2...acl8*	アクセス コントロール リスト（ACL）を指定します。各 ACL の値は 1 ～ 199 です。 （注） 少なくとも 1 つの ACL を ACL ベースのポリシーに関連付ける必要があります。ただし、ACL ベースのポリシーに関連付けることができる ACL は最大で 8 つです。
dscp-ip *value1* [*value2...value8*	集約予約を照合するための DiffServ コードポイント（DSCP）を指定します。有効な値は次のとおりです。 • 0 ～ 63：DSCP の数値。デフォルト値は 0 です。 • af11 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）プレシデンス値。 • default：デフォルト DSCP 値。 • ef：Expedited Forwarding（EF; 完全優先転送）DSCP 値。 （注） 少なくとも 1 つの DSCP を DSCP ベースのポリシーに関連付ける必要があります。ただし、DSCP ベースのポリシーに関連付けることができる DSCP 値は最大で 8 つです。
default	RSVP メッセージが ACL、DSCP、ID、または自律システムに一致しない場合のデフォルトを指定します。
identity *alias1* [*alias2...alias4*	**iprsvppolicyidentity** コマンドを使用して以前に設定されたアプリケーション ID のアプリケーション ID エイリアスを指定します。 （注） 少なくとも 1 つのエイリアスをアプリケーション ID ベースのポリシーに関連付ける必要があります。ただし、関連付けることができるのは最大で 4 つです。

origin-as *as1* [*as2...as8*	自律システムを指定します。各自律システムの値は 1 ～ 65535 です。 （注） 少なくとも1つの自律システムを自律システムベースのポリシーに関連付ける必要があります。ただし、関連付けることができるのは最大で 8 つです。

コマンド デフォルト

このコマンドは、デフォルトでは無効になっています。そのため、ローカル ポリシ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（config）
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	変更箇所
12.2(13)T	このコマンドが導入されました。
12.0(29)S	このコマンドが変更されました。**origin-as***as* キーワードと引数の組み合わせと、新しいサブモード コマンドが追加されました。
12.0(30)S	このコマンドが変更されました。ACL を設定するときに、プロトコルとして 0 を使用することができなくなりました。
12.4(4)T	このコマンドが Cisco IOS Release 12.4(4)T に統合されました。
12.4(6)T	コマンドが変更されました。次の点が変更されました。 • インターフェイス コンフィギュレーション モードが追加され、インターフェイスごとのローカル ポリシーがサポートされました。 • **Theidentity***alias* キーワードと引数の組み合わせが追加されました。 • **maximum** サブモード コマンドが、RESV メッセージをサポートするように変更されました。
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。
12.2(33)SRC	このコマンドが変更されました。**dscp-ip***value* キーワードと引数の組み合わせが追加されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

iprsvppolicylocal コマンドを使用して、RSVP 要求に対する認証の実行方法を決定します。

（注） **origin-as***as* キーワードと引数の組み合わせを入力すると、BGP が動作するまで自律システムベースのポリシーが無効になることを示す RSVP 警告メッセージが表示されます。

すべてのタイプの一致基準を非トラフィック エンジニアリング（TE）予約に使用できます。シスコ ルータから送信される TE PATH および RESV メッセージにはアプリケーション ID が含まれていないため、アプリケーション ID を除くすべてのタイプの一致基準を TE 予約に使用できます。

1 つのデフォルト ローカル ポリシー、1 つ以上の ACL ベースのポリシー、1 つ以上の自律システムベースのポリシー、1 つ以上のアプリケーション ID ベースのポリシー、1 つ以上の DSCP ベースのポリシーの、5つのタイプのローカルポリシーがあります。RSVP メッセージが ACL、自律システム、アプリケーション ID、または DSCP ベースのポリシーと一致しない場合は、デフォルト ポリシーが使用されます。

同じインターフェイス上に、またはグローバルに、ACL、自律システム、アプリケーション ID、DSCP、またはデフォルトのローカルポリシータイプを混在させて設定することができます。ポリシーの優先順位は次のとおりです（高いものから低いものへの順序）。

- デフォルト以外のインターフェイス ポリシー
- デフォルトのインターフェイス ポリシー
- デフォルト以外のグローバル ポリシー
- グローバル デフォルト ポリシー

（注） TE トンネルで使用するために ACL を設定する場合は、プロトコルとして 0 を使用しないでください。RSVP が ACL と一致しないため、どのメッセージも受け入れることができなくなります。

ポリシー一致基準

（注） **iprsvppolicylocal** コマンドを使用して、ポリシー一致基準を複数回指定することはできません

ACL ベースのポリシーには少なくとも 1 つの ACL が関連付けられている必要がありますが、オプションで最大 8 つの ACL を関連付けることができます。ACL は標準または拡張 IP ACL に設定できます。以下に説明するように、RSVP シグナリング メッセージ内の RSVP オブジェクトに基づく送信元/宛先のアドレス/ポートと照合されます。

- ACL 送信元アドレス：RSVP メッセージの SENDER_TEMPLATE オブジェクトの送信元アドレスと照合されます。このオブジェクトが存在しない場合は、IP ヘッダーの送信元アドレスが使用されます。

- ACL 宛先アドレス：RSVP メッセージの SESSION オブジェクトの宛先アドレスと照合されます。このオブジェクトが存在しない場合は、IP ヘッダーの宛先アドレスが使用されます。
- ACL 送信元ポート：RSVP メッセージの SENDER_TEMPLATE オブジェクトの送信元ポートと照合されます。このオブジェクトが存在しない場合は、0 の送信元ポートが使用されます。
- ACL 宛先ポート：RSVP メッセージの SESSION オブジェクトの宛先ポートと照合されます。このオブジェクトが存在しない場合は、0 の宛先ポートが使用されます。
- ACL IP プロトコル：RSVP メッセージの SESSION オブジェクトの IP プロトコルと照合されます。このオブジェクトが存在しない場合は、0 の IP プロトコルが使用されます。TE セッション用の IP プロトコルの場合、ACL IP プロトコルが UDP である必要があります。
- ACL DiffServ コード ポイント（DSCP）値：RSVP メッセージの IP ヘッダーの DSCP 値と照合されます。

（注） **debugiprsvpfilter** コマンドの ACL を作成する場合、コマンドが DSCP を使用せず、TE セッションのプロトコルが無視されるという点を除いて、同じポリシー一致基準が適用されます。

自律システムベースのポリシーには少なくとも 1 つの自律システムが関連付けられている必要がありますが、オプションで最大 8 つの自律システムを関連付けることができます。これらは、RSVP メッセージの IP ヘッダーではなく、RSVP シグナリング メッセージ内の RSVP オブジェクトに含まれる着信インターフェイス/送信元 IP アドレスと照合されます。

アプリケーション ID ベースのポリシーには少なくとも 1 つのアプリケーション ID が関連付けられている必要がありますが、オプションで最大 4 つのアプリケーション ID を関連付けることができます。これらは、RSVP メッセージの IP ヘッダーではなく、RSVP シグナリング メッセージ内の RSVP オブジェクトに含まれる着信インターフェイス/送信元 IP アドレスと照合されます。

DSCP ベースのポリシーには少なくとも 1 つの DSCP が関連付けられている必要がありますが、オプションで最大 4 つの DSCP を関連付けることができます。RSVP は、集約メッセージの SESSION オブジェクトから DSCP を抽出し、DSCP 基準に一致するローカル ポリシーを適用します。

コマンドの制限

- 1 台のルータに 300 を超えるローカル ポリシーを設定することはできません。この制限は、ポリシーの場所（グローバルまたはインターフェイスごと）や、アプリケーション ID、ACL、または自律システムなどの一致基準とは無関係です。
- 4 つを超える RSVP ID を持つ単一のローカル ポリシーを設定することはできません。

CLISubmodes

iprsvppolicylocal コマンドを入力すると、作成しているローカル ポリシーのプロパティを定義する、ローカル ポリシー CLI サブモードになります。

（注） 作成するローカルポリシーは、受け入れるメッセージまたは転送するメッセージのタイプについてRSVPに指示するサブモードコマンドを入力しないかぎり、すべてのRSVPメッセージを自動的に拒否します。

サブモード コマンドは次のとおりです。

- **accept**：RSVP メッセージを受け入れますが、転送しません。

accept {all | path | path-error | resv | resv-error}

- **all**：すべての着信 RSVP メッセージを受け入れます。
- **path**：ACL、自律システム、アプリケーションID、またはデフォルトなどの、このポリシーの一致基準を満たす着信 PATH メッセージを受け入れます。このコマンドを省略した場合、ポリシー一致基準を満たす着信 PATH メッセージは拒否され、応答で PATHERROR メッセージが送信されます。ただし、PATHERROR 応答もローカル ポリシーに従います。
- **path-error**：このポリシーの一致基準を満たす着信 PATHERROR メッセージを受け入れます。このコマンドを省略した場合、ポリシー一致基準を満たすローカルで生成された PATHERROR メッセージを含めて、着信が拒否されます。
- **resv**：このポリシーの一致基準を満たす着信 RESV メッセージを受け入れ、必要なアドミッション コントロールを実行します。このコマンドを省略した場合、ポリシー一致基準を満たす着信 RESV メッセージは拒否され、応答で RESVERROR メッセージが送信されます。ただし、RESVERROR 応答もローカル ポリシーに従います。

ポリシーのデフォルトの帯域幅は無制限です。そのため、ポリシーに帯域幅が設定されていない場合は、すべての帯域幅要求が制限以下となるため、RESVメッセージは常にローカルポリシーによって受け入れられます。ただし、RESV メッセージが適用される入力インターフェイスの RSVP プールの帯域幅が不十分な場合には、その後に RESV メッセージのアドミッション コントロールに失敗する可能性があります。（詳細については、**iprsvpbandwidth** コマンドを参照してください）。RESV メッセージによって要求された帯域幅が大きすぎる場合は、同様にローカル ポリシーに従う RESVERROR メッセージが RESV 送信者に送信されます。

- **resv-error**：このポリシーのポリシー一致基準を満たす着信 RESVERROR メッセージを受け入れます。このコマンドを省略した場合、ポリシー一致基準を満たすローカルで生成された RESVERROR メッセージを含めて、着信が拒否されます。

- **default**：コマンドをデフォルトに設定します。
- **exit**：ローカル ポリシー コンフィギュレーション モードを終了します。
- **fast-reroute**：Fast Reroute サービスを要求する TE LSP を許可します。デフォルト値では受け入れられます。
- **forward**：RSVP メッセージを受け入れ、転送します。

forward {**all**|**path** | **path-error** | **resv** | **resv-error**}

- • **all**：すべての RSVP メッセージを受け入れ、転送します。
  - **path**：このポリシーの一致基準を満たす PATH メッセージを受け入れ、転送します。このコマンドを省略した場合、ポリシー一致基準を満たす PATH メッセージが次の（ダウンストリームの）ホップに転送されません。
  - **path-error**：このポリシーの一致基準を満たす PATHERROR メッセージを受け入れ、転送します。このコマンドを省略した場合、一致基準を満たすPATHERRORメッセージが前の（アップストリームの）ホップに転送されません。誰かがRSVPのポートスキャンを試みている可能性があるため、信頼できないノードからの PATH メッセージを受信した場合に、アウトバウンド PATHERROR メッセージを拒否することもできます。PATHERROR メッセージで返信すると、RSVP をサポートしていることと、使用しているIPアドレスが、信頼できないノードに把握されます。このような情報は、RSVP ベースの攻撃を試みるために使用される可能性があります。
  - **resv**：このポリシーの一致基準を満たす RESV メッセージを受け入れ、転送します。このコマンドを省略した場合、一致基準を満たすRESVメッセージが前の（アップストリームの）ホップに転送されません。
  - **resv-error**：このポリシーの一致基準を満たす RESVERROR メッセージを受け入れ、転送します。このコマンドを省略した場合、一致基準を満たすRESVERRORメッセージが次の（ダウンストリームの）ホップに転送されません。誰かがRSVPのポートスキャンを試みている可能性があるため、信頼できないノードからのRESVメッセージを受信した場合に、アウトバウンド RESVERROR メッセージを拒否することもできます。RESVERROR メッセージで返信すると、RSVP をサポートしていることと、使用しているIPアドレスが、信頼できないノードに把握されます。このような情報は、RSVP ベースの攻撃を試みるために使用される可能性があります。

- **local-override**：このローカル ポリシーを適用して、他のポリシー ソースを上書きします。すべての判断がこのポリシーによって確定されます。local-override を省略した場合、RSVP はローカル ポリシーの判断を保留し、RSVP メッセージに関する判断を行う別のローカルまたはリモート ポリシーが存在するかどうかを確認して、他のポリシーの判断がない場合に限り、ローカル ポリシーの判断が適用されます。

- **maximum** [**bandwidth**[**group***x*] [**single***y*] | **senders***n*]：リソースの制限を設定します。

  - **bandwidth**[**group***x*] [**single***y*]：RSVP 予約の帯域幅制限を示します。**group** キーワードは、このポリシーの対象となるすべての予約によって要求できる帯域幅の量を指定します。**single** キーワードは、このポリシーの対象となる特定の RSVP 予約によって要求できる最大帯域幅を指定します。x と y の値はキロビット/秒単位で、1 ～ 10,000,000 の範囲で指定します（既存のインターフェイス モードの **iprsvpbandwidth** コマンドと同様の概念です）。bandwidth コマンドがない場合は、帯域幅要求に関するポリシー制限がなくなります。

以前は、**maximumbandwidth** コマンドは PATH メッセージにのみ適用されました。しかし、アプリケーション ID の強化の一環として、このコマンドは RESV メッセージにのみ適用されるようになりました。この変更には、次のような利点があります。まず、共有予約と非共有予約の両方に対する RSVP のアドミッション コントロール プロセスでローカル ポリシー帯域幅制限を使用できます。PATH メッセージのグループ帯域幅チェックを実行していた以前のリ

リースでは、帯域幅の共有が考慮できなかったため、ポリシー用により大きな最大グループ帯域幅を作成することで共有を考慮する必要がありました。また、ポリシー帯域幅が不十分で着信 RESV メッセージのニーズを満たせない場合に、ローカル ポリシーでアドミッション コントロール機能中のプリエンプションをトリガーできます。

- • **senders** *n*：このルータで同時にアクティブにできる、このポリシーの影響を受ける RSVP 送信者の数を制限します。*n* の値の範囲は 1 ～ 50,000 で、デフォルトは 1000 です。

（注） **iprsvppolicypreempt** コマンドを設定しない場合、**maximum** コマンドが拒否され、次のようなエラー メッセージが表示されることがあります：
‘RSVP [illegible]

- **no**：コマンドを無効にするか、デフォルト設定にします。
- **preempt-priority** [**traffic-eng***x*] *setup-priority* [*hold-priority*]：アップストリームまたはダウンストリームのネイバーまたはローカルクライアントアプリケーションから伝えられなかった場合に PATH および RESV メッセージに挿入される RSVP QoS 優先順位と、RSVP QoS または MPLS/TE セッションが伝えることができる最大設定または保持優先度を指定します。これらの制限を超えると、PATHERROR、RESVERROR、またはローカル アプリケーション エラーが返されます。

x 値は、TE 予約の優先順位の上限を示します。*x* 値の範囲は 0 ～ 7 で、番号が小さいほど予約の優先順位が高くなります。非 TE 予約の場合は、*x* 値の範囲は 0 ～ 65535 で、番号が大きくなるほど予約の優先順位が高くなります。

setup-priority 引数は、最初にインストールされたときの予約の優先順位を示します。オプションの *hold-priority* 引数は、インストール後の予約の優先順位を示します。省略した場合は、デフォルトの *setup-priority* になります。*setup-priority* 引数と *hold-priority* 引数の値の範囲は 0 ～ 7 で、0 が最も高い優先順位と見なされます。

着信メッセージが、ポリシーで許可されている優先順位よりも高い優先順位を要求するプリエンプション優先順位を持っている場合、そのメッセージは拒否されます。
tunnelmplstraffic-engpriority コマンドを使用して、TE トンネルのプリエンプション優先順位を設定します。

単一のポリシーには、**preempt-prioritytraffic-eng** および **preempt-priority** コマンドを含めることができます。このコマンドは、TEおよび非TEエンドポイントまたはミッドポイントが混在するサブネットを識別する ACL にポリシーがバインドされている場合に役立ちます。

（注） サブモード コマンドを入力せずにローカル ポリシー コンフィギュレーション モードを終了すると、作成したポリシーはすべての RSVP メッセージを拒否するようになります。

Per-InterfaceLocalPolicies

すべてのローカル ポリシー サブモード コマンドは、インターフェイス単位でもサポートされています。選択したインターフェイスの Cisco IOS インターフェイス コンフィギュレーション モードにして、任意の数とサブモード コマンドの組み合わせを入力するだけです。

インターフェイスごとのローカル ポリシーが、グローバル ローカル ポリシーよりも優先されます。ただし、インターフェイスにデフォルトのローカル ポリシーが設定されている場合、ルータはそのインターフェイスに着信した RSVP メッセージとグローバル ローカル ポリシーの照合を試みません。ポリシーの優先順位は次のとおりです（高いものから低いものへの順序）。

- デフォルト以外のインターフェイス ポリシー
- デフォルトのインターフェイス ポリシー
- デフォルト以外のグローバル ポリシー
- グローバル デフォルト ポリシー

インターフェイスごとのローカル ポリシーについて注意する必要がある重要な点がいくつかあります。

- インターフェイスごとのローカル ポリシーは、**iprsvpbandwidth** コマンドの代わりになりません。**iprsvpbandwidth** コマンドは、インターフェイスで RSVP が有効になっているかどうかと、RSVP 帯域幅プールのサイズを示します。**iprsvpbandwidth** プールは RSVP のアドミッション コントロール機能によって使用され、インターフェイスごとのポリシーは RSVP のポリシー制御機能によって使用されます。ポリシー制御は、検証、認証、ポリシー制御（承認）、およびアドミッション コントロールからなる RSVP メッセージ処理の第 3 フェーズです。
- インターフェイスに割り当てられたすべてのローカル ポリシーのグループ帯域幅の合計は、**iprsvpbandwidth** コマンドで設定された最大合計帯域幅よりも大きくなる可能性があります。ただし、**iprsvpbandwidth** コマンドは予約を許可するために十分な帯域幅があるかどうかを最終的に判断します。

例

ACL、デフォルト、および自律システムベースのポリシー

次の例では、192.168.101.0 サブネット内の任意の RSVP ノードは予約要求の開始または応答を行うことができますが、他のすべてのノードは予約要求への応答のみができます。これは、任意の 192.168.101.x ノードで、PATH、PATHERROR、RESV、または RESVERROR メッセージを送受信できることを意味します。他のすべてのノードでは RESV または RESVERROR メッセージのみを送信できるため、自律システム 1 のすべての予約が拒否されます。

```
Router# configure terminal
Router(config)# access-list 104 permit ip 192.168.101.0 0.0.0.255 any
Router(config)# ip rsvp policy local acl 104
Router(config-rsvp-policy-local)# forward all
Router(config-rsvp-policy-local)# exit
Router(config)# ip rsvp policy local default
```

```
Router(config-rsvp-policy-local)# forward resv
Router(config-rsvp-policy-local)# forward resverror
Router(config-rsvp-policy-local)# exit
Router(config)# ip rsvp policy local origin-as 1
Router(config-rsvp-policy-local)# end
```

アプリケーション ID ベースのポリシー

RSVP は、ID を持つ着信 RSVP メッセージを設定された ID とポリシーに一致させます。次の例では、RSVP シグナリングが行われているインターフェイスに関係なく、ルータ全体のボイス コールを 200 kbps に制限するグローバル RSVP ローカル ポリシーを設定します。

```
Router# configure terminal
Router(config)# ip rsvp policy local identity rsvp-voice policy-locator
"GUID=www.cisco.com, APP=Voice"
Router(config)# ip rsvp policy local identity rsvp-voice
Router(config-rsvp-local-policy)# forward all
Router(config-rsvp-local-policy)# maximum bandwidth group 200
Router(config-rsvp-local-policy)# end
```

インターフェイスごとのアプリケーション ID ベースのポリシー

次の例では、シリアル インターフェイス 2/0/0 のすべての RSVP ボイス コールを合計 200 kbps に制限するローカル ポリシーを設定します。

```
Router# configure terminal
Router(config)# ip rsvp policy local identity rsvp-voice policy-locator APP=Voice
Router(config)# interface serial2/0/0
Router(config-if)# ip rsvp policy local identity rsvp-voice
Router(config-rsvp-local-policy)# forward all
Router(config-rsvp-local-policy)# maximum bandwidth group 200
Router(config-rsvp-local-policy)# exit
Router(config-if)# ip rsvp policy local default
Router(config-rsvp-local-policy)# forward all
Router(config-rsvp-local-policy)# maximum bandwidth group 50
Router(config-rsvp-local-policy)# end
```

DSCP ベースのポリシー

次の例では、RSVP 集約予約を RSVP セッション オブジェクトの DSCP 値 46 と照合し、設定および保持優先順位 5 で preempt-priority を設定するようにローカル ポリシーを設定します。

```
Router# configure terminal
Router(config)# ip rsvp policy local dscp-ip 46
Router(config-rsvp-local-policy)# forward all
Router(config-rsvp-local-policy)# preempt-priority 5 5
Router(config-rsvp-local-policy)# end
```

関連コマンド

コマンド	説明
debugiprsvpfilter	RSVP デバッグ メッセージ フィルタのデバッグ メッセージを表示します。
iprsvppolicypreempt	RSVP が優先順位の低い予約から新しい優先順位の高い予約に帯域幅を再配布できるようにします。
showiprsvppolicy	設定されたローカル ポリシーを表示します。
show ip rsvp policy cops	ポリシー サーバのアドレス、ACL ID、および COPS サーバへのルータの TCP 接続の現在の状態を表示します。
showiprsvppolicylocal	設定されている選択されたローカル ポリシーを表示します。
tunnelmplstraffic-engpriority	MPLS トラフィック エンジニアリング トンネルの設定および予約プライオリティを設定します。

ip rsvp policy preempt

リソース予約プロトコル（RSVP）が優先順位の低い予約から帯域幅を取得して、新しい優先順位の高い予約に割り当てられるようにするには、グローバル コンフィギュレーション モードで **iprsvppolicypreempt** 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。

ip rsvp policy preempt
no ip rsvp policy preempt

構文の説明

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

RSVP は、優先順位の低い予約から優先順位の高い予約に帯域幅を再割り当てしません。

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	変更箇所
12.2(13)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

各ポリシーのプリエンプション パラメータを個別に設定せずに、設定されているすべてのローカル ポリシーとリモート ポリシーのプリエンプション パラメータを有効または無効にするには、**iprsvppolicypreempt** コマンドを使用します。このコマンドにより、RSVP ホストまたはアプリケーションの 1 つのグループに対して、優先的な QoS 処理を使用できます。

例

次に、プリエンプションを有効にする例を示します。

```
Router(config)# ip rsvp policy preempt
```

次に、プリエンプションを無効にする例を示します。

```
Router(config)# no ip rsvp policy preempt
```

関連コマンド

コマンド	説明
showiprsvppolicy	設定されたローカル ポリシーを表示します。

ip rsvp policy vrf

Virtual Routing and Forwarding（VRF）インスタンスのリソース予約プロトコル（RSVP）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 **iprsvppolicyvrf** コマンドを使用します。VRF 固有の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。

ip rsvp policy vrf *vrf-name* {**identity** *alias* **policy-locator** *regular-expression*|**local** {**acl acl1 [acl2...acl8]|default|identity** *alias1* [*alias2...alias4*]|**origin-as** *as1* [*as2...as8*]}}
no ip rsvp policy vrf *vrf-name* {**identity** *alias* **policy-locator** *regular-expression*|**local** {**acl acl1 [acl2...acl8]|default|identity** *alias1* [*alias2...alias4*]|**origin-as** *as1* [*as2...as8*]}}

構文の説明

vrf-name	指定した VRF の名前です。
identity	RSVP メッセージの POLICY-DATA オブジェクトで伝えられる固有の情報です。
alias	RSVP コンフィギュレーション コマンドと show 表示で ID を参照するためにルータ内で使用される文字列です。文字列には、印刷可能文字（0x20 ～ 0x7E の範囲）を 64 文字まで使用できます。 （注） 空白文字または疑問符（?）を、エイリアスの一部またはロケータ文字列自体として使用する場合、空白文字または疑問符を入力する前に、CTRL/V キー シーケンスを入力する必要があります。エイリアスが他のルータに送信されることはありません。
policy-locator	RSVP メッセージで伝えられ、X.500 識別名（DN）形式のアプリケーション ID を含む文字列です。
regular-expression	複数の X.500 DN に一致できるローカル ポリシーで使用する、単一 ID を設定できるパターン一致文字列の一種です。
local	ローカル ポリシーです。
acl	ローカル ポリシーのアクセス コントロール リスト（ACL）です。
acl1 acl2...acl8	ACL です。各 ACL の値は 1 ～ 199 です。 （注） 少なくとも 1 つの ACL を ACL ベースのポリシーに関連付ける必要があります。ただし、関連付けることができるのは最大で 8 つです。
default	RSVP メッセージが ACL、ID、または自律システムに一致しない場合に使用されるポリシーです。
identity	アプリケーション ID です。

alias1 [*alias2...alias4*]	**iprsvppolicyidentity** コマンドを使用して以前に設定されたアプリケーション ID のアプリケーション ID エイリアスです。 （注） 少なくとも 1 つのエイリアスをアプリケーション ID ベースのポリシーに関連付ける必要があります。ただし、関連付けることができるのは最大で 4 つです。
origin-as	自律システム（AS）です。
as1 [*as2...as8*]	AS です。各自律システムの値は 1 ～ 65535 です。 （注） 少なくとも 1 つの自律システムを自律システムベースのポリシーに関連付ける必要があります。ただし、関連付けることができるのは最大で 8 つです。

コマンド デフォルト

VRF の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（config）

コマンド履歴

リリース	変更箇所
15.0(1)M	このコマンドが導入されました。

使用上のガイドライン

存在しない VRF を入力すると、次のエラー メッセージが表示されます。

```
RSVP error: VRF: myvrf doesn't exist.First create this VRF.
```

エラー メッセージを削除するには、myvrf という名前の VRF を作成し、コマンドを再発行します。

ルータで VRF 固有のポリシーを設定し、その VRF がルータから削除された場合は、その VRF に設定されたすべてのポリシーも設定から削除されます。

例

次に、myvrf という名前の VRF を作成した後に、ローカル デフォルト ポリシーを設定する例を示します。

```
Router(config)# ip rsvp policy vrf myvrf local default
```

関連コマンド

コマンド	説明
iprsvppolicyidentity	RSVP アプリケーション ID を定義します。
iprsvppolicylocal	RSVP ローカル ポリシーを定義します。

ip rsvp pq-profile

重み付け均等化キューイング（WFQ）内でプライオリティキュー（PQ）に直接送信するフローを決定するために使用するリソース予約プロトコル（RSVP）の基準を指定するには、グローバル コンフィギュレーション モードで **iprsvppq-profile** コマンドを使用します。指定した基準を無効にするには、このコマンドの **no** 形式を使用します。

ip rsvp pq-profile [{*voice-like*|*r'* [*b'* [{*p-to-r'ignore-peak-value*}]]}]
no ip rsvp pq-profile

構文の説明

voice-like	（任意）ほとんどの音声フローに十分な pq-profile パラメータを示します。r'、b'、および p-to-r' のデフォルト値が使用されます。これらの値により、Cisco IOS アプリケーションから生成されたすべての音声フローと、Microsoft NetMeeting などのその他の RSVP アプリケーションの音声フローの大半が、PQ に直接送信されるようになります。
r'	（任意）フローの最大レートを、バイト/秒で示します。有効な範囲は、1 ～ 1048576 バイト/秒です。
b'	（任意）フローの最大バーストを、バイトで示します。有効な範囲は、1 ～ 8192 バイトです。
p-to-r'	（任意）平均レートに対するピーク レートの最大比をパーセンテージで示します。有効範囲は 100 ～ 4000% です。
ignore-peak-value	（任意）RSVP によりフローが識別されたときに、フローのピーク レートと平均レートの比率が評価されないことを示します。

コマンド デフォルト

r' のデフォルト値は 12288 バイト/秒です。

b' のデフォルト値は 592 バイトです。

p-to-r' のデフォルト値は 110% です。

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	変更箇所
12.1(3)T	このコマンドが導入されました。
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。

使用上のガイドライン

このコマンドを使用して、WFQ システム内の PQ に入れられる RSVP フローのプロファイルを定義します。有効にできるプロファイルは一度に 1 つだけです。この設定の変更は、新しいフローにのみ影響し、既存のフローには影響しません。

このコマンドは、RSVP および WFQ を実行しているインターフェイスにのみ適用されます。

RSVP は、受信側のフロースペック内の r、b、および p の値に基づいて、音声フローを認識します。受信側のフロースペック パラメータが以下のデフォルトの基準を満たす限り、予約されたフローが PQ に与えられます。

(r <= r') AND (b <= b') AND (p/r <= p-to-r')

例

次に、（音声のデフォルト基準を使用して）voice-like フローを PQ に入れる例を示します。

```
Router(config)# ip rsvp pq-profile
Router(config)# ip rsvp pq-profile voice-like
Router(config)# ip rsvp pq-profile 12288 592 110
Router(config)# default ip rsvp pq-profile
Router# show running-config | include pq-profile
```

次に、音声の基準に一致するすべてのフローを PQ に入れる例を示します。

```
Router(config)# ip rsvp pq-profile 10240 512 100
Router# show running-config | include pq-profile
ip rsvp pq-profile 10240 512 100
```

次に、フローが PQ に入れられないように定義する例を示します。

```
Router(config)# no ip rsvp pq-profile
Router# show running-config | include pq-profile
no ip rsvp pq-profile
```

次に、r' および b' に与えられた基準と、p-to-r' のデフォルト値を使用してフローを PQ に入れる例を示します。

```
Router(config)# ip rsvp pq-profile 9000 300
Router# show running-config | include pq-profile
ip rsvp pq-profile 9000 300 110
```

次に、r' および b' に与えられた基準を使用し、フローのピーク値を無視してフローを PQ に入れる例を示します。

```
Router(config)# ip rsvp pq-profile 9000 300 ignore-peak-value
Router# show running-config | include pq-profile
ip rsvp pq-profile 9000 300 ignore-peak-value
```

次に、G.711 または適応差分パルス符号変調（ADPCM）コーデックを使用して Microsoft NetMeeting の音声フローを PQ に入れる例を示します。

```
Router(config)# ip rsvp pq-profile 10200 1200
```

ip rsvp precedence から load protocol

- ip rsvp precedence （339 ページ）
- ip rsvp qos （342 ページ）
- ip rsvp reservation （343 ページ）
- ip rsvp reservation-host （347 ページ）
- ip rsvp resource-provider （351 ページ）
- ip rsvp sender （353 ページ）
- ip rsvp sender-host （356 ページ）
- ip rsvp signalling dscp （359 ページ）
- ip rsvp signalling fast-local-repair notifications （360 ページ）
- ip rsvp signalling fast-local-repair rate （362 ページ）
- ip rsvp signalling fast-local-repair wait-time （364 ページ）
- ip rsvp signalling hello（コンフィギュレーション） （365 ページ）
- ip rsvp signalling hello（インターフェイス） （366 ページ）
- ip rsvp signalling hello dscp （368 ページ）
- ip rsvp signalling hello graceful-restart （370 ページ）
- ip rsvp signalling hello graceful-restart dscp （371 ページ）
- ip rsvp signalling hello graceful-restart mode （372 ページ）
- ip rsvp signalling hello graceful-restart mode help-neighbor （374 ページ）
- ip rsvp signalling hello graceful-restart neighbor （376 ページ）
- ip rsvp signalling hello graceful-restart refresh interval （378 ページ）
- ip rsvp signalling hello graceful-restart refresh misses （380 ページ）
- ip rsvp signalling hello graceful-restart send （382 ページ）
- ip rsvp signalling hello refresh interval （384 ページ）
- ip rsvp signalling hello refresh misses （386 ページ）
- ip rsvp signalling hello reroute dscp （388 ページ）
- ip rsvp signalling hello reroute refresh interval （390 ページ）
- ip rsvp signalling hello reroute refresh misses （391 ページ）
- ip rsvp signalling hello statistics （392 ページ）
- ip rsvp signalling initial-retransmit-delay （393 ページ）

- ip rsvp signalling patherr state-removal （394 ページ）
- ip rsvp signalling rate-limit （396 ページ）
- ip rsvp signalling refresh interval （398 ページ）
- ip rsvp signalling refresh misses （400 ページ）
- ip rsvp signalling refresh reduction （402 ページ）
- ip rsvp signalling refresh reduction ack-delay （404 ページ）
- ip rsvp snooping （405 ページ）
- ip rsvp source （407 ページ）
- ip rsvp svc-required （409 ページ）
- ip rsvp tos （411 ページ）
- ip rsvp transport （414 ページ）
- ip rsvp transport sender-host （416 ページ）
- ip rsvp tunnel overhead-percent （418 ページ）
- ip rsvp udp-multicasts （420 ページ）
- ip rsvp udp neighbor （422 ページ）
- ip rtp compression-connections （423 ページ）
- ip rtp header-compression （425 ページ）
- ip rtp priority （429 ページ）
- ip tcp compression-connections （433 ページ）
- ip tcp header-compression （435 ページ）
- iphc-profile （438 ページ）
- lacp max-bundle （442 ページ）
- lane client qos （443 ページ）
- lane qos database （444 ページ）
- load protocol （446 ページ）

ip rsvp precedence

ルータがリソース予約プロトコル（RSVP）フロースペックに適合するパケットまたはそれを超えるパケットに指定された値を使用して、RSVP 予約済みパス内のパケットのタイプ オブ サービス（ToS）バイトの IP プレシデンス値をマークできるようにするには、インターフェイス コンフィギュレーション モードで **iprsvpprecedence** コマンドを使用します。既存の IP プレシデンス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。

ip rsvp precedence {**conform** *precedence-value*|**exceed** *precedence-value*}
no ip rsvp precedence [{**conform**|**exceed**}]

構文の説明

conform *precedence-value*	RSVP フロースペックに適合するトラフィックの IP プレシデンス値を 0 ～ 7 の範囲で指定します。IP プレシデンス値は、パケットの IP ヘッダーの ToS バイトの上位 3 ビット（ビット 5 ～ 7）に書き込まれます。**conform** または **exceed** キーワードが必要です。両方のキーワードを指定することもできます。 このコマンドの **no** 形式で使用する場合は、**conform** キーワードはオプションになります。
exceed *precedence-value*	RSVP フロースペックを超えるトラフィックの IP プレシデンス値を 0 ～ 7 の範囲で指定します。IP プレシデンス値は、パケットの IP ヘッダーの ToS バイトの上位 3 ビット（ビット 5 ～ 7）に書き込まれます。**conform** または **exceed** キーワードが必要です。両方のキーワードを指定することもできます。 このコマンドの **no** 形式で使用する場合は、**exceed** キーワードはオプションになります。

コマンド デフォルト

このコマンドが使用されていない場合は、ToS バイトの IP プレシデンス ビットは変更されません。デフォルトの状態は、**noiprsvpprecedence** コマンドを実行したときの状態と同じです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
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。

使用上のガイドライン

RSVP 予約済みパスのパケットは、予約フロースペックに適合するパケットと、予約に対応するものの予約フロースペックを超える（または、予約フロースペック外の）パケットの、2 つのクラスに分類されます。

iprsvpprecedence コマンドにより、この 2 つのクラスに属するパケットに適用する IP プレシデンス値を設定できます。このコマンドを使用する場合は、トラフィックの少なくとも 1 つのクラスに IP プレシデンス値を指定する必要があります。コマンドの単一のインスタンスを使用して、両方のクラスの値を指定することができます。この場合、**conform** および **exceed** キーワードを任意の順序で指定できます。

入力処理の一部として、RSVP は **iprsvpprecedence** コマンドを使用し、適合するパケットと適合しないパケットに IP プレシデンス ビットを設定します。per-VC DWRED が設定されている場合、システムはパケット ドロップ プロセスで出力インターフェイスの IP プレシデンス ビット設定と ToS ビット設定を使用します。パケットの IP プレシデンス設定は、ダウンストリーム ルータのインターフェイスでも使用できます。

iprsvpprecedence コマンドを実行すると、インターフェイス上にあるすべての既存の予約の IP プレシデンス値が変更されます。

（注） このコマンドを使用するには、インターフェイスで RSVP を有効にする必要があります。つまり、**iprsvpbandwidth** コマンドを使用してから、**iprsvpprecedence** コマンドを使用する必要があります。RSVP は、VIP 分散型シスコ エクスプレス フォワーディング（dCEF）で設定できません。

RSVP は、基礎となる転送メカニズムからパケットを受信します。そのため、**iprsvpprecedence** コマンドを使用して IP プレシデンスを設定するには、次のいずれかの機能が必要です。

- インターフェイスで重み付け均等化キューイング（WFQ）が有効になっている必要があります。
- RSVP 相手先選択接続（SVC）が使用されている必要があります。
- RSVP を支援するように NetFlow が設定されている必要があります。

（注） このコマンドの **no** 形式を使用することは、以前のプレシデンス設定にかかわらず、パケットのすべてのプレシデンスを 0 に設定する **iprsvpprecedence0** コマンドを使用することと同じではありません。

例

次の例では、ATM インターフェイス 0 上の RSVP フロースペックに適合するすべてのトラフィックに対して IP プレシデンス値を 3 に設定し、フロースペックを超えるすべてのトラフィックに対して IP プレシデンス値を 2 に設定します。

```
interface atm0
 ip rsvp precedence conform 3 exceed 2
```

次の例では、ATM インターフェイス 1 上の RSVP フロースペックに適合するすべてのトラフィックに対して IP プレシデンス値を 2 に設定します。フロースペックを超えるパケットの IP プレシデンス値は変更されません。

```
interface ATM1
 ip rsvp precedence conform 2
```

関連コマンド

Command	Description
ip rsvp bandwidth	インターフェイスで IP 用 RSVP をイネーブルにします。
ip rsvp policy cops minimal	COPS サーバの負荷を軽減し、管理対象ルータでのメッセージの遅延時間を改善します。
iprsvptos	RSVP フロースペックに適合するパケットまたは RSVP フロースペックを超過するパケットに適用する ToS 値を設定できます。
s howiprsvp	指定されたインターフェイスの、RSVP フロースペックに適合するパケットまたは RSVP フロースペックを超過するパケットに適用される IP プレシデンス ビット値と ToS ビット値を表示します。

ip rsvp qos

マルチプロトコル ラベル スイッチング トラフィック エンジニアリング（MPLS TE）を実行しているルータでリソース予約プロトコル（RSVP）の Quality of Service（QoS）フローを有効にするには、グローバル コンフィギュレーション モードで **iprsvpqos** コマンドを使用します。RSVP QoS フローを無効にするには、このコマンドの **no** 形式を使用します。

ip rsvp qos
no ip rsvp 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

RSVP QoS フロー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	変更箇所
12.2(33)SRC	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

RSVP QoS フローと MPLS TE が有効になっている場合は、ルータが RSVP ラベル スイッチド パス（LSP）および IPv4 メッセージ（PATH や RESV など）を処理およびインストールします。IPv4 および LSP がインストールされた状態で RSVP QoS フローおよび MPLS TE が無効になると、インストールされているすべての IPv4 状態がただちにクリアされます。LSP 状態は変更されません。追加の更新または新しい IPv4 RSVP メッセージは、変更されずに転送されます。

showiprsvp コマンドを使用して、**iprsvpqos** コマンドの状態を表示します。

例

次の例では、MPLS TE を実行しているルータの RSVP QoS フローを設定します。

```
Router> enable
Router# configure terminal
Router(config)# ip rsvp qos
```

関連コマンド

コマンド	説明
showiprsvp	RSVP カテゴリの詳細情報を表示します。

ip rsvp reservation

ルータがダウンストリーム ホストからのリソース予約プロトコル（RSVP）RESV メッセージの受信をシミュレートできるようにするには、グローバル コンフィギュレーション モードで **iprsvpreservation** 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。

ip rsvp reservation *session-ip-address sender-ip-address* {*ip-protocol*|**tcp**|**udp**} *session-dest-port sender-source-port next-hop-address next-hop-interface* {**ff**|**se**|**wf**} {**load**|**rate**} *bandwidth burst-size* [**identity** *alias*]
no ip rsvp reservation *session-ip-address sender-ip-address* {*ip-protocol*|**tcp**|**udp**} *session-dest-port sender-source-port next-hop-address next-hop-interface* {**ff**|**se**|**wf**} {**load**|**rate**} *bandwidth burst-size* [**identity** *alias*]

構文の説明

session-ip-address	ユニキャストセッションの場合は、対象とする受信者のアドレスです。マルチキャスト セッションの場合は、セッションの IP マルチキャスト アドレスです。
sender-ip-address	送信元の IP アドレス。
ip-protocol |**tcp** | **udp**	IP プロトコルを 0 ～255 の範囲の TCP または UDP で指定します。
session-dest-port *sender-source-port*	*session-dest-port* 引数は、宛先ポートです。*sender-source-port* 引数は、送信元ポートです。ポート番号は、すべてのケースで指定します。IP ヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先をゼロにする場合は、送信元もゼロにする必要があります。これは、ポートがチェックされないことを意味します。宛先をゼロ以外にする場合は、送信元もゼロ以外にする必要があります（ワイルドカードフィルタ予約を除きます。この場合、送信元ポートは常に無視されるため、ゼロにすることができます）。
next-hop-address	受信者または受信者に最も近いルータのホスト名または IP アドレスです。
next-hop-interface	ネクストホップのインターフェイスまたはサブインターフェイスのタイプおよび番号です。インターフェイス タイプには、**ethernet**、**loopback**、**null**、または **serial** を使用できます。
ff | **se** | **wf**	予約スタイルを指定します。 • **ff--**単一の予約による固定フィルタです。 • **se**：共有予約と限られた範囲による明示共有です。 • **wf**：共有予約と無制限の範囲によるワイルドカードフィルタです。
load	制御対象負荷サービスを指定します。

rate	Quality of Service（QoS）保証ビット レート サービスを指定します。
bandwidth	インターフェイス上の合計の最大 75 パーセントを予約する、kbps 単位の平均ビット レートです。範囲は 1 ～ 10000000 です。
burst-size	最大バースト サイズ（キュー内のデータの kbps）です。指定できる範囲は 1 ～ 65535 です。
identity alias	（任意）アプリケーションIDエイリアスを指定します。エイリアスは、印刷可能文字（0x20 ～ 0x7E の範囲）を 64 文字まで使用できる文字列です。 （注） 空白文字または疑問符（?）を、エイリアスの一部またはロケータ文字列自体として使用する場合、空白文字または疑問符を入力する前に、CTRL-V キー シーケンスを入力する必要があります。エイリアスが他のルータに送信されることはありません。

コマンド デフォルト

ルータは RSVP RESV メッセージの受信をシミュレートしません。

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	変更箇所
11.2	このコマンドが導入されました。
12.4(6)T	このコマンドが変更されました。オプションの **identity***alias* キーワードと引数の組み合わせが追加されました。
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。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

iprsvpreservation コマンドを使用して、ルータがダウンストリーム ホストからの RSVP RESV メッセージの受信をシミュレートするようにして、そのホストの RSVP RESV メッセージをプロキシします。ローカル（ループバック）ネクストホップアドレスとネクストホップインターフェイスを指定することで、このコマンドを使用して設定するルータの RSVP をプロキシすることや、**iprsvpreservation-host** コマンドを使用することもできます。

エイリアスは、**iprsvpidentity** コマンドを使用して作成した RSVP ID を参照する必要があります。この ID に関連付けられた policy-locator 文字列が、RESV メッセージで伝えられます。この ID は、一致する PATH メッセージに含まれているアプリケーション ID を上書きします。

一致する PATH メッセージにアプリケーション ID があり、**iprsvpreservation** コマンドを使用してアプリケーション ID を指定していない場合には、RESV メッセージにはアプリケーション ID は含まれません。ただし、**iprsvplistener** コマンドによってプロキシされた RESV メッセージは、一致する PATH メッセージ アプリケーション ID をプロキシされた RESV メッセージに入れます。

例

次の例では、100 または 150 kbps のトークン バケットと、60 または 65 kbps の最大キューの深さを使用する、共有明示スタイルの予約と制御対象負荷サービスの使用を指定します。

```
Router(config)# ip rsvp reservation 192.168.0.2 172.16.1.1 udp 20 30 172.16.4.1 Ethernet1
 se load 100 60
Router(config)# ip rsvp reservation 192.168.0.2 172.16.2.1 tcp 20 30 172.16.4.1 Ethernet1
 se load 150 65
```

次の例では、300 または 350 kbps のトークンバケット、60 または 65 kbps の最大キューの深さ、およびアプリケーション ID を使用する、ワイルドカード フィルタ スタイルの予約と保証ビット レート サービスの使用を指定します。

```
Router(config)# ip rsvp reservation 192.168.0.3 0.0.0.0 udp 20 0 172.16.4.1 Ethernet1
wf rate 300 60 identity xyz
Router(config)# ip rsvp reservation 192.168.1.1 0.0.0.0 udp 20 0 172.16.4.1 Ethernet1
wf rate 350 65 identity xyz
```

ワイルドカードフィルタでは送信者の指定が許可されないことに注意してください。すべての送信者が承認されます。このアクションは、発信元アドレスとポートをゼロに設定することで示されます。どのフィルタ スタイルでも、宛先ポートがゼロに指定されている場合、RSVP では送信元ポートを他のポートにすることは許可されません。このようなプロトコルではポートが使用されないと認識されるか、この指定がすべてのポートに適用されると認識されます。

関連コマンド

Command	Description
ip rsvp bandwidth	インターフェイスで IP 用 RSVP をイネーブルにします。
ip rsvp identity	RSVP アプリケーション ID を定義します。
ip rsvp neighbor	承認済みとするネイバーをルータが制御できるようにします。
iprsvpreservation-host	RSVP RESV メッセージを生成するホストをシミュレートするようにルータをイネーブルにします。
iprsvpsender	ルータが RSVP PATH メッセージの受信をシミュレートできるようにします。

Command	Description
iprsvpsender-host	ルータで RSVP PATH メッセージを生成するホストをシミュレートできるようにします。
showiprsvpinstalled	RSVP 関連の帯域幅情報を表示します。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。
showiprsvpneighbor	現在の RSVP ネイバーを表示します。
show ip rsvp policy identity	ルータ設定で選択された RSVP ID を表示します。
showiprsvpreservation	現在データベースに格納されている RSVP RESV 関連の受信側情報を表示します。
showiprsvpsender	現在データベース上に存在する RSVP PATH 関連の送信側情報を表示します。

ip rsvp reservation-host

ルータがリソース予約プロトコル（RSVP）RESV メッセージを生成するホストをシミュレートできるようにするには、グローバル コンフィギュレーション モードで**iprsvpreservation-host** 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。

ip rsvp reservation-host *session-ip-address sender-ip-address* {*ip-protocol*|**tcp**|**udp**} *session-dest-port sender-source-port* {**ff**|**se**|**wf**} {**load**|**rate**} *bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]
no ip rsvp reservation-host *session-ip-address sender-ip-address* {*ip-protocol*|**tcp**|**udp**} *session-dest-port sender-source-port* {**ff**|**se**|**wf**} {**load**|**rate**} *bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]

構文の説明

session-ip-address	ユニキャストセッションの場合は、対象とする受信者のアドレスです。IP マルチキャストアドレスは、この引数では使用できません。設定するルータのインターフェイスに設定された論理アドレスである必要があります。
sender-ip-address	送信元の IP アドレス。
ip-protocol | **tcp** | **udp**	IP プロトコルを 0 ～255 の範囲の TCP または UDP で指定します。
session-dest-port sender-source-port	*session-dest-port* 引数は、宛先ポートです。*sender-source-port* 引数は、送信元ポートです。ポート番号は、すべてのケースで指定します。IP ヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先をゼロにする場合は、送信元もゼロにする必要があります。これは、ポートがチェックされないことを意味します。宛先をゼロ以外にする場合は、送信元もゼロ以外にする必要があります（ワイルドカードフィルタ予約を除きます。この場合、送信元ポートは常に無視されるため、ゼロにすることができます）。
ff | **se** | **wf**	予約スタイルを指定します。 • **ff--**単一の予約による固定フィルタです。 • **se**：共有予約と限られた範囲による明示共有です。 • **wf**：共有予約と無制限の範囲によるワイルドカードフィルタです。
load	制御対象負荷サービスを指定します。
rate	Quality of Service（QoS）保証ビット レート サービスを指定します。
bandwidth	インターフェイス上の合計の最大 75 パーセントを予約する、kbps 単位の平均ビット レートです。範囲は 1 ～ 10000000 です。
burst-size	最大バーストサイズ（キュー内のデータの kbps）です。指定できる範囲は 1 ～ 65535 です。

identity alias	（任意）アプリケーションIDエイリアスを指定します。エイリアスは、印刷可能文字（0x20 ～ 0x7E の範囲）を 64 文字まで使用できる文字列です。 （注） 空白文字または疑問符（?）を、エイリアスの一部またはロケータ文字列自体として使用する場合、空白文字または疑問符を入力する前に、CTRL-V キーシーケンスを入力する必要があります。エイリアスが他のルータに送信されることはありません。
vrfvrf-name	（任意）仮想ルーティングおよび転送（VRF）インスタンスを指定します。

コマンド デフォルト

ルータは RSVP RESV メッセージを生成するホストをシミュレートしません。

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	変更箇所
12.0	このコマンドが導入されました。
12.4(6)T	このコマンドが変更されました。オプションの **identity***alias* キーワードと引数の組み合わせが追加されました。
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。
15.0(1)M	このコマンドが変更されました。オプションの **vrf***vrf-name* キーワードと引数の組み合わせが追加されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

（注） コマンドの構文は、プラットフォームとリリースによって異なります。**vrf***vrf-name* キーワードと引数の組み合わせは、ASR 1000 シリーズアグリゲーション サービス ルータではサポートされていません。

iprsvpreservation-host コマンドを使用して、ルータが独自の RSVP RESV メッセージを生成するホストをシミュレートするようにします。このコマンドは、ルータが別のホストの代わりに

RESV メッセージを生成するようにできる、**iprsvpreservation** コマンドと似ています。**iprsvpreservation-host** コマンドと **iprsvpreservation** コマンドの主な違いは、次のとおりです。

- **iprsvpreservation-host** コマンドを入力する場合、*session-ip-address* 引数はルータのインターフェイスに設定されているローカルアドレスにする必要があります。そのため、別のホスト宛てのフローの代わりに予約をプロキシすることはできません。また、このコマンドを使用してマルチキャスト セッションの予約メッセージを生成することはできません。
- メッセージは設定するルータから発信されたものとみなされるため、**iprsvpreservation-host** コマンドを入力するときは、RSVP RESV メッセージのネクストホップまたは着信インターフェイスを指定しません。
- **iprsvpreservation-host** コマンドは RSVP に対応していないホストまたはマルチキャスト セッションのために RSVP をプロキシするために使用することはできないため、デバッグとテストの目的で使用します。

エイリアスは、**iprsvpidentity** コマンドを使用して作成した RSVP ID を参照する必要があります。この ID に関連付けられた policy-locator 文字列が、RESV メッセージで伝えられます。この ID は、一致する PATH メッセージに含まれているアプリケーション ID を上書きします。

一致する PATH メッセージにアプリケーション ID があり、**iprsvpreservation-host** コマンドを使用してアプリケーション ID を指定していない場合には、RESV メッセージにはアプリケーション ID は含まれません。ただし、**iprsvplistener** コマンドによってプロキシされた RESV メッセージは、一致する PATH メッセージ アプリケーション ID をプロキシされた RESV メッセージに入れます。

例

次の例では、100 または 150 kbps のトークンバケット、60 または 65 kbps の最大キューの深さ、およびアプリケーション ID を使用する、共有明示スタイルの予約と制御対象負荷サービスの使用を指定します。

```
Router(config)# ip rsvp reservation-host 10.1.1.1 10.30.1.4 udp 20 30 se load 100 60
identity xyz
Router(config)# ip rsvp reservation-host 10.40.2.2 10.22.1.1 tcp 20 30 se load 150 65
identity xyz
```

関連コマンド

Command	Description
iprsvpbandwidth	インターフェイスで IP 用 RSVP をイネーブルにします。
ip rsvp identity	RSVP アプリケーション ID を定義します。
iprsvpneighbor	承認済みとする RSVP ネイバーをルータが制御できるようにします。
iprsvpreservation	ルータが RSVP RESV メッセージの受信をシミュレートできるようにします。
ip rsvp sender	ルータが RSVP PATH メッセージの受信をシミュレートできるようにします。

Command	Description
ip rsvp sender-host	ルータで RSVP PATH メッセージを生成するホストをシミュレートできるようにします。
showiprsvpinstalled	RSVP 関連の帯域幅情報を表示します。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。
showiprsvpneighbor	現在の RSVP ネイバーを表示します。
show ip rsvp policy identity	ルータ設定で選択された RSVP ID を表示します。
showiprsvpreservation	現在データベースに格納されている RSVP RESV 関連の受信側情報を表示します。
showiprsvpsender	現在データベース上に存在する RSVP PATH 関連の送信側情報を表示します。

ip rsvp resource-provider

集約フローのリソースプロバイダーを設定するには、インターフェイスコンフィギュレーション モードで **iprsvpresource-provider** コマンドを使用します。集約フローのリソース プロバイダーを無効にするには、このコマンドの **no** 形式を使用します。

ip rsvp resource-provider {**none**|**wfq interface**|**wfq pvc**}
no ip rsvp resource-provider

構文の説明

none	インターフェイス上でリソースプロバイダーが設定されているかどうかにかかわらず、リソース プロバイダーを指定しません。
wfqinterface	インターフェイスのリソース プロバイダーとして重み付け均等化キューイング（WFQ）を指定します。
wfqpvc	相手先固定接続（PVC）または接続のリソース プロバイダーとして WFQ を指定します。

コマンド デフォルト

リソース予約プロトコル（RSVP）がインターフェイスに設定するデフォルトのリソース プロバイダーは、WFQ（**wfqinterface** キーワード）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（config-if）

コマンド履歴

リリース	変更箇所
12.2(2)T	このコマンドが導入されました。
12.0(24)S	このコマンドが、Cisco IOS Release 12.0(24)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(18)SXF2	このコマンドが、Cisco IOS Release 12.2(18)SXF2 に統合されました。
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。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

（注） コマンドの構文は、プラットフォームとイメージによって異なります。**wfqinterface** キーワードと **wfqpvc** キーワードは、Cisco ASR 1000 シリーズ ルータではサポートされません。

iprsvpresource-provider コマンドを使用して、予約をインストールするときに RSVP が対話するリソース プロバイダーを設定します。

フロー単位で WFQ を使用する場合に、フローが確実に Quality of Service（QoS）保証を受けるようにするには、リソース プロバイダーとして **wfqinterface** または **wfqpvc** を設定します。データ パケット処理にクラスベース重み付け均等化キューイング（CBWFQ）を使用する場合に、フローが確実に QoS 保証を受けるようにするには、リソース プロバイダーとして **none** を設定します。

（注） 以前は、リソース プロバイダーが QoS プロバイダーと呼ばれていました。

例

次の例では、**iprsvpresource-provider** コマンドが **wfqpvc** をリソース プロバイダーとして設定されており、フロー単位で WFQ を使用する場合に、フローが確実に QoS 保証を受けます。

```
Router# configure terminal
Router(config)# interface atm 6/0
Router(config-if)# ip rsvp resource-provider wfq pvc
```

次の例では、**iprsvpresource-provider** コマンドが **none** をリソース プロバイダーとして設定されており、データ パケット処理に CBWFQ を使用する場合に、フローが確実に QoS 保証を受けます。

```
Router# configure terminal
Router(config)# interface atm 6/0
Router(config-if)# ip rsvp resource-provider none
```

関連コマンド

コマンド	説明
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。

ip rsvp sender

ルータがリソース予約プロトコル（RSVP）PATH メッセージの受信をシミュレートできるようにするには、グローバル コンフィギュレーション モードで **iprsvpsender** 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。

ip rsvp sender *session-ip-address sender-ip-address* {*ip-protocol*|**tcp**|**udp**} *session-dest-port sender-source-port previous-hop-ip-address previous-hop-interface bandwidth burst-size* [**identity** *alias*]
no ip rsvp sender *session-ip-address sender-ip-address* {*ip-protocol*|**tcp**|**udp**} *session-dest-port sender-source-port previous-hop-ip-address previous-hop-interface bandwidth burst-size* [**identity** *alias*]

構文の説明

session-ip-address	ユニキャスト セッションの場合は、対象とする受信者のアドレスです。マルチキャスト セッションの場合は、セッションの IP マルチキャスト アドレスです。
sender-ip-address	送信元の IP アドレス。
ip-protocol | **tcp** | **udp**	IP プロトコルを 0 ～255 の範囲の TCP または UDP で指定します。
session-dest-port *sender-source-port*	*session-dest-port* 引数は、宛先ポートです。*sender-source-port* 引数は、送信元ポートです。ポート番号は、すべてのケースで指定します。IP ヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先をゼロにする場合は、送信元もゼロにする必要があります。これは、ポートがチェックされないことを意味します。宛先をゼロ以外にする場合は、送信元もゼロ以外にする必要があります。
previous-hop-ip-address	送信者または送信者に最も近いルータのアドレスです。
previous-hop-interface	前のホップのインターフェイスまたはサブインターフェイスです。インターフェイス タイプには、**ethernet**、**gigabitethernet**、**loopback**、**null**、または **serial** を使用できます。
bandwidth	インターフェイス上の合計の最大 75 パーセントを予約する、kbps 単位の平均ビット レートです。範囲は 1 ～ 10000000 です。
burst-size	最大バースト サイズ（キュー内のデータの kbps）です。指定できる範囲は 1 ～ 65535 です。

identity *alias*	（任意）アプリケーション ID エイリアスを指定します。エイリアスは、印刷可能文字（0x20 ～ 0x7E の範囲）を 64 文字まで使用できる文字列です。 （注） 空白文字または疑問符（?）を、エイリアスの一部またはロケータ文字列自体として使用する場合、空白文字または疑問符を入力する前に、CTRL-V キー シーケンスを入力する必要があります。エイリアスが他のルータに送信されることはありません。

コマンド デフォルト

ルータは RSVP PATH メッセージの受信をシミュレートしません。

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	変更箇所
11.2	このコマンドが導入されました。
12.4(6)T	このコマンドが変更されました。オプションの **identity***alias* キーワードと引数の組み合わせが追加されました。
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。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

iprsvpsender コマンドを使用して、ルータがアップストリーム ホストからの RSVP PATH メッセージの受信をシミュレートするようにして、そのホストからの RSVP PATH メッセージをプロキシします。ローカル（ループバック）の前のホップのアドレスと前のホップのインターフェイスを含めることで、このコマンドを使用して、設定するルータの RSVP をプロキシすることもできます。

エイリアスは、**iprsvpidentity** コマンドを使用して作成した RSVP ID を参照する必要があります。この ID に関連付けられた policy-locator 文字列が、PATH メッセージで提供されます。

例

次の例では、ルータがループバック インターフェイス 1 で UDP を使用した RSVP PATH メッセージの受信をシミュレートするように設定します。

```
Router(config)# ip rsvp sender 192.168.0.1 172.16.2.1 udp 20 30 172.16.2.1 loopback1 50
 5 identity xyz
```

```
Router(config)# ip rsvp sender 192.168.0.2 172.16.2.1 udp 20 30 172.16.2.1 loopback1 50
 5 identity xyz
```

関連コマンド

Command	Description
iprsvpbandwidth	インターフェイスで IP 用 RSVP をイネーブルにします。
ip rsvp identity	RSVP アプリケーション ID を定義します。
iprsvpneighbor	承認済みとする RSVP ネイバーをルータが制御できるようにします。
iprsvpreservation	ルータが RSVP RESV メッセージの受信をシミュレートできるようにします。
iprsvpreservation-host	RSVP RESV メッセージを生成するホストをシミュレートするようにルータをイネーブルにします。
ip rsvp sender-host	ルータで RSVP PATH メッセージを生成するホストをシミュレートできるようにします。
showiprsvpinstalled	RSVP 関連の帯域幅情報を表示します。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。
showiprsvpneighbor	現在の RSVP ネイバーを表示します。
show ip rsvp policy identity	ルータ設定で選択された RSVP ID を表示します。
showiprsvpreservation	現在データベースに格納されている RSVP RESV 関連の受信側情報を表示します。
showiprsvpsender	現在データベース上に存在する RSVP PATH 関連の送信側情報を表示します。

ip rsvp sender-host

ルータがリソース予約プロトコル（RSVP）PATH メッセージを生成するホストをシミュレートできるようにするには、グローバル コンフィギュレーション モードで **iprsvpsender-host** 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。

ip rsvp sender-host *session-ip-address sender-ip-address* {*ip-protocol*|**tcp**|**udp**} *session-dest-port sender-source-port bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]
no ip rsvp sender-host *session-ip-address sender-ip-address* {*ip-protocol*|**tcp**|**udp**} *session-dest-port sender-source-port bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]

構文の説明

session-ip-address	ユニキャストセッションの場合は、対象とする受信者のアドレスです。マルチキャスト セッションの場合は、セッションの IP マルチキャスト アドレスです。
sender-ip-address	送信元の IP アドレス。設定するルータのインターフェイスに設定された論理アドレスである必要があります。
ip-protocol |**tcp** | **udp**	IP プロトコルを 0 ～255 の範囲の TCP または UDP で指定します。
session-dest-port *sender-source-port*	*session-dest-port* 引数は、宛先ポートです。*sender-source-port* 引数は、送信元ポートです。ポート番号は、すべてのケースで指定します。IPヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先をゼロにする場合は、送信元もゼロにする必要があります。これは、ポートがチェックされないことを意味します。宛先をゼロ以外にする場合は、送信元もゼロ以外にする必要があります。
bandwidth	インターフェイス上の合計の最大 75 パーセントを予約する、kbps 単位の平均ビット レートです。範囲は 1 ～ 10000000 です。
burst-size	最大バースト サイズ（キュー内のデータの kbps）です。指定できる範囲は 1 ～ 65535 です。
identity *alias*	（任意）アプリケーションIDエイリアスを指定します。エイリアスは、印刷可能文字（0x20 ～ 0x7E の範囲）を 64 文字まで使用できる文字列です。 （注） 空白文字または疑問符（?）を、文字列自体の一部として使用する場合、空白文字または疑問符を入力する前に、CTRL-V キー シーケンスを入力する必要があります。エイリアスが他のルータに送信されることはありません。
vrfvrf-name	（任意）仮想ルーティングおよび転送（VRF）インスタンスを指定します。

コマンド デフォルト

ルータは RSVP PATH メッセージの生成をシミュレートしません。

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	変更箇所
12.0	このコマンドが導入されました。
12.4(6)T	このコマンドが変更されました。オプションの **identity***alias* キーワードと引数の組み合わせが追加されました。
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。
15.0(1)M	このコマンドが変更されました。オプションの **vrf***vrf-name* キーワードと引数の組み合わせが追加されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

（注） コマンドの構文は、プラットフォームとリリースによって異なります。**vrf***vrf-name* キーワードと引数の組み合わせは、ASR 1000 シリーズ アグリゲーション サービス ルータではサポートされていません。

iprsvpsender-host コマンドを使用して、ルータが独自の RSVP PATH メッセージを生成するホストをシミュレートするようにします。このコマンドは、ルータが別のホストの代わりにRSVP PATH メッセージを生成するようにできる、**iprsvpsender** コマンドと似ています。
iprsvpsender-host コマンドと **iprsvpsender** コマンドの主な違いは、次のとおりです。

- **iprsvpsender-host** コマンドを入力する場合、*sender-ip-address* 引数はルータのインターフェイスに設定されているローカル アドレスにする必要があります。
- メッセージは設定するルータから発信されたものとみなされるため、**iprsvpsender-host** コマンドを入力するときは、RSVP PATH メッセージの前のホップまたは着信インターフェイスを指定しません。
- **iprsvpsender-host** コマンドは RSVP に対応していないホストのために RSVP をプロキシするために使用することはできないため、デバッグとテストの目的で使用します。

エイリアスは、**iprsvpidentity** コマンドを使用して作成した RSVP ID を参照する必要があります。この ID に関連付けられた policy-locator 文字列が、RESV メッセージで伝えられます。この ID は、一致する PATH メッセージに含まれているアプリケーション ID を上書きします。

例

次の例では、指定されたアドレスにトラフィックを送信するホストのように機能するようにルータを設定します。

```
Router(config)# ip rsvp sender-host 10.0.0.7 10.0.0.1 udp 1 1 10 10 identity xyz
```

関連コマンド

Command	Description
iprsvpbandwidth	インターフェイスで IP 用 RSVP をイネーブルにします。
ip rsvp identity	RSVP アプリケーション ID を定義します。
iprsvpneighbor	承認済みとするネイバーをルータが制御できるようにします。
iprsvpreservation	ルータが RSVP RESV メッセージの受信をシミュレートできるようにします。
iprsvpreservation-host	RSVP RESV メッセージを生成するホストをシミュレートするようにルータをイネーブルにします。
ip rsvp sender	ルータが RSVP PATH メッセージの受信をシミュレートできるようにします。
showiprsvpinstalled	RSVP 関連の帯域幅情報を表示します。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。
showiprsvpneighbor	現在の RSVP ネイバーを表示します。
show ip rsvp policy identity	ルータ設定で選択された RSVP ID を表示します。
showiprsvpreservation	現在データベースに格納されている RSVP RESV 関連の受信側情報を表示します。
showiprsvpsender	現在データベース上に存在する RSVP PATH 関連の送信側情報を表示します。

ip rsvp signalling dscp

インターフェイス上で送信されるすべてのリソース予約プロトコル（RSVP）メッセージで使用される DiffServ コード ポイント（DSCP）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 **iprsvpsignallingdscp** 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。

ip rsvp signalling dscp *value*
no ip rsvp signalling dscp

構文の説明

value	DSCP の番号です。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

デフォルト値は 0 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1	このコマンドが追加されました。
12.2(18)SXF2	このコマンドが、Cisco IOS Release 12.2(18)SXF2 に統合されました。
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。

使用上のガイドライン

フローごとではなく、インターフェイスごとに DSCP を設定します。DSCP は、パケットが宛先に移動するときに、さまざまなホップからパケットが受け取る優先順位を決定します。

DSCP は、特定のインターフェイスにインストールされたすべての RSVP フローに適用されます。DSCP のために各インターフェイスを個別に設定できます。

例

これは、DSCP 値が 6 の **iprsvpsignallingdscp** コマンドの一例です

```
Router(config-if)# ip rsvp signalling dscp 6
Router(config-if)# end
```

DSCP 値を確認するには、**showiprsvpinterfacedetail** コマンドを入力します。

```
Router# show ip rsvp interface serial2/0 detail
Se2/0:
   Bandwidth:
     Curr allocated:10K bits/sec
     Max. allowed (total):1536K bits/sec
     Max. allowed (per flow):1536K bits/sec
   Neighbors:
     Using IP enacp:1.  Using UDP encaps:0
   DSCP value used in Path/Resv msgs:0x6
   Burst Police Factor:300%
   RSVP:Data Packet Classification provided by: none
```

ip rsvp signalling fast-local-repair notifications

リソース予約プロトコル（RSVP）が一時停止する前に高速ローカル修復（FLR）プロシージャ中に処理するフローごとの通知の数を設定するには、グローバル コンフィギュレーション モードで **iprsvpsignallingfast-local-repairnotifications** コマンドを使用します。通知の数をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

ip rsvp signalling fast-local-repair notifications *number*
no ip rsvp signalling fast-local-repair notifications

構文の説明

number	送信される通知の合計数です。範囲は 10 ～ 10000 です。デフォルト値は 1000 です。

コマンド デフォルト

通知はルーティング情報ベース（RIB）によって送信され、RSVP によって処理されます。**iprsvpsignallingfast-local-repairnotifications** コマンドが設定されていない場合、RSVP は 1000 件の通知を処理し、通知を一時停止してから、別の 1000 件の通知の処理を再開します。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。
15.0(1)M	このコマンドが、Cisco IOS Release 15.0(1)M よりも前のリリースに統合されました。

使用上のガイドライン

ルートが変更されると、RIB は影響を受けたフローごとに 1 つの通知のリストを作成し、これらの通知を含むイベントを送信することでRSVPに通知します。そのため、影響を受けるパス ステートブロック（PSB）の数に応じて、これらのイベントには数千の要素が含まれる可能性があります。

デフォルトでは、RSVP は一度に 1000 件の通知を処理して、必要に応じて一時停止し、CPU に負荷がかかりすぎないようにします。ただし、**iprsvpsignallingfast-local-repairnotifications** コマンドを使用してこの数を設定することができます。

例

次に、RSVP が一時停止する前に修復されるフローの数を 100 に設定する例を示します。

```
Router(config)# ip rsvp signalling fast-local-repair notifications 100
```

関連コマンド

コマンド	説明
iprsvpsignallingfast-local-repairrate	FLR 手順のために RSVP で使用される修復を設定します。
iprsvpsignallingfast-local-repairwait-time	RSVP により FLR プロシージャの開始に使用される遅延を設定します。
showiprsvpsignallingfast-local-repair	RSVP によって保持されている FLR 固有の情報を表示します。

ip rsvp signalling fast-local-repair rate

リソース予約プロトコル（RSVP）が高速ローカル修復（FLR）プロシージャに使用する修復レートを設定するには、グローバル コンフィギュレーション モードで **iprsvpsignallingfast-local-repairrate** コマンドを使用します。修復レートをデフォルトに設定するには、このコマンドの **no** 形式を使用します。

ip rsvp signalling fast-local-repair rate *messages-per-second*
no ip rsvp signalling fast-local-repair rate

構文の説明

messages-per-second	PATH 状態の更新と修復の FLR レート（1 秒あたりのメッセージ数）です。指定できる範囲は 1 ～ 2500 です。デフォルトは 400 です。

コマンド デフォルト

このコマンドが設定されていない場合は、RSVP メッセージ ペーシング レートが使用されます。

（注） Cisco IOS リリース 12.2 以降のリリースでは、RSVP メッセージ ペーシング レートがデフォルトで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（config）

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。
15.0(1)M	このコマンドが、Cisco IOS Release 15.0(1)M よりも前のリリースに統合されました。

使用上のガイドライン

デフォルトの修復レートは、RSVP メッセージ ペーシング レートに基づきます。

iprsvpsignallingfast-local-repairrate コマンドを使用して FLR レートを設定し、RSVP メッセージ ペーシングが有効になっている場合は、FLR レートと RSVP メッセージ ペーシング レートのうち、低い方が有効になります。**noiprsvpsignallingrate-limit** コマンドを使用して RSVP レート制限を無効にした場合は、FLR レートが使用されます。ただし、RSVP レート制限を無効にして FLR レートを設定しない場合、RSVP はメッセージ ペーシングを実行せず、メッセージは連続して送信されます。ローカル修復ポイント（PLR）が PATH メッセージでダウンストリーム ノードをフラッディングして、その一部がドロップされる可能性があるため、このアクションは推奨されません。

修復レートは通知時に決定され、修復中に RSVP メッセージ ペーシング レートまたは FLR レートを変更した場合でも、その修復中は決定済みのレートと同じレートが使用されます。

例

次に、1 秒あたり 100 メッセージの修復レートを設定する例を示します。

```
Router(config)# ip rsvp signalling fast-local-repair rate 100
```

関連コマンド

コマンド	説明
iprsvpsignallingfast-local-repairnotifications	RSVP が一時停止する前に処理される通知の数を設定します。
iprsvpsignallingfast-local-repairwait-time	FLR プロシージャの開始に使用される遅延を設定します。
iprsvpsignallingrate-limit	指定の期間中に隣接ルータに送信される RSVP メッセージの伝送レートを制御します。

ip rsvp signalling fast-local-repair wait-time

リソース予約プロトコル（RSVP）が高速ローカル修復（FLR）プロシージャを開始する前に使用する遅延を設定するには、インターフェイス コンフィギュレーション モードで **iprsvpsignallingfast-local-repairwait-time** コマンドを使用します。遅延をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

ip rsvp signalling fast-local-repair wait-time *interval*
no ip rsvp signalling fast-local-repair wait-time

構文の説明

interval	FLR プロシージャが開始されるまでのミリ秒（ms）単位の時間です。指定できる範囲は 0 ～ 5000 です。デフォルトは 0 です。

コマンド デフォルト

このコマンドは、デフォルトでは無効になっています。そのため、遅延は設定されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

iprsvpsignallingfast-local-repairwait-time コマンドを使用して、FLR プロシージャを開始する際に必要な遅延を設定します。遅延を設定しない場合は、RSVP がルーティング情報ベース（RIB）からのルート変更通知を受信した直後に、パスの更新がトリガーされます。

例

次の例では、100 ms の遅延を設定します。

```
Router(config-if)# ip rsvp signalling fast-local-repair wait-time 100
```

関連コマンド

コマンド	説明
iprsvpsignallingfast-local-repairnotifications	RSVP が一時停止する前に処理される通知の数を設定します。
iprsvpsignallingfast-local-repairrate	FLR 手順のために RSVP で使用される修復を設定します。

ip rsvp signalling hello（コンフィギュレーション）

ルータでグローバルにHello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 **iprsvpsignallinghello** コマンドを使用します。ルータでグローバルに Hello 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 rsvp signalling hello
no ip rsvp signalling hello

構文の説明

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

グローバル設定

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

ルータでグローバルに Hello を有効にするには、このコマンドを入力する必要があります。また、インターフェイスでも Hello を有効にする必要があります。

例

次の例では、ルータでグローバルに Hello が有効になっています。

```
Router(config)# ip rsvp signalling hello
```

関連コマンド

コマンド	説明
iprsvpsignallinghello(interface)	Fast Reroute の保護が必要なインターフェイスでの hello を有効にします。
iprsvpsignallinghellostatistics	ルータで Hello 統計情報を有効にします。

ip rsvp signalling hello（インターフェイス）

Fast Reroute 保護が必要なインターフェイス上で hello 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 **iprsvpsignallinghello** コマンドを使用します。Fast Reroute 保護が必要なインターフェイス上で hello 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 rsvp signalling hello
no ip rsvp signalling hello

構文の説明

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

hello は有効になりません。

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	変更箇所
12.0(22)S	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

ルータおよび特定のインターフェイス上で hello をグローバルに設定する必要があります。

例

次の例では、インターフェイス上で hello が有効になります。

```
Router(config-if)# ip rsvp signalling hello
```

関連コマンド

コマンド	説明
iprsvpsignallinghello(configuration)	ルータで Hello をグローバルに有効にします。
iprsvpsignallinghellodscp	インターフェイスから送信される Hello メッセージの IP ヘッダーの DSCP 値を設定します。
iprsvpsignallinghellorefreshmisses	ノードが、そのネイバーとの通信がダウンしているとみなすまでに連続して失うことができる Hello 確認応答の数を指定します。

コマンド	説明
iprsvpsignallinghellorefreshinterval	Hello 要求間隔を設定します。

ip rsvp signalling hello dscp

インターフェイスから送信されたリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）hello メッセージの IP ヘッダーにある DiffServ コード ポイント（DSCP）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 **iprsvpsignallinghellodscp** コマンドを使用します。DSCP 値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

ip rsvp signalling hello [fast-reroute] dscp *num*
no ip rsvp signalling hello [fast-reroute] dscp

構文の説明

fast-reroute	（任意）Fast Reroute 機能を開始します。
num	DSCP 値。有効な値は 0 ～ 63 です。

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

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.0(29)S	オプションの **fast-reroute** キーワードが追加されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

リンクが輻輳している場合は、hello メッセージがドロップされる可能性を減らすために、DSCP を 0 よりも大きい値に設定することを推奨します。

フローごとではなく、インターフェイスごとに DSCP を設定します。

DSCP は、特定のインターフェイスで作成された RSVP hello に適用されます。DSCP のために各インターフェイスを個別に設定できます。

iprsvpsignallinghellodscp コマンドをオプションの **fast-reroute** キーワードを使用せずに発行した場合、このコマンドは Fast Reroute hello に適用されます。このコマンドは後方互換性のために提供されています。ただし、**iprsvpsignallinghellofast-reroutedscp** コマンドを使用することを推奨します。

例

次の例では、このインターフェイスから送信される hello メッセージは 30 の DSCP 値を持ち、**fast-reroute** キーワードを指定することで Fast Reroute 機能が有効になっています。

```
Router(config-if)# ip rsvp signalling hello fast-reroute dscp 30
```

次の例では、このインターフェイスから送信される hello メッセージは 30 の DSCP 値を持ち、Fast Reroute 機能がデフォルトで有効になっています。

```
Router(config-if)# ip rsvp signalling hello dscp 30
```

関連コマンド

コマンド	説明
iprsvpsignallinghello(interface)	Fast Reroute 保護が必要なインターフェイスで hello を有効にします。
iprsvpsignallinghellorefreshinterval	hello メッセージの hello の更新間隔を設定します。
iprsvpsignallinghellorerouterefreshmisses	hello メッセージの失われた更新の制限を設定します。

ip rsvp signalling hello graceful-restart

隣接ルータでリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）のグレースフル リスタート機能を有効にするには、インターフェイス コンフィギュレーション モードで **iprsvpsignallinghellograceful-restart** コマンドを使用します。グレースフル リスター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。

ip rsvp signalling hello graceful-restart
no ip rsvp signalling hello graceful-restart

構文の説明

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

隣接ルータには hello が有効になっているノードのみがあります。

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	変更箇所
12.2(33)SRE	このコマンドが導入されました。

使用上のガイドライン

iprsvpsignallinghellograceful-restart コマンドを使用して、ルータでのグレースフル リスタートのサポートを有効にし、ルータのネイバーがステートフル スイッチオーバー（SSO）の後に TE トンネルを回復できるように支援します。

（注） このコマンドはオプションです。ノード hello がサポートされていない場合に使用します。

例

次の例では、IP アドレス 10.0.0.1 の隣接ルータの POS インターフェイス 1/0/0 でグレースフル リスタートを設定します。

```
Router# configure terminal

Enter configuration commands, one per line. End with CTTL/Z.
Router(config)# interface POS1/0/0

Router(config-if)# ip rsvp signalling hello graceful-restart
```

関連コマンド

コマンド	説明
iprsvpsignallinghellograceful-restartmode	RP の RSVP TE グレースフル リスタート サポート機能を有効にして、ノード hello を有効にします。
showiprsvphellograceful-restart	RSVP TE グレースフル リスタート hello メッセージに関する情報を表示します。

ip rsvp signalling hello graceful-restart dscp

リソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）グレースフル リスタート hello メッセージの IP ヘッダーにある DiffServ コード ポイント（DSCP）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 **iprsvpsignallinghellograceful-restartdscp** コマンドを使用します。DSCP 値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

ip rsvp signalling hello graceful-restart dscp *num*
no ip rsvp signalling hello graceful-restart dscp

構文の説明

nm	DSCP 値。有効な値は 0 ～ 63 です。

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	変更箇所
12.0(29)S	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

リンクが輻輳している場合は、hello メッセージがドロップされる可能性を減らすために、DSCP を 0 よりも大きい値に設定します。

DSCP は、特定のルータで作成された RSVP hello に適用されます。DSCP のために各ルータを個別に設定できます。

例

次の例では、hello メッセージの DSCP 値は 30 です。

```
Router(config)# ip rsvp signalling hello graceful-restart dscp 30
```

関連コマンド

コマンド	説明
iprsvpsignallinghellograceful-restartrefreshinterval	グレースフル リスタート hello メッセージの hello 要求間隔を設定します。
iprsvpsignallinghellograceful-restartrefreshmisses	グレースフル リスタート hello メッセージの失われた更新の制限を設定します。

ip rsvp signalling hello graceful-restart mode

ルートプロセッサ（RP）でリソース予約プロトコル（RSVP）トラフィックエンジニアリング（TE）のグレースフル リスタート機能を有効にするには、グローバル コンフィギュレーション モードで **iprsvpsignallinghellograceful-restartmode** コマンドを使用します。グレースフル リスター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。

Cisco IOS 12.0(29)S、12.2(33)SRA、12.2(33)SXH 以降のリリース
ip rsvp signalling hello graceful-restart mode {help-neighbor|full}
no ip rsvp signalling hello graceful-restart mode

Cisco IOS T および XE トレイン
ip rsvp signalling hello graceful-restart mode help-neighbor
no ip rsvp signalling hello graceful-restart mode help-neighbor

構文の説明

help-neighbor	障害発生後の隣接ルータの再起動のサポートを有効にします。
full	障害発生後のルータのセルフリカバリの実行またはネイバーの再起動の支援のサポートを有効にします。

コマンド デフォルト

グレースフル リスタート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	変更箇所
12.0(29)S	このコマンドは、**iprsvpsignallinghellograceful-restartmodehelp-neighbor** として導入されました。
12.2(33)SRA	このコマンドが変更されました。**full** キーワードが追加されました。このコマンドで **iprsvpsignallinghellograceful-restartmodehelp-neighbor** コマンドが置き換えられます。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
15.0(1)M	このコマンドが、Cisco IOS Release 15.0(1)M よりも前のリリースに統合されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。

使用上のガイドライン

iprsvpsignallinghellograceful-restartmodehelp-neighbor コマンドを使用して、障害発生後に隣接ルータを再起動するためのサポート機能を有効にします。

iprsvpsignallinghellograceful-restartmodefull コマンドを使用して、スタンバイ RP がインストールおよび設定されている場合に、Cisco 7600 シリーズルータなどのステートフル スイッチオーバー（SSO）をサポートするプラットフォームで、ルータがセルフリカバリを開始したり、ネイバーの再起動を支援したりするためのサポート機能を有効にします。

例

次に、障害発生後にセルフリカバリを実行するためのサポート機能を RP に設定する例を示します。

```
Router(config)# ip rsvp signalling hello graceful-restart mode full
```

関連コマンド

コマンド	説明
iprsvpsignallinghellograceful-restartdscp	RSVP TE グレースフル リスタート hello メッセージの IP ヘッダーの DSCP 値を設定します。
iprsvpsignallinghellograceful-restartneighbor	隣接ルータで RSVP-TE グレースフル リスタート サポート機能を有効にします。
iprsvpsignallinghellograceful-restartrefreshinterval	グレースフル リスタート Hello メッセージの Request 間隔を制御するための値を設定します。
iprsvpsignallinghellograceful-restartrefreshmisses	グレースフル リスタート hello メッセージの失われた更新の制限を制御するための値を設定します。
showiprsvphellograceful-restart	RSVP-TE グレースフル リスタート hello メッセージに関する情報を表示します。

ip rsvp signalling hello graceful-restart mode help-neighbor

（注） Cisco IOS Release 12.2(33)SRA 以降では、**iprsvpsignallinghellograceful-restartmodehelp-neighbor** コマンドは、**iprsvpsignallinghellograceful-restartmode** コマンドによって置き換えられます。詳細については、**iprsvpsignallinghellograceful-restartmode** コマンドを参照してください。

隣接ルータでリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）のグレースフル リスタート機能を有効にするには、グローバル コンフィギュレーション モードで **iprsvpsignallinghellograceful-restartmodehelp-neighbor** コマンドを使用します。グレースフル リスター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。

ip rsvp signalling hello graceful-restart mode help-neighbor
no ip rsvp signalling hello graceful-restart mode help-neighbor

構文の説明

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

グレースフル リスタートは無効になっています。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.0(29)S	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、**iprsvpsignallinghellograceful-restartmode** コマンドによって置き換えられました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

iprsvpsignallinghellograceful-restartmodehelp-neighbor コマンドを使用して隣接ルータを再起動します。

例

次の例では、グレースフル リスタートが有効になります。

```
Router(config)# ip rsvp signalling hello graceful-restart mode help-neighbor
```

関連コマンド

コマンド	説明
iprsvpsignallinghellograceful-restartdscp	RSVP TE グレースフル リスタート hello メッセージの IP ヘッダーの DSCP 値を設定します。
iprsvpsignallinghellograceful-restartrefreshinterval	グレースフル リスタート Hello メッセージの Request 間隔を制御するための値を設定します。
iprsvpsignallinghellograceful-restartrefreshmisses	グレースフル リスタート hello メッセージの失われた更新の制限を制御するための値を設定します。

ip rsvp signalling hello graceful-restart neighbor

隣接ルータでリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）のグレースフル リスタート機能を有効にするには、インターフェイス コンフィギュレーション モードで **iprsvpsignallinghellograceful-restartneighbor** コマンドを使用します。グレースフル リスター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。

ip rsvp signalling hello graceful-restart neighbor *ip-address*
no ip rsvp signalling hello graceful-restart neighbor *ip-address*

構文の説明

ip-address	特定のインターフェイス上のネイバーの IP アドレスです。

コマンド デフォルト

このコマンドを発行するまで、隣接ルータのグレースフル リスタート機能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

コマンド履歴

リリース	変更箇所
12.2(33)SRA	このコマンドが導入されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

iprsvpsignallinghellograceful-restartneighbor コマンドを使用して、ルータでのグレースフル リスタートのサポートを有効にし、ルータのネイバーがステートフル スイッチオーバー（SSO）の後に TE トンネルを回復できるように支援します。

（注） 再起動を支援する隣接ルータの各インターフェイスでこのコマンドを発行する必要があります。

例

次の例では、IP アドレス 10.0.0.1 の隣接ルータの POS インターフェイス 1/0/0 でグレースフル リスタートを設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface POS1/0/0
Router(config-if)# ip rsvp
 signalling hello graceful-restart neighbor 10.0.0.1
```

関連コマンド

コマンド	説明
iprsvpsignallinghellograceful-restartmode	RP で RSVP-TE グレースフル リスタート サポート機能を有効にします。
showiprsvphellograceful-restart	RSVP-TE グレースフル リスタート hello メッセージに関する情報を表示します。

ip rsvp signalling hello graceful-restart refresh interval

グレースフル リスタート hello メッセージのリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）更新間隔を設定するには、グローバル コンフィギュレーション モードで **iprsvpsignallinghellograteful-restartrefreshinterval** コマンドを使用します。間隔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 rsvp signalling hello graceful-restart refresh interval *interval-value*
no ip rsvp signalling hello graceful-restart refresh interval

構文の説明

interval-value	ノードが hello メッセージをネイバーに送信する、ミリ秒（ms）単位の周期です。有効な値は 1000 ～ 30000 です。

コマンド デフォルト

1000 ミリ秒（10 秒）

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.0(29)S	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

ノードは、そのすべてのネイバーの Hello 要求オブジェクトを含む hello メッセージを定期的に生成します。この hello メッセージの頻度は、hello インターバルによって決まります。

（注） このコマンドのデフォルト値を変更し、**iprsvpsignallingrefreshinterval** コマンドも使用する場合は、**iprsvpsignallinghellograceful-restartrefreshintervalcommandislessthanthevaluefortheiprsvpsignallingrefreshinterval** コマンドの値が ip rsvp signalling refresh interval コマンドの値よりも小さくなるようにします。そうしないと、ラベル スイッチド パス（LSP）の一部またはすべてが、ステートフル スイッチオーバー（SSO）の発生後に回復されないおそれがあります。**iprsvpsignallingrefreshinterval** コマンドの値は、の値の 2 倍にすることを推奨します。**iprsvpsignallinghellograceful-restartrefreshintervalcommand.**

例

次の例では、hello 要求が 5000 ms ごとにネイバーに送信されます。

```
Router(config)# ip rsvp signalling hello graceful-restart refresh interval 5000
```

関連コマンド

コマンド	説明
iprsvpsignallinghellograceful-restartdscp	RSVP TE グレースフル リスタート hello メッセージの IP ヘッダーの DSCP 値を設定します。
iprsvpsignallinghellograceful-restartrefreshmisses	グレースフル リスタート hello メッセージの失われた更新の制限を設定します。
iprsvpsignallingrefreshinterval	各 RSVP 状態の更新メッセージの送信間隔を指定します。

ip rsvp signalling hello graceful-restart refresh misses

ノードがそのネイバーとの通信が失われたとみなすまでに失うことができる、連続したリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）グレースフル リスタート hello 確認応答（ACK）の数を指定するには、グローバル コンフィギュレーション モードで **iprsvpsignallinghellograceful-restartrefreshmisses** コマンドを使用します。失われた更新の制限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。

ip rsvp signalling hello graceful-restart refresh misses *msg-count*
no ip rsvp signalling hello graceful-restart refresh misses

構文の説明

msg-count	RSVP が状態を期限切れとみなして破棄する前に、ノードが失うことができる連続した hello 確認応答（ACK）の数です。有効な値は 4 ～ 10 です。

コマンド デフォルト

連続した hello 確認応答のデフォルトの数は 4 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	変更箇所
12.0(29)S	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS リリース 12.2(33)SXH に統合されました
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました

使用上のガイドライン

hello メッセージは、hello メッセージ、Hello 要求オブジェクト、および Hello ACK オブジェクトで構成されます。各要求は、確認応答によって応答されます。リンクが輻輳している場合やルータの負荷が大きい場合には、この数をデフォルト値よりも大きな値に設定して、hello によりネイバーがダウンしていると誤って宣言されないようにします。

（注） このコマンドのデフォルト値を変更し、**iprsvpsignallinghellorefreshmisses** コマンドも使用する場合は、**iprsvpsignallinghellograceful-restartrefreshmisses** コマンドの値が **iprsvpsignallinghellorefreshmisses** コマンドの値よりも小さくなるようにします。そうしないと、ラベル スイッチド パス（LSP）の一部またはすべてが、ステートフル スイッチオーバー（SSO）の発生後に回復されないおそれがあります。**iprsvpsignallinghellorefreshmisses** コマンドの値は、**iprsvpsignallinghellograceful-restartrefreshmisses** コマンドの値の 2 倍にすることを推奨します。

例

次の例では、ノードが 5 つの連続した hello 確認応答を受信しなかった場合に、ネイバーがダウンしているとノードが宣言します。

```
Router(config)# ip rsvp signalling hello graceful-restart refresh misses 5
```

関連コマンド

コマンド	説明
iprsvpsignallinghellograceful-restartdscp	グレースフル リスタート hello メッセージの DSCP 値を設定します。
iprsvpsignallinghellograceful-restartrefreshinterval	グレースフル リスタート hello メッセージの更新間隔を設定します。
iprsvpsignallingrefreshmisses	RSVP がデータベースから状態を削除するまでに失うことができる、連続したリフレッシュ メッセージの数を指定します。
iprsvpsignallinghellorefreshmisses	ノードが、そのネイバーとの通信がダウンしているとみなすまでに連続して失うことができる Hello 確認応答の数を指定します。

ip rsvp signalling hello graceful-restart send

ステートフル スイッチオーバー（SSO）が行われた後にマルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）ネットワークのリソース予約プロトコル（RSVP）ラベルスイッチドパス（LSP）が回復または再起動する時間を設定するには、グローバル コンフィギュレーション モードで **iprsvpsignallinghellograceful-restartsend** コマンドを使用します。デフォルトの回復時間と再起動時間を維持するには、このコマンドの **no** 形式を使用します。

ip rsvp signalling hello graceful-restart send {**recovery-time** *ms*|**restart-time** *ms*}
no ip rsvp signalling hello graceful-restart send {**recovery-time** *ms*|**restart-time** *ms*}

構文の説明

recovery-time *ms*	SSO が行われた後に LSP を回復できるようにする時間を、ミリ秒（ms）単位で発信 hello メッセージに設定します。値は 0 ～ 3600000 です。
restart-time *ms*	SSO が行われた後に LSP を再起動できるようにする時間を、ms 単位で発信 hello メッセージに設定します。値は 0 ～ 3600000 です。

コマンド デフォルト

デフォルトの回復時間と再起動時間はそれぞれ 120,000 ms と 30,000 ms で、変更するまで有効です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
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

iprsvpsignallinghellograceful-restartsend コマンドを使用して、SSO が行われた後に LSP が回復または再起動するまでの時間を長くします。これを行わない場合、すべての LSP が復旧しない可能性があり、ネットワークのパフォーマンスに悪影響を与えます。

例

次の例では、300,000 ms の回復時間が設定されています。

```
Router(config)# ip rsvp signalling hello graceful-restart send recovery-time 300000
```

関連コマンド

コマンド	説明
iprsvpsignallinghellograceful-restartdscp	RSVP TE グレースフル リスタート hello メッセージの IP ヘッダーの DSCP 値を設定します。

コマンド	説明
iprsvpsignallinghellograceful-restartmode	RP 上で RSVP TE グレースフル リスタート機能をイネーブルにします。
iprsvpsignallinghellograceful-restartneighbor	隣接ルータで RSVP TE グレースフル リスタート機能を有効にします。
iprsvpsignallinghellograceful-restartrefresh interval	グレースフル リスタート hello メッセージの RSVP TE 更新間隔を設定します。
iprsvpsignallinghellograceful-restartrefreshmisses	ノードが RSVP TE グレースフル リスタート hello 確認応答を何回連続して失敗するとネイバーとの通信が失われたとみなすか、その回数を指定します。

ip rsvp signalling hello refresh interval

リソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）hello 更新間隔を設定するには、インターフェイス コンフィギュレーション モードで **iprsvpsignallinghellorefreshinterval** コマンドを使用します。更新間隔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 rsvp signalling hello [fast-reroute] refresh interval *interval-value*
no ip rsvp signalling hello [fast-reroute] refresh interval

構文の説明

fast-reroute	（任意）Fast Reroute 機能を開始します。
interval-value	ノードが hello メッセージをネイバーに送信する、ミリ秒単位の周期です。有効な値は 10 ～ 30000 ミリ秒です。 （注） デフォルトの 200 ミリ秒未満の値にすることは推奨されません。RSVP Hello がネイバー ダウン イベントを誤検出し、Fast ReRoute を不必要にトリガーする可能性があるためです。

コマンド デフォルト

ノードが hello メッセージをネイバーに送信するデフォルトの頻度は 200 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

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.0(29)S	オプションの **fast-reroute** キーワードが追加されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

hello 要求間隔は、インターフェイス単位で設定できます。ノードは、状態がトラックされている各ネイバー用に、Hello 要求オブジェクトを含む hello メッセージを定期的に生成します。この hello メッセージの頻度は、hello インターバルによって決まります。

iprsvpsignallinghellorefreshinterval コマンドをオプションの **fast-reroute** キーワードを使用せずに発行した場合、このコマンドは Fast Reroute hello に適用されます。このコマンドは後方互換性のために提供されています。ただし、**iprsvpsignallinghellofast-rerouterefreshinterval** コマンドを使用することを推奨します。

例

次の例では、hello 要求が 5000 ミリ秒ごとにネイバーに送信され、**fast-reroute** キーワードを指定することで Fast Reroute 機能が有効になっています。

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh interval 5000
```

次の例では、hello 要求が 5000 ミリ秒ごとにネイバーに送信され、Fast Reroute 機能がデフォルトで有効になっています。

```
Router(config-if)# ip rsvp signalling hello refresh interval 5000
```

関連コマンド

コマンド	説明
iprsvpsignallinghellodscp	hello メッセージの DSCP 値を設定します。
iprsvpsignallinghellograceful-restartfreshinterval	グレースフル リスタート hello メッセージの更新間隔を設定します。
iprsvpsignallinghellorerouterefreshmisses	hello メッセージの失われた更新の制限を設定します。

ip rsvp signalling hello refresh misses

ノードがそのネイバーとの通信がダウンしているとみなすまでに、連続で失うことができるリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）hello 確認応答の数を指定するには、インターフェイス コンフィギュレーション モードで **iprsvpsignallinghellorefreshmisses** コマンドを使用します。失われた更新の制限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。

ip rsvp signalling hello [fast-reroute] refresh misses *msg-count*
no ip rsvp signalling hello [fast-reroute] refresh misses

構文の説明

fast-reroute	（任意）Fast Reroute 機能を開始します。
msg-count	RSVP が状態を期限切れとみなして破棄する前に、ノードが失うことができる連続した hello 確認応答の数です。有効な値は 4 ～ 10 です。

コマンド デフォルト

連続した hello 確認応答のデフォルトの数は 4 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.0(29)S	オプションの **fast-reroute** キーワードが追加されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました

使用上のガイドライン

hello は、hello メッセージ、Hello 要求オブジェクト、および Hello ACK オブジェクトで構成されます。各要求は、確認応答によって応答されます。リンクが非常に輻輳している場合やルータの負荷が非常に大きい場合には、この数をデフォルト値よりも大きな値に設定して、hello によりネイバーがダウンしていると誤って宣言されないようにします。

iprsvpsignallinghellorefreshmisses コマンドをオプションの **fast-reroute** キーワードを使用せずに発行した場合、このコマンドは Fast Reroute hello に適用され、Fast Reroute 機能がデフォルトで有効になります。このコマンドは後方互換性のために提供されています。ただし、**iprsvpsignallinghellofast-rerouterefreshmisses** コマンドを使用することを推奨します。

例

次の例では、ノードが 5 つの連続した hello 確認応答を受信しなかった場合にネイバーのダウンを宣言し、**fast-reroute** キーワードを指定することで Fast Reroute が有効になります。

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh misses 5
```

次の例では、ノードが 5 つの連続した hello 確認応答を受信しなかった場合にネイバーのダウンを宣言し、デフォルトで Fast Reroute が有効になります。

```
Router(config-if)# ip rsvp signalling hello refresh misses 5
```

関連コマンド

コマンド	説明
iprsvpsignallinghellodscp	hello メッセージの DSCP 値を設定します。
iprsvpsignallinghellorefreshinterval	hello メッセージの更新間隔を設定します。

ip rsvp signalling hello reroute dscp

インターフェイスから送信されたリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）再ルーティング hello（状態タイムアウト用）メッセージの IP ヘッダーにある DiffServ コードポイント（DSCP）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 **iprsvpsignallinghelloreroutedscp** コマンドを使用します。DSCP 値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

ip rsvp signalling hello reroute dscp *num*
no ip rsvp signalling hello reroute dscp

構文の説明

num	DSCP 値。有効な値は 0 ～ 63 です。

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

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(29)S	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

リンクが輻輳している場合は、hello メッセージがドロップされる可能性を減らすために、DSCP を 0 よりも大きい値に設定する必要があります。

フローごとではなく、インターフェイスごとに DSCP を設定します。

DSCP は、特定のインターフェイスで作成された RSVP hello に適用されます。DSCP のために各インターフェイスを個別に設定できます。

例

次の例では、このインターフェイスから送信される hello メッセージの DSCP 値は 30 です。

```
Router(config-if)# ip rsvp signalling hello reroute dscp 30
```

関連コマンド

コマンド	説明
ip rsvp signalling hello reroute refresh interval	再ルーティング hello メッセージの hello 要求間隔を設定します。

コマンド	説明
ip rsvp signalling hello reroute refresh misses	再ルーティング hello メッセージの失われた更新の制限を設定します。

ip rsvp signalling hello reroute refresh interval

リソース予約プロトコル（RSVP）トラフィックエンジニアリング（TE）再ルーティングhello（状態タイムアウト用）更新間隔を設定するには、インターフェイスコンフィギュレーションモードで**iprsvpsignallinghellorerouterefreshinterval**コマンドを使用します。更新間隔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 rsvp signalling hello reroute refresh interval *interval-value*
no ip rsvp signalling hello reroute refresh interval

構文の説明

interval-value	ノードがhelloメッセージをネイバーに送信する、ミリ秒単位の周期です。有効な値は1000 ～ 30000です（1 ～ 30秒）。

コマンドデフォルト

ノードがhelloメッセージをネイバーに送信するデフォルトの頻度は1000ミリ秒（10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	変更箇所
12.0(29)S	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXHに統合されました。
12.4(20)T	このコマンドがCisco IOS Release 12.4(20)Tに統合されました。

使用上のガイドライン

hello要求間隔は、インターフェイス単位で設定できます。ノードは、状態がトラックされている各ネイバー用に、Hello要求オブジェクトを含むhelloメッセージを定期的に生成します。このhelloメッセージの頻度は、helloインターバルによって決まります。一部のルータでは、間隔をデフォルト値よりも小さい値に設定すると、CPU使用率が高くなることがあります。

例

次の例では、hello要求が5000ミリ秒ごとにネイバーに送信され、Fast Reroute機能がデフォルトで有効になっています。

```
Router(config-if)# ip rsvp signalling hello reroute refresh interval 5000
```

関連コマンド

コマンド	説明
ip rsvp signalling hello reroute refresh misses	再ルーティングhelloメッセージの失われた更新の制限を設定します。

ip rsvp signalling hello reroute refresh misses

ノードがそのネイバーとの通信がダウンしているとみなすまでに、連続で失うことができるリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）再ルーティング hello（状態タイムアウト用）確認応答（ACK）の数を指定するには、インターフェイス コンフィギュレーション モードで **iprsvpsignallinghellorerouterefreshmisses** コマンドを使用します。失われた更新の制限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。

ip rsvp signalling hello reroute refresh misses *msg-count*
no ip rsvp signalling hello reroute refresh misses

構文の説明

msg-count	RSVP が状態を期限切れとみなして破棄する前に、ノードが失うことができる連続した hello 確認応答（ACK）の数です。有効な値は 4 ～ 10 です。

コマンド デフォルト

デフォルトは 4 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(29)S	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

hello は、hello メッセージ、Hello 要求オブジェクト、および Hello ACK オブジェクトで構成されます。各要求は、確認応答によって応答されます。リンクが非常に輻輳している場合やルータの負荷が非常に大きい場合には、この数をデフォルト値よりも大きな値に設定して、hello によりネイバーがダウンしていると誤って宣言されないようにします。

例

次の例では、ノードが 5 つの連続した hello 確認応答を受信しなかった場合に、ネイバーがダウンしているとノードが宣言します。

```
Router(config-if)# ip rsvp signalling hello reroute refresh misses 5
```

関連コマンド

コマンド	説明
ip rsvp signalling hello reroute dscp	再ルーティング hello メッセージの DSCP 値を設定します。
ip rsvp signalling hello reroute refresh interval	再ルーティング hello メッセージの更新間隔を設定します。

ip rsvp signalling hello statistics

ルータ上の Hello 統計を有効にするには、グローバル コンフィギュレーション モードで **iprsvpsignallinghellostatistics** コマンドを使用します。ルータ上の Hello 統計を無効にするには、このコマンドの **no** 形式を使用します。

ip rsvp signalling hello statistics
no ip rsvp signalling hello statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

例

次の例では、ルータ上の Hello 統計が有効になります。

```
Router(config)# ip rsvp signalling hello statistics
```

関連コマンド

コマンド	説明
cleariprsvphelloinstancestatistics	インスタンスの Hello 統計をクリアします。
iprsvpsignallinghello(configuration)	ルータで Hello をグローバルに有効にします。
showiprsvphellostatistics	hello パケットが hello 入力キューに入っていた時間を表示します。

ip rsvp signalling initial-retransmit-delay

リソース予約プロトコル（RSVP）設定済みルータが、同じメッセージを再送信する前に確認応答（ACK）メッセージを待機する最小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 **iprsvpsignallinginitial-retransmit-delay** コマンドを使用します。遅延値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。

ip rsvp signalling initial-retransmit-delay *delay-value*
no ip rsvp signalling initial-retransmit-delay

構文の説明

delay-value	ルータが同じメッセージを最初に再送信する前に ACK メッセージを待機する最小時間です。遅延値の範囲は、500 ～ 30,000 ミリ秒（ms）です。

コマンド デフォルト

デフォルト値は 1000 ms（1.0 秒）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	変更箇所
12.2(13)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

ip rsvp signalling initial-retransmit-delay コマンドを使用して、ルータが同じメッセージを再送信する前に ACK メッセージを待機する最小時間を設定します。

状態に ACK が受信されない場合、最初の再送信間隔の後に、最初の再送信が行われます。最初の再送信の後に ACK が受信されない場合は、2 回目の再送信が行われます。ACK が受信されるまで、連続する再送信の間隔を前の間隔の 2 倍にして、メッセージが再送信され続けます。その後、メッセージを更新する必要がある場合には、メッセージが通常の更新スケジュールに入れられます（Path および Resv メッセージ）。または、メッセージが処理されます（Error および Tear メッセージ）。5 回の再送信後に ACK が受信されない場合は、メッセージが必要に応じて破棄されます。

例

次に、initial-retransmit-delay を 2 秒に設定するコマンドを示します。

```
Router(config)# ip rsvp signalling initial-retransmit-delay 2000
```

次に、initial-retransmit-delay をデフォルト（1.0 秒）にリセットするコマンドを示します。

```
Router(config)# no ip rsvp signalling initial-retransmit-delay
```

ip rsvp signalling patherr state-removal

ネットワーク内のリソース予約プロトコル（RSVP）トラフィック メッセージの量を減らすには、グローバル コンフィギュレーション モードで **iprsvpsignallingpatherrstate-removal** 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。

ip rsvp signalling patherr state-removal [**neighbor** *acl*]
no ip rsvp signalling patherr state-removal

構文の説明

neighbor	（任意）特定のトラフィック エンジニアリング トンネルの一部である隣接ルータです。
acl	（任意）1 ～ 99 の値を使用する簡易アクセス リストです。

コマンド デフォルト

無効

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(13)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

iprsvpsignallingpatherrstate-removal コマンドを使用して、ルータが PathError メッセージを転送するときに自動的に Path 状態を削除できるようにして、後続の PathTear メッセージを不要にします。

このコマンドは、すべてのネットワーク ノードがこの機能をサポートしている場合に最も効果的です。すべてのノードで最新バージョンの Cisco IOS ソフトウェアを設定する必要があります。

このコマンドは、ラベルスイッチド パス（LSP）フローにのみ適用されます。

例

次に、**iprsvpsignallingpatherrstate-removal** を有効にするコマンドを示します。

```
Router(config)# ip rsvp signalling patherr state-removal
```

次に、**iprsvpsignallingpatherrstate-removal** を無効にするコマンドを示します。

```
Router(config)# no ip rsvp signalling patherr state-removal
```

次に、アクセス コントロール リスト（ACL）に基づいて **iprsvpsignallingpatherrstate-removal** を有効にするコマンドを示します。

```
Router(config)# ip rsvp signalling patherr state-removal neighbor 98
```

次に、ACL に基づいて **iprsvpsignallingpatherrstate-removal** を無効にするコマンドを示します。

```
Router(config)# no ip rsvp signalling patherr state-removal neighbor 98
```

ip rsvp signalling rate-limit

指定された時間内に隣接デバイスに送信されるリソース予約プロトコル（RSVP）メッセージの転送速度を制御するには、グローバル コンフィギュレーション モードで **ip rsvp signalling rate-limit** 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。

Cisco IOS Release 12.4(20)T よりも前のリリース
ip rsvp signalling rate-limit [**burst** *number*] [**maxsize** *bytes*] [**period** *ms*]
no ip rsvp signalling rate-limit

Cisco IOS 12.0S リリース、12.2S リリース、XE 2 リリース、Release 12.4(20)T 以降の T リリース
ip rsvp signalling rate-limit [**burst** *number*] [**limit** *number*] [**maxsize** *bytes*] [**period** *ms*]
no ip rsvp signalling rate-limit

構文の説明

burst *number*	（任意）各間隔で隣接デバイスに送信される RSVP メッセージの最大数を指定します。範囲は 1 ～ 5000 です。デフォルトは 8 です。
maxsize *bytes*	（任意）メッセージ キューの最大サイズをバイト単位で指定します。有効な範囲は 1 ～ 5000 です。デフォルトは 2000 です。
period *ms*	（任意）時間の長さをミリ秒（ms）単位で指定します。有効な範囲は 10 ～ 5000 です。デフォルトは 20 です。
limit *number*	（任意）送信されたメッセージの数が正常に送信されたメッセージの数を下回っている場合に、キューの間隔で送信できるメッセージの最大数を指定します。有効な範囲は 1 ～ 5000 です。デフォルトは 37 です。

コマンド デフォルト

このコマンドを入力しない場合は、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（config）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。このコマンドで **ip rsvp msg pacing** コマンドが置き換えられます。
12.0(24)S	このコマンドが変更されました。**limit** キーワードが追加されました。
12.0(29)S	このコマンドが変更されました。**burst** キーワードと **maxsize** キーワードのデフォルトの引数の値が、それぞれ 8 メッセージと 2000 バイトに増やされました。

リリース	変更箇所
12.2(18)SXF5	このコマンドが、Cisco IOS Release 12.2(18)SXF5 に統合されました。
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。
Cisco IOS XE リリース 2.3	このコマンドが、Cisco IOS XE Release 2.3 に統合されました。
15.2(3)T	このコマンドが変更されました。IPv6 のサポートが追加されました。

使用上のガイドライン

ip rsvp signalling rate-limit コマンドを使用して、RSVP トラフィック エンジニアリング シグナリング メッセージのバーストにより、受信デバイスが一部のメッセージをドロップする原因となる、受信デバイスのインプット キューのオーバーフローが引き起こされることを防ぎます。メッセージがドロップされると、シグナリングの完了が大幅に遅延します。

このコマンドで **ip rsvp msg-pacing** コマンドが置き換えられます。

ip rsvp signalling rate-limit コマンドに関連するすべての設定は、IPv4 セッションと IPv6 セッションの両方に適用できます。

例

次に、500 バイトのメッセージ キューを持つ 6 つのメッセージが 10 ms ごとに隣接デバイスに送信されるコマンドを示します。

```
Device(config)# ip rsvp signalling rate-limit burst 6 maxsize 500 period 10
```

関連コマンド

コマンド	説明
clearipsvpsignallingrate-limit	最大キューのためにドロップされたメッセージの数をクリア（ゼロに設定）します。
debugiprsvprate-limit	RSVP レート制限イベントのデバッグ メッセージを表示します。
show ip rsvp signalling rate-limit	RSVP レート制限パラメータを表示します。

ip rsvp signalling refresh interval

各リソース予約プロトコル（RSVP）状態の更新メッセージの送信間隔を指定するには、グローバル コンフィギュレーション モードで **iprsvpsignallingrefreshinterval** コマンドを使用します。間隔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 rsvp signalling refresh interval *interval-value*
no ip rsvp signalling refresh interval

構文の説明

interval-value	各 RSVP 状態の更新の送信間隔（ミリ秒単位）です。範囲は 5000 ～ 4294967295 ミリ秒です。デフォルト値は 30000 です。

コマンド デフォルト

30000 ミリ秒（30 秒）

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.0(26)S	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(18)SXF5	このコマンドが、Cisco IOS Release 12.2(18)SXF5 に統合されました。
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。
15.0(1)M	このコマンドが、Cisco IOS Release 15.0(1)M よりも前のリリースに統合されました。

使用上のガイドライン

iprsvpsignallingrefreshinterval コマンドを使用して、各 RSVP 状態の更新メッセージの送信間隔を指定します。

RSVP プロトコルでは、ネットワーク損失が発生した場合の状態の一貫性管理にソフトステートメカニズムを採用しています。このメカニズムは、継続的に更新メッセージを使用して、最新の状態を維持します。各 RSVP ルータは、定期的にリフレッシュ メッセージをネイバーに送信する必要があります。

（注） このコマンドのデフォルト値を変更し、**iprsvpsignallinghellograceful-restartrefreshinterval** コマンドも使用する場合は、**iprsvpsignallinghellograceful-restartrefreshinterval** コマンドの値が **iprsvpsignallingrefreshinterval** コマンドの値よりも小さくなるようにします。そうしないと、ラベルスイッチドパス（LSP）の一部またはすべてが、ステートフルスイッチオーバー（SSO）の発生後に回復されないおそれがあります。**iprsvpsignallingrefreshinterval** コマンドの値は、**iprsvpsignallinghellograceful-restartrefreshinterval** コマンドの値の 2 倍にすることを推奨します。

例

次に、更新間隔を 60000 ミリ秒（60 秒）に指定する例を示します。

```
Router(config)# ip rsvp signalling refresh interval 60000
```

次の例では、更新間隔をデフォルト値の 30 秒に戻します。

```
Router(config)# no ip rsvp signalling refresh interval
```

関連コマンド

コマンド	説明
iprsvpsignallingrefreshmisses	RSVP がデータベースから状態を削除するまでに失うことができる、連続したリフレッシュ メッセージの数を指定します。

ip rsvp signalling refresh misses

リソース予約プロトコル（RSVP）がデータベースから状態を削除する前に失うことができる連続した更新メッセージの数を指定するには、グローバル コンフィギュレーション モードで **iprsvpsignallingrefreshmisses** コマンドを使用します。失われた更新の制限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。

ip rsvp signalling refresh misses *msg-count*
no ip rsvp signalling refresh misses

構文の説明

msg-count	RSVP が状態を期限切れとみなして破棄する前に、失うことができる連続した更新メッセージの数です。指定できる範囲は 2 ～ 10 です。デフォルトは 4 です。

コマンド デフォルト

4 メッセージ

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	変更箇所
12.0(26)S	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(18)SXF5	このコマンドが、Cisco IOS Release 12.2(18)SXF5 に統合されました。
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。
15.0(1)M	このコマンドが、Cisco IOS Release 15.0(1)M よりも前のリリースに統合されました。

使用上のガイドライン

iprsvpsignallingrefreshmisses コマンドを使用して、RSVP がルータの状態を期限切れとみなしてその状態をデータベースから削除する前に失うことができる、連続した更新メッセージの数を指定します。

（注） このコマンドのデフォルト値を変更し、**iprsvpsignallinghellograceful-restartrefreshmisses** コマンドも使用する場合は、**iprsvpsignallinghellograceful-restartrefreshmisses** コマンドの値が **iprsvpsignallingrefreshmisses** コマンドの値よりも小さくなるようにします。そうしないと、ラベル スイッチド パス（LSP）の一部またはすべてが、ステートフル スイッチオーバー（SSO）の発生後に回復されないおそれがあります。**iprsvpsignallingrefreshmisses** コマンドの値は、**iprsvpsignallinghellograceful-restartrefreshmisses** コマンドの値の 2 倍にすることを推奨します。

例

次に、失われた更新の制限を 6 メッセージに指定する例を示します。

```
Router(config)# ip rsvp signalling refresh misses 6
```

次に、失われた更新の制限をデフォルト値の 4 に戻す例を示します。

```
Router(config)# no ip rsvp signalling refresh misses
```

関連コマンド

コマンド	説明
iprsvpsignallingrefreshinterval	各 RSVP 状態の更新メッセージの送信間隔を指定します。

ip rsvp signalling refresh reduction

リソース予約プロトコル（RSVP）リフレッシュ削減を有効にするには、グローバル コンフィギュレーション モードで **iprsvpsignallingrefreshreduction** コマンドを使用します。リフレッシュ削減を無効にするには、このコマンドの **no** 形式を使用します。

ip rsvp signalling refresh reduction
no ip rsvp signalling refresh reduction

構文の説明

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

無効

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(13)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

RSVP リフレッシュ削減は、RSVP によるメッセージング負荷を削減し、より多くのフローをサポートするための拡張を支援する、拡張機能のセットです。

次のリフレッシュ削減標準（RFC 2961）の機能がサポートされており、このコマンドで有効になります。

- メッセージ ヘッダー内に refresh-reduction-capable ビットの設定
- メッセージ識別子（ID）の使用
- 迅速な再送信、確認応答（ACK）メッセージ、および MESSAGE_ID オブジェクトによる信頼性の高いメッセージング
- サマリー リフレッシュ拡張
- バンドル メッセージ（受信のみ）

リフレッシュ削減の運用には、ネイバーの協力が必要です。そのため、ネイバーも標準をサポートしている必要があります。直接接続ネイバーがリフレッシュ削減標準をサポートしていないことをルータが検出すると（ネクスト ホップから受信したメッセージに含まれる refresh-reduction-capable ビットを確認するか、ネクスト ホップに MESSAGE_ID オブジェクトを送信したときにエラーを受信した場合）、このコマンドを問わず、このリンクでリフレッシュ削減は使用されません。

例

次に、RSVP リフレッシュ削減を有効にするコマンドを示します。

```
Router(config)# ip rsvp signalling refresh reduction
```

次に、RSVP リフレッシュ削減を無効にするコマンドを示します。

```
Router(config)# no ip rsvp signalling refresh reduction
```

関連コマンド

コマンド	説明
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。
showiprsvpsignallingrefreshreduction	RSVP メッセージのリフレッシュ削減パラメータを表示します。

ip rsvp signalling refresh reduction ack-delay

リソース予約プロトコル（RSVP）設定済みルータが、送信する前に確認応答（ACK）メッセージを保持する最大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 **iprsvpsignallingrefreshreductionack-delay** コマンドを使用します。ack-delay の値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。

ip rsvp signalling refresh reduction ack-delay *delay-value*
no ip rsvp signalling refresh reduction ack-delay

構文の説明

delay-value	ルータが ACK メッセージを送信する前に保持する最大時間です。値の範囲は 100 ～ 10000 ミリ秒（ms）です。

コマンド デフォルト

デフォルト値は 250 ms（0.25 秒）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	変更箇所
12.2(13)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

iprsvpsignallingrefreshreductionack-delay コマンドを使用して、RSVP 設定済みルータが ACK メッセージを送信する前に保持する最大時間を設定します。

例

次に、ack-delay 値を 1 秒に設定するコマンドを示します。

```
Router(config)# ip rsvp signalling refresh reduction ack-delay 1000
```

次に、ack-delay 値をデフォルト値に設定するコマンドを示します。

```
Router(config)# no ip rsvp signalling refresh reduction ack-delay
```

ip rsvp snooping

特定の VLAN セットでリソース予約プロトコル（RSVP）スヌーピ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 **ip rsvp snooping** コマンドを使用します。RSVP スヌーピ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 rsvp snooping ［**vlan** *vlan-id* | **vlan-range** *vlan-id-start vlan-id-end*］

no ip rsvp snooping ［**vlan** *vlan-id* | **vlan-range** *vlan-id-start vlan-id-end*］

構文の説明

vlan *vlan-id*	（任意）RSVP スヌーピングを有効にする必要がある VLAN を指定します。
vlan-range *vlan-id-start vlan-id-end*	（任意）RSVP スヌーピングを有効にする必要がある VLAN の範囲を指定します。

コマンド デフォルト

RSVP スヌーピングは、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（config）

コマンド履歴

リリース	変更箇所
12.2(44)SE	このコマンドが導入されました。

使用上のガイドライン

ip rsvp snooping コマンドを使用して、特定の VLAN または VLAN の範囲で RSVP スヌーピングを有効または無効にします。VLAN の指定は任意です。キーワードと引数のペア **vlan** *vlan-id* および **vlan-range** *vlan-id-start vlan-id-end* は、VLAN 単位のスヌーピングをサポートするプラットフォームでのみ表示されます。VLAN の詳細を指定しない場合は、すべての VLAN でスヌーピングが有効になります。このコマンドを複数回使用しても、前の設定は無効になりません。新しい VLAN を作成する場合、すべての VLAN で RSVP スヌーピングが有効になっているときは、新しい VLAN でも RSVP スヌーピングが有効になります。VLAN を指定せずに **no ip rsvp snooping** コマンドを使用した場合は、すべての VLAN で RSVP スヌーピングが無効になります。

例

次に、特定の VLAN で RSVP スヌーピングを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip rsvp snooping vlan 10
```

関連コマンド

コマンド	説明
show ip rsvp snooping	RSVP スヌーピングが有効になっている VLAN のリストを表示します。

ip rsvp source

そのインターフェイスにPATHメッセージを転送するときに、リソース予約プロトコル（RSVP）ルータが前のホップ（PHOP）オブジェクトの PHOP アドレス フィールドにネイティブ インターフェイス アドレス以外のアドレスを入力するように設定するには、インターフェイス コンフィギュレーション モードで **iprsvpsource** コマンドを使用します。PHOP アドレス フィールドにネイティブ インターフェイス アドレスを保持するには、このコマンドの **no** 形式を使用します。

ip rsvp source {**address** *ip-address*|**interface** *type number*}
no ip rsvp source

構文の説明

address *ip-address*	PHOP アドレス フィールドの IP アドレスです。
interface *type number*	PHOP アドレス フィールドのソースとして使用されるインターフェイスのタイプと番号です。

コマンド デフォルト

ネイティブ インターフェイス アドレスが PHOP アドレス フィールドに書き込まれます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.4(20)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。

例

次の例では、PHOP アドレス フィールドに IP アドレス 10.1.3.13 を設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ethernet 0/0
Router(config-if)# ip rsvp bandwidth
Router(config-if)# ip rsvp source address 10.1.3.13
Router(config-if)# end
```

次の例では、アドレスが PHOP アドレス フィールドで使用される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 0 を設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ethernet 1/0
Router(config-if)# ip rsvp bandwidth
Router(config-if)# ip rsvp source interface loopback 0
Router(config-if)# end
```

関連コマンド

コマンド	説明
showiprsvpinterface	RSVP 関連情報を表示します。

ip rsvp svc-required

拡張 ATM ポート アダプタ（PA-A3）のインターフェイスまたはサブインターフェイスで行われた新しいリソース予約プロトコル（RSVP）予約を処理するために相手先選択接続（SVC）を作成できるようにするには、インターフェイス コンフィギュレーション モードで **iprsvpsvc-required** コマンドを使用します。RSVP 予約のための SVC の作成を無効にするには、このコマンドの **no** 形式を使用します。

ip rsvp svc-required
no ip rsvp svc-required

構文の説明

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

無効

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
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。

使用上のガイドライン

このコマンドは、RSVP-ATM QoS インターワーキング機能にのみ適用されます。

通常、予約は RSVP がパケットを分類するときに処理され、輻輳を管理するためにキューイング メカニズムにより伝送がスケジュールされます。伝統的に、RSVP は重み付け均等化キューイング（WFQ）とともに使用されます。RSVP と WFQ を組み合わせることで、WFQ で確認できるすべてのパケットが RSVP でも確認できるため、RSVP は重要なパケットを特定してアクションを実行できるようになります。この場合、WFQ が帯域幅を保証します。

ただし、**iprsvpsvc-required** コマンドがインターフェイスまたはサブインターフェイスを設定するために使用される場合は、新しい SVC が確立され、インターフェイス上の新しい各予約を処理するために使用されます。帯域幅を保証するために ATM SVC が使用され、RSVP がデータ パケットを確認できるようにするために入力インターフェイスで NetFlow が使用されます。

（注） RSVP が有効になっている場合は、すべてのパケットが Route Switch Processor（RSP）により処理されます。

このコマンドは、RSVPによって行われるSVCの両端で実行する必要があります。このコマンドは、拡張 ATM ポート アダプタ（PA-A3）およびそのサブインターフェイスでのみサポートされています。

（注） このコマンドを有効にするには、NetFlow を有効にする必要があります。そのため、設定ではこのコマンドの前に **iproute-cacheflow** コマンドを使用する必要があります。

showiprsvpinterface コマンドを使用して、このコマンドがインターフェイスまたはサブインターフェイスで有効になっているかどうかを判断します。

例

次の例では、ATM インターフェイス 2/0/0 で行われた予約が SVC を作成することで処理されることを RSVP に示します。

```
interface atm2/0/0
 ip rsvp svc-required
```

関連コマンド

Command	Description
iproute-cacheflow	IP ルーティングの NetFlow スイッチングをイネーブルにします。
iprsvpatm-peak-rate-limit	現在のインターフェイスまたはそのサブインターフェイス上に確立された、すべての新しく作成されたRSVP SVCの予約のピーク セルレートに制限を設定します。
iprsvpprecedence	RSVP フロースペックに適合するパケットまたはRSVP フロースペックを超過するパケットに適用する IP プレシデンス値を設定できます。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。

ip rsvp tos

ルータがリソース予約プロトコル（RSVP）フロースペックに適合するトラフィックまたはそれを超えるトラフィックに指定された値を使用して、RSVP 予約済みパスのパケットの IP ヘッダー ToS バイトの 5 つの下位タイプ オブ サービス（ToS）ビットをマークできるようにするには、インターフェイス コンフィギュレーション モードで **iprsvptos** コマンドを使用します。ToS ビットの既存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。**conform** キーワードと **exceed** キーワードのどちらも指定されていない場合には、ToS ビットのすべての設定が削除されます。

ip rsvp tos conform *tos-value* **exceed** *tos-value*
no ip rsvp tos [conform] [exceed]

構文の説明

conform *tos-value*	RSVP フロースペックに適合するトラフィックの ToS 値を 0 ～ 31 の範囲で指定します。ToS 値は、パケットの IP ヘッダーの ToS バイトの下位 5 ビット（ビット 0 ～ 4）に書き込まれます。**conform** または **exceed** キーワードが必要です。両方のキーワードを指定することもできます。 このコマンドの **no** 形式で使用する場合は、**conform** キーワードはオプションになります。
exceed *tos-value*	（任意）RSVP フロースペックを超えるトラフィックの ToS 値を 0 ～ 31 の範囲で指定します。ToS バイト値は、パケットの IP ヘッダーの ToS バイトの下位 5 ビット（ビット 0 ～ 4）に書き込まれます。**conform** または **exceed** キーワードが必要です。両方のキーワードを指定することもできます。 このコマンドの **no** 形式で使用する場合は、**exceed** キーワードはオプションになります。

コマンド デフォルト

このコマンドが使用されていない場合は、ToS バイトの ToS ビットは変更されません。（デフォルトの動作は、**noiprsvptos** コマンドを使用したときの動作と同じです）。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
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。

使用上のガイドライン

RSVP 予約済みパスのパケットは、予約フロースペックに適合するパケットと、予約に対応するものの予約フロースペックを超える（または、予約フロースペック外の）パケットの、2 つのクラスに分類されます。

iprsvptos コマンドにより、この 2 つのクラスに属するパケットに適用する ToS 値を設定できます。このコマンドを使用する場合は、トラフィックの少なくとも 1 つのクラスに ToS 値を指定する必要があります。コマンドの単一のインスタンスを使用して、両方のクラスの値を指定することができます。この場合、**conform** および **exceed** キーワードを任意の順序で指定できます。

入力処理の一部として、RSVP は **iprsvptos** コマンド設定を使用し、適合するパケットと適合しないパケットに ToS バイトの ToS ビットを設定します。仮想回線（VC）ごとの VIP 分散重み付けランダム早期検出（DWRED）が設定されている場合、システムはパケット ドロップ プロセスで出力インターフェイスの ToS ビット設定と IP プレシデンス ビット設定を使用します。パケットの ToS ビット設定と IP プレシデンス ビット設定は、ダウンストリーム ルータのインターフェイスでも使用できます。

iprsvptos コマンドを実行すると、インターフェイス上にあるすべての既存の予約の ToS ビット値が変更されます。

（注） このコマンドを使用するには、インターフェイスで RSVP を有効にする必要があります。つまり、**iprsvpbandwidth** コマンドを使用してから、**iprsvptos** コマンドを使用する必要があります。RSVP は、VIP 分散型シスコ エクスプレス フォワーディング（dCEF）で設定できません。

（注） **iprsvptos** コマンドはビット 0 ～ 4 を設定し、IP プレシデンス ビット設定と組み合わせることで、ToS バイトのすべてのビットが設定されるようにします。これらのビットは、ToS バイトを扱う特定の標準化テキストが、ビット 1 ～ 4 のみが ToS ビットとして使用されることを指定することを十分に把握したうえで使用します。

RSVP は、基礎となる転送メカニズムからパケットを受信します。そのため、**iprsvptos** コマンドを使用して ToS ビットを設定するには、次のいずれかの機能が必要です。

- インターフェイスで重み付け均等化キューイング（WFQ）が有効になっている必要があります。
- RSVP 相手先選択接続（SVC）が使用されている必要があります。
- RSVP を支援するように NetFlow が設定されている必要があります。

（注） このコマンドの **no** 形式を使用することは、以前のプレシデンス設定にかかわらず、パケットのすべてのプレシデンスを 0 に設定する **iprsvptos0** コマンドを使用することと同じではありません。

例

次の例では、ATM インターフェイス 1 上の RSVP フロースペックに適合するすべてのトラフィックに対して ToS ビット値を 4 に設定します。フロースペックを超えるパケットの ToS ビットは変更されません。

```
interface atm1
 ip rsvp tos conform 4
```

関連コマンド

Command	Description
iprsvpbandwidth	インターフェイスで IP 用 RSVP をイネーブルにします。
iprsvpflow-assist	RSVP が、NetFlow に接続して NetFlow サービスを活用できるようにします。
iprsvppolicycopsminimal	COPS サーバの負荷を軽減し、管理対象ルータでのメッセージの遅延時間を改善します。
showiprsvp	指定されたインターフェイスの、RSVP フロースペックに適合するパケットまたは RSVP フロースペックを超過するパケットに適用される IP プレシデンス ビット値と ToS ビット値を表示します。

ip rsvp transport

リソース予約プロトコル（RSVP）トランスポートセッションを作成するには、グローバル コンフィギュレーション モードで **iprsvptransport** コマンドを使用します。RSVP トランスポート セッショ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。

ip rsvp transport {**client** *client-id*|**statistics**}
no ip rsvp transport {**client** *client-id*|**statistics**}

構文の説明

client	RSVP トランスポート クライアントを開始します。
client-id	クライアント ID。指定できる範囲は 1 ～ 65535 です。
statistics	RSVP トランスポート プロトコル（TP）情報のバッファ サイズを設定します。

コマンド デフォルト

RSVP がトランスポート プロトコルとして設定されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
15.1(3)T	このコマンドが導入されました。
15.1(1)S	このコマンドが、Cisco IOS Release 15.1(1)S に統合されました。

使用上のガイドライン

iprsvptransport コマンドを使用して、RSVP がクライアントのトランスポート メカニズムとして使用されるように設定することができます。*client-id* は、RSVP をトランスポート プロトコルとして開始するクライアントの識別に使用されます。**statistics** キーワードは、RSVP TP セッションの統計を記録するために使用されます。記録される統計には、コールバックの一部として RSVP により RSVP TP クライアントに渡された情報が含まれます。記録できる情報の最大量は 32 MB です。

iprsvptransport コマンドは、ルータで RSVP PATH メッセージを生成するホストをシミュレートできるようにします。このコマンドは、テストとデバッグの目的に使用されます。

例

次に、クライアントを識別して RSVP トランスポート セッションを確立する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ip rsvp transport client 12
```

関連コマンド

コマンド	説明
iprsvptransportsender-host	トランスポートクライアントIDをRSVPに登録します。

ip rsvp transport sender-host

トランスポートクライアントIDをリソース予約プロトコル（RSVP）に登録するには、グローバル コンフィギュレーション モードで **iprsvptransportsender-host** コマンドを使用します。静的 RSVP ホスト パス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 rsvp transport sender-host [{**tcp**|**udp**}] *destination-address source-address ip-protocol dest-port source-port client-id init-id instance-id* [**vrf** *vrf-name*] [**data** *data-value*]
no ip rsvp transport sender-host [{**tcp**|**udp**}] *destination-address source-address ip-protocol dest-port source-port client-id init-id instance-id* [**vrf** *vrf-name*] [**data** *data-value*]

構文の説明

tcp	（任意）トランスポート メカニズムとして使用する TCP を指定します。
udp	（任意）トランスポート メカニズムとして使用する User Datagram Protocol（UDP）を指定します。
destination-address	PATH メッセージが送信される宛先アドレスです。
source-address	PATH メッセージの送信元となる発信元アドレスです。
ip-protocol	RSVP をトランスポート プロトコルとして設定するための識別子です。範囲は 0 ～ 255 です。
dest-port	PATH メッセージが送信される宛先ポートです。
source-port	PATH メッセージの送信元となる送信元ポートです。
client-id	RSVP クライアントを開始する識別子です。
init-id	トランスポート サービス要求を開始するノードを識別するホスト名または IP アドレスです。
instance-id	特定のクライアント アプリケーションと特定のイニシエータからのトランスポート サービス要求を識別するインスタンス ID です。指定できる範囲は 1 ～ 65535 です。
vrf *vrf-name*	（任意）RSVP クライアント上の VPN ルーティングおよび転送（VRF）インスタンスを設定します。
data *data-value*	（任意）RSVP トランスポート データ値を設定します。

コマンド デフォルト

静的 RSVP ホスト パスが設定されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
15.1(3)T	このコマンドが導入されました。
15.1(1)S	このコマンドが、Cisco IOS Release 15.1(1)S に統合されました。

使用上のガイドライン

iprsvptransportsender-host コマンドを使用して、RSVP トランスポートプロキシパスを設定します。このコマンドが設定されると、RSVP が PATH メッセージをダウンストリームに送信します。

例

次に、RSVP 送信者ホスト パスを設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ip rsvp transport sender-host 10.1.1.1 10.2.1.1 2 3 4 3 192.168.1.2 2
vrf vrf1 data d1
```

関連コマンド

コマンド	説明
iprsvptransport	RSVP をトランスポートプロトコルとして設定します。

ip rsvp tunnel overhead-percent

リソース予約プロトコル（RSVP）のパーセンテージ帯域幅を手動で上書きするには、インターフェイス コンフィギュレーション モードで **iprsvptunneloverhead-percent** コマンドを使用します。トンネル オーバーヘッド パーセンテージ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。

ip rsvp tunnel overhead-percent *percentage*
no ip rsvp tunnel overhead-percent

構文の説明

percentage	トンネルのパーセンテージオーバーヘッドです。

コマンド デフォルト

Generic Routing Encapsulation（GRE）または multipoint Generic Routing Encapsulation（mGRE）インターフェイスのパーセンテージ オーバーヘッドは 4 パーセントです。IPsec インターフェイスによる GRE および mGRE のパーセンテージ オーバーヘッドの範囲は 4 ～ 15 パーセントで、平均は 10 パーセントです。

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 モード（config-if）

コマンド履歴

リリース	変更箇所
15.1(2)T	このコマンドが導入されました。
15.1(1)S	このコマンドが、Cisco IOS Release 15.1(1)S に統合されました。

使用上のガイドライン

帯域幅のアドミッション コントロール中に、Cisco IOS ソフトウェアは、トンネリングとトンネルに対して行われる可能性がある暗号化のために、導入される追加の IP オーバーヘッドを考慮する必要があります。オーバーヘッドのデフォルト値は、インターネット パケットの平均サイズに応じて異なります。ただし、**iprsvptunneloverhead-percent** コマンドを使用することでデフォルト値を手動で上書きできます。

たとえば、Cisco IOS ソフトウェアが 100 バイトの予約要求を取得したときに、発信インターフェイスが GRE または mGRE インターフェイスの場合は、そのトンネル インターフェイスで 104 バイトの帯域予約要求がローカルで使用可能になります。GRE または mGRE インターフェイスが保護モードの場合は、それぞれのリンクで 110 バイトが要求されます。この IP オーバーヘッドは、RSVP を介して示される帯域幅には影響しません。

例

次に、ルータを設定してパーセンテージ帯域幅を手動で上書きする例を示します。

```
Router(config)# interface tunnel 1
Router(config-if)# ip rsvp tunnel overhead-percent 20
```

関連コマンド

コマンド	説明
showiprsvpinterfacedetail	すべてのインターフェイスの hello 設定を表示します。

ip rsvp udp-multicasts

IP カプセル化マルチキャスト パケットを生成するたびに、User Datagram Protocol（UDP）カプセル化リソース予約プロトコル（RSVP）マルチキャストを生成するようにルータに指示するには、インターフェイス コンフィギュレーション モードで **iprsvpudp-multicasts** 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。

ip rsvp udp-multicasts [*multicast-address*]
no ip rsvp udp-multicasts [*multicast-address*]

構文の説明

multicast-address	（任意）ルータのホスト名または UDP マルチキャスト アドレスです。

コマンド デフォルト

UDP マルチキャストの生成は無効になっています。システムが UDP カプセル化 RSVP メッセージをルータに送信すると、ルータは隣接システムとの通信のために UDP の使用を開始します。ルータはマルチキャスト アドレス 224.0.0.14 を使用し、UDP ポート 1699 への送信を開始します。マルチキャスト アドレスを指定せずにコマンドを入力した場合、ルータは同じマルチキャスト アドレスを使用します。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
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。

使用上のガイドライン

このコマンドを使用して、ルータが IP カプセル化マルチキャスト パケットを生成するときはいつでも、UDP カプセル化 RSVP マルチキャストを生成するようにルータに指示します。一部のホストは、ルータからのこのトリガーを必要とします。

RSVP は、VIP 分散型シスコ エクスプレス フォワーディング（dCEF）で設定できません。

例

次の例では、イーサネット インターフェイス 2 で最大 7500 kbps を予約し、フローごとに最大 1 Mbps を予約します。ルータは、マルチキャスト アドレス 224.0.0.14 で UDP カプセル化を使用するように設定されます。

```
interface ethernet 2
 ip rsvp bandwidth 7500 1000
 ip rsvp udp-multicasts 224.0.0.14
```

関連コマンド

Command	Description
iprsvpbandwidth	インターフェイスで IP 用 RSVP をイネーブルにします。
iprsvpneighbor	ネイバーによる予約の要求を有効にします。
iprsvpreservation	ルータが RSVP RESV メッセージの受信と転送をシミュレートできるようにします。
iprsvpsender	ルータが RSVP PATH メッセージの受信と転送をシミュレートできるようにします。

ip rsvp udp neighbor

ネイバールータがUDPを介してリソース予約プロトコル（RSVP）制御パケットを処理および送信できるようにするには、グローバル コンフィギュレーション モードで **ip rsvp udp neighbor** コマンドを使用します。ネイバー ルータがUDPを介してRSVPコントロール パケットを処理および送信できないようにするには、このコマンドの **no** 形式を使用します。

ip rsvp udp neighbor *neighbor-IP-address* **router** [**vrf** *vrf-name*]

no ip rsvp udp neighbor *neighbor-IP-address* **router** [**vrf** *vrf-name*]

構文の説明

neighbor-IP-address	ネイバー ルータのIPアドレス。
router	ネイバーがルータであることを指定します。
vrf *vrf-name*	（任意）。Virtual Routing and Forwarding（VRF）インスタンス名を指定します。

コマンド デフォルト

ip rsvp udp neighbor コマンドはデフォルトで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	変更箇所
15.2(4)M	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 rsvp udp neighbor コマンドは、ネイバー ルータが未加工のIPではなくUDPを介して最初のホップルータと通信できるようにするために使用できます。また、このコマンドは、2台のルータの間にあるファイアウォールがセキュリティ上の懸念のために未加工のIPパケットをドロップし、UDPパケットは許可するシナリオで使用できます。

例

次に、IPアドレス10.1.1.1のネイバー ルータが、UDPを介してRSVP制御パケットを処理および送信できるようにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip rsvp udp neighbor 10.1.1.1 router vrf vrf-1
```

関連コマンド

コマンド	説明
ip rsvp bandwidth	インターフェイスでIP用RSVPを有効にします。

ip rtp compression-connections

インターフェイスに存在できる Real-Time Transport Protocol（RTP）ヘッダー圧縮接続の総数を指定するには、インターフェイス コンフィギュレーション モードで **iprtpcompression-connections** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ip rtp compression-connections *number*
no ip rtp compression-connections

構文の説明

number	3 ～ 1000 の範囲の、キャッシュがサポートする RTP ヘッダー圧縮接続の数です。

コマンド デフォルト

PPP およびハイレベル データ リンク制御（HDLC）インターフェイスの場合、デフォルトの圧縮接続数は 16 です。

フレーム リレー インターフェイスの場合、デフォルトの圧縮接続数は 256 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
11.3	このコマンドが導入されました。
12.0(7)T	PPP および HDLC インターフェイスの場合の圧縮接続の最大数が 256 から 1000 に増加しました。 フレーム リレー インターフェイスの場合の圧縮接続の最大数が 32 から 256 に増加しました。デフォルトの圧縮接続数が 32（固定）から 256（設定可能）に増加しました。
12.1(4)E	このコマンドは、Cisco 7100 シリーズに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
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。

使用上のガイドライン

指定されたインターフェイスを介した RTP コールごとに 1 つの接続を設定する必要があります。

各接続によって、圧縮のキャッシュ エントリが設定され、結果として、キャッシュ エントリの最大数とキャッシュのサイズを指定することになります。指定したインターフェイスのキャッシュ エントリが少なすぎるとパフォーマンスが低下し、キャッシュ エントリが多すぎると、メモリが無駄になる可能性があります。

（注） シリアル接続の両端では、同じ数のキャッシュ エントリを使用する必要があります。

例

次の例では、サポートされる RTP ヘッダー圧縮接続の数を 150 に変更します。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression
Router(config-if)# ip rtp compression-connections 150
Router(config-if)# end
```

関連コマンド

Command	Description
iprtpheader-compression	RTP ヘッダー圧縮をイネーブルにします。
showiprtpheader-compression	RTPヘッダー圧縮の統計情報を表示します。

ip rtp header-compression

Real-Time Transport Protocol（RTP）ヘッダー圧縮を有効にするには、インターフェイス コンフィギュレーション モードで **iprtpheader-compression** コマンドを使用します。RTP ヘッダー圧縮を無効にするには、このコマンドの **no** 形式を使用します。

ip rtp header-compression [{**passive**|**iphc-format**|**ietf-format**}] **[periodic-refresh]**
no ip rtp header-compression [{**passive**|**iphc-format**|**ietf-format**}] **[periodic-refresh]**

構文の説明

passive	（任意）同じインターフェイス上の着信 RTP パケットが圧縮されている場合にだけ、発信 RTP パケットを圧縮します。**passive** キーワードを指定しない場合、すべての RTP パケットが圧縮されます。
iphc-format	（任意）ヘッダー圧縮に IP ヘッダー圧縮（IPHC）形式を使用することを意味します。
ietf-format	（任意）ヘッダー圧縮にインターネット技術特別調査委員会（IETF）形式を使用することを意味します。
periodic-refresh	（任意）圧縮された IP ヘッダーを定期的にリフレッシュすることを意味します。

コマンド デフォルト

無効

PPP インターフェイスの場合、ヘッダー圧縮のデフォルト形式は IPHC です。

High-Level Data Link Control（HDLC; ハイレベル データリンク制御）およびフレームリレー インターフェイスの場合、ヘッダー圧縮のデフォルト形式はオリジナルのシスコ独自形式です。シスコ独自形式の圧縮接続数は最大 256 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
11.3	このコマンドが導入されました。
12.0	このコマンドが Cisco IOS Release 12.0 に統合されました。**iphc-format** キーワードが含まれるように、このコマンドが変更されました。
12.3(2)T	このコマンドが、Cisco IOS Release 12.3(2)T に統合されました。このコマンドは、**periodic-refresh** キーワードを含むように変更されました。
12.3(4)T	**ietf-format** キーワードが含まれるように、このコマンドが変更されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
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。

リリース	変更箇所
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

ヘッダーの圧縮

IP/ユーザ データグラム プロトコル（UDP）/RTP ヘッダーを圧縮してパケットのサイズを小さくできます。RTP の場合、RTP ペイロード サイズを 20 バイトまで圧縮できるため、ヘッダーの圧縮は特に有効です。未圧縮のヘッダーは 40 バイトです。

passive キーワード

デフォルトでは、**iprtpheader-compression** コマンドは発信 RTP トラフィックを圧縮します。**passive** キーワードを指定すると、発信 RTP トラフィックが圧縮されるのは、同じインターフェイスの着信 RTP トラフィックが圧縮される場合のみです。**passive** キーワードを指定しない場合、すべての発信 RTP トラフィックが圧縮されます。

PPP インターフェイスでは、**passive** キーワードは無視されます。PPP インターフェイスでは、**passive** キーワードの指定の有無にかかわらず、ヘッダー圧縮の使用をネゴシエートします。したがって、**passive** キーワードは PPP インターフェイスのデフォルト形式である IPHC 形式に置き換えられます。

iphc-format キーワード

iphc-format キーワードは、ヘッダー圧縮に IPHC 形式を使用することを意味します。PPP および HDLC インターフェイスの場合、**iphc-format** キーワードを指定すると、TCP ヘッダー圧縮も有効化されます。このような理由から、**showrunning-config** コマンドの出力には、**iptcpheader-compression** コマンドが表示されます。RTP ヘッダー圧縮と TCP ヘッダー圧縮の両方がイネーブルなので、UDP パケットと TCP パケットの両方が圧縮されます。

iphc-format キーワードには、宛先ポート番号が偶数かどうかの確認と、その範囲が 16,385 ～ 32,767 であるか（シスコ オーディオの場合）または 49,152 ～ 65,535 であるか（シスコ ビデオの場合）の確認が含まれます。基準を満たす有効な RTP パケット（つまり、ポート番号が偶数で指定した範囲内であるパケット）の場合、圧縮 RTP パケット形式を使用して圧縮されます。それ以外の場合、効率が低い圧縮の非 TCP パケット形式を使用してパケットが圧縮されます。

iphc-format キーワードは、フレームリレー カプセル化を使用するインターフェイスに使用できません。

（注） ヘッダー圧縮形式（この場合は IPHC）は、ネットワークの両端で同じにする必要があります。つまり、ローカル ルータで **iphc-format** キーワードを指定する場合、リモート ルータでも **iphc-format** キーワードを指定する必要があります。

ietf-format キーワード

ietf-format キーワードは、ヘッダー圧縮に IETF 形式を使用することを意味します。HDLC インターフェイスの場合、**ietf-format** キーワードで UDP パケットのみが圧縮されます。PPP インターフェイスの場合、**ietf-format** キーワードを指定すると、TCP ヘッダー圧縮も有効化されます。このような理由から、**showrunning-config** コマンドの出力には、**iptcpheader-compression** コマンドが表示されます。RTP ヘッダー圧縮と TCP ヘッダー圧縮の両方がイネーブルなので、UDP パケットと TCP パケットの両方が圧縮されます。

ietf-format キーワードを使用する場合、1025 以上の任意の偶数の宛先ポート番号を使用できます。基準を満たす有効な RTP パケット（つまり、ポート番号が偶数で 1025 以上のパケット）の場合、圧縮 RTP パケット形式を使用して圧縮されます。それ以外の場合、効率が低い圧縮の非 TCP パケット形式を使用してパケットが圧縮されます。

ietf-format キーワードは、フレームリレーカプセル化を使用するインターフェイスに使用できません。

（注） ヘッダー圧縮形式（この場合はIETF）は、ネットワークの両端で同じにする必要があります。つまり、ローカル ルータで **ietf-format** キーワードを指定する場合、リモート ルータでも **ietf-format** キーワードを指定する必要があります。

シリアル回線のサポート

RTP ヘッダー圧縮は、フレームリレー、HDLC、または PPP カプセル化を使用するシリアル回線上でサポートされます。シリアル接続の両端で圧縮をイネーブルにする必要があります。

ユニキャストまたはマルチキャスト RTP パケット

このコマンドによりユニキャストまたはマルチキャスト RTP パケットを圧縮できます。したがって、低速リンクを使用する Multicast Backbone（MBONE; マルチキャスト バックボーン）トラフィックも圧縮できます。この圧縮方式は、オーディオ トラフィックのようにペイロード サイズが小さい場合にだけ効果があります。

カスタムまたはプライオリティ キューイング

iprtpheader-compression コマンドを使用して、カプセル化 HDLC またはフレーム リレー インターフェイスでカスタムまたはプライオリティ キューイングを設定する場合、圧縮パケットがユーザ定義のキューの代わりにデフォルト キューに移動することがあり、これによりプロトコル フラップ（キープアライブの損失）が発生します。そのため、Quality of Service（QoS）機能の設定には、モジュラ QoS コマンドライン インターフェイス（CLI）（MQC）モデルを使用することをお勧めします。

例

次に、Serial1/0 インターフェイスでの RTP ヘッダー圧縮をイネーブルにし、RTP ヘッダー圧縮接続の数を 10 までに制限する例を示します。この例では、**iprtpheader-compression** コマンドのオプションの **iphc-format** キーワードが指定されています。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0
```

```
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# end
```

次に、Serial2/0 インターフェイスでの RTP ヘッダー圧縮を有効にし、RTP ヘッダー圧縮接続の数を 20 までに制限する例を示します。この例では、**iprtpheader-compression** コマンドのオプションの **ietf-format** キーワードが指定されています。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression ietf-format
Router(config-if)# ip rtp compression-connections 20
Router(config-if)# end
```

次の例では、Serial1/0 インターフェイスで RTP ヘッダー圧縮が有効になり、**iprtpheader-compression** コマンドのオプションの **periodic-refresh** キーワードが指定されています。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format periodic-refresh
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# end
```

関連コマンド

Command	Description
cleariprtpheader-compression	RTP ヘッダー圧縮構造および統計情報をクリアします。
iprtpcompression-connections	インターフェイス上に存在できる RTP ヘッダー圧縮接続数の合計数を指定します。
showiprtpheader-compression	RTP ヘッダー圧縮の統計情報を表示します。
showrunning-config	現在実行中のコンフィギュレーション ファイルまたは特定のインターフェイスのコンフィギュレーションの内容、またはマップ クラス情報を表示します。

ip rtp priority

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**iprtppriority** コマンドは非表示です。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンド シーケンス）を使用する必要があります。詳細（代替コマンドのリストを含む）については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**iprtppriority** コマンドは、モジュラ QoS CLI（MQC）コマンド（または MQC コマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

User Datagram Protocol（UDP）宛先ポートの範囲に属する Real-Time Transport Protocol（RTP）パケット フローのセットのための絶対優先キューを予約するには、インターフェイス コンフィギュレーション モードで **iprtppriority** コマンドを使用します。絶対優先キューを無効にするには、このコマンドの **no** 形式を使用します。

ip rtp priority *starting-rtp-port-number port-number-range bandwidth*
no ip rtp priority

構文の説明

starting-rtp-port-number	開始 RTP ポート番号。パケットが送信先となる最小のポート番号です。ポート番号の範囲は、2000 ～ 65,535 です。
port-number-range	UDP 宛先ポートの範囲。*starting-rtp-port-number* 引数に加算することで、最大 UDP ポート番号が求められる番号です。UDP 宛先ポートの範囲は 0 ～ 16,383 です。
bandwidth	許可される最大の帯域幅（kbps 単位）。最大許容帯域幅は 0 ～ 2000 です。

コマンド デフォルト

無効

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
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。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

使用上のガイドライン

このコマンドは、音声アプリケーション、またはその他の遅延の影響を受けやすいアプリケーションに最も効果的です。

このコマンドは、同じ出力インターフェイスを使用するその他のキューまたはクラスに対して、音声トラフィックの絶対優先サービスが保証される UDP/RTP ポートの範囲を指定できるようにすることで、**iprtpreserve** コマンドによって提供される機能を拡張し、向上させます。絶対優先とは、パケットがプライオリティ キューに存在する場合、そのパケットのキューが解除され、最初に送信されるということです。つまり、キューが解除されたその他のパケットよりも先に送信されます。音声設定には、**iprtpreserve** コマンドの代わりに **iprtppriority** コマンドを使用することをお勧めします。

このコマンドは、同じ発信インターフェイスで重み付け均等化キューイング（WFQ）またはクラスベース WFQ（CBWFQ）と併用できます。いずれの場合にも、プライオリティ キューに対して指定された範囲のポートに一致するトラフィックは、他の CBWFQ クラスまたは WFQ フローよりも確実に優先されることが保証され、プライオリティ キュー内の音声パケットは常に最初に処理されます。

iprtppriority コマンドを使用するときは、次のガイドラインに従ってください。

- WFQ と併用する場合、**iprtppriority** コマンドで音声に絶対優先を与え、WFQ スケジューリングは残りのキューに適用されます。
- CBWFQ と併用する場合、**iprtppriority** コマンドで音声に絶対優先を与えます。CBWFQ は、専用帯域幅が必要な、またベストエフォートよりは優先する必要があるが絶対優先は必要ではない、他の種類のトラフィック（システム ネットワーク アーキテクチャ（SNA）など）のクラスの設定に使用できます。非音声トラフィックは、キューに入力されたパ

ケットに割り当てられた重みに基づいて均等に処理されます。またCBWFQは、設定されている場合、デフォルトの CBWFQ クラスでフローベース WFQ をサポートします。

bandwidth 引数を設定するときは、次のガイドラインに従ってください。

- プライオリティ キューに、必要だとわかっている帯域幅の量より少し多めに割り当てるのが最も安全です。これにより、ネットワーク バーストが発生しても対応できます。
- IP RTP プライオリティ アドミッション コントロール ポリシーは、RTP ヘッダー圧縮を考慮します。したがって、**iprtppriority** コマンドの *bandwidth* 引数を設定している間は、圧縮コールの帯域幅の設定のみが必要です。*bandwidth* 引数は最大合計帯域幅です。複数のコールがある場合は、すべてのコールに十分な帯域幅を割り当てる必要があります。
- レイヤ2ヘッダーに対応できる帯域幅を設定します。帯域幅の割り当てでは、ペイロードと IP、UDP、および RTP ヘッダーについては考慮されていますが、レイヤ 2 ヘッダーは考慮されていません。他のオーバーヘッドに対し 25 % の帯域幅を割り当てるのが、慎重で安全です。
- デフォルトの予約可能な最大帯域幅を変更していない限り、インターフェイス上の音声およびデータ フローのためのすべての帯域幅割り当ての合計は、利用可能な全帯域幅の 75 %を超えないようにしてください。予約可能な最大帯域幅を変更するには、そのインターフェイスで **max-reserved-bandwidth** コマンドを使用します。

IP RTP プライオリティ帯域幅割り当ての詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の章「Congestion Management Overview」のセクション「IP RTP Priority」を参照してください。

例

次の例では、まず CBWFQ 設定を定義してから、開始 RTP ポート番号 16384、16383 の範囲の UDP ポート、最大帯域幅 40 kbps の値を使用して、絶対優先キューを予約します。

```
! The following commands define a class map:
class-map class1
 match access-group 101
 exit
! The following commands create and attach a policy map:
policy-map policy1
class class1
 bandwidth 3000
 queue-limit 30
 random-detect
 random-detect precedence 0 32 256 100
 exit
interface Serial1
 service-policy output policy1
! The following command reserves a strict priority queue:
 ip rtp priority 16384 16383 40
```

関連コマンド

Command	Description
bandwidth(policy-mapclass)	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。
fairqueue(WFQ)	インターフェイスに対する WFQ を有効にします。
frame-relayiprtppriority	UDP 宛先ポートの範囲に属する RTP パケット フロー セットのフレーム リレー PVC について、絶対優先キューを予約します。
iprtpreserve	UDP宛先ポートの範囲に属するRTPパケットフローのセット用に、特殊キューを確保します。
max-reserved-bandwidth	CBWFQ、LLQ、および IP RTP プライオリティに割り当てるインターフェイス帯域幅のパーセント比率を変更します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
pppmultilink	インターフェイス上で MLP を有効にして、オプションで動的帯域幅割り当てを有効にします。
pppmultilinkfragment-delay	MLP バンドル上のパケット フラグメントの伝送に許容される最大遅延を設定します。
pppmultilinkinterleave	MLP バンドル上でのより大きなパケットのフラグメント間での RTP パケットのインターリーブを有効にします。
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与えます。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。

ip tcp compression-connections

インターフェイス上に存在できる Transmission Control Protocol（TCP）ヘッダー圧縮接続の総数を指定するには、インターフェイス コンフィギュレーション モードで **iptcpcompression-connections** コマンドを使用します。デフォルトに復元するには、このコマンドの **no** 形式を使用します。

ip tcp compression-connections *number*
no ip tcp compression-connections

構文の説明

number	3 ～ 256 の範囲の、キャッシュがサポートする TCP ヘッダー圧縮接続の数です。

コマンド デフォルト

PPP およびハイレベルデータ リンク制御（HDLC）インターフェイスの場合、デフォルトの圧縮接続数は 16 です。

フレーム リレー インターフェイスの場合、デフォルトの圧縮接続数は 256 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	変更箇所
10.0	このコマンドが導入されました。
12.0(7)T	フレーム リレー インターフェイスの場合の圧縮接続の最大数が 32 から 256 に増加しました。デフォルトの圧縮接続数が 32（固定）から 256（設定可能）に増加しました。
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。

使用上のガイドライン

指定されたインターフェイスを介した TCP 接続ごとに 1 つの接続を設定する必要があります。

各接続によって、圧縮のキャッシュ エントリが設定され、結果として、キャッシュ エントリの最大数とキャッシュのサイズを指定することになります。指定したインターフェイスのキャッシュ エントリが少なすぎるとパフォーマンスが低下し、キャッシュ エントリが多すぎると、メモリが無駄になる可能性があります。

（注） シリアル接続の両端では、同じ数のキャッシュ エントリを使用する必要があります。

例

次に、最初のシリアル インターフェイスに、最大 10 個のキャッシュ エントリを使用するヘッダー圧縮を設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

関連コマンド

Command	Description
iptcpheader-compression	TCPヘッダー圧縮をイネーブルにします。
showiptcpheader-compressions	TCPヘッダー圧縮統計情報を表示します。

ip tcp header-compression

Transmission Control Protocol（TCP）ヘッダー圧縮を有効にするには、インターフェイス コンフィギュレーション モードで **iptcpheader-compression** コマンドを使用します。圧縮を無効にするには、このコマンドの **no** 形式を使用します。

ip tcp header-compression [{**passive**|**iphc-format**|**ietf-format**}]
no ip tcp header-compression [{**passive**|**iphc-format**|**ietf-format**}]

構文の説明

passive	（任意）同じインターフェイス上の着信TCPパケットが圧縮されている場合にだけ、発信 TCP パケットを圧縮します。**passive** キーワードを指定しない場合、すべての TCP パケットが圧縮されます。
iphc-format	（任意）ヘッダー圧縮に IP ヘッダー圧縮（IPHC）形式を使用することを意味します。
ietf-format	（任意）ヘッダー圧縮にインターネット技術特別調査委員会（IETF）形式を使用することを意味します。

コマンド デフォルト

PPP インターフェイスの場合、ヘッダー圧縮のデフォルト形式は IPHC です。

ハイレベル データリンク制御（HDLC）およびフレーム リレー インターフェイスの場合、デフォルト形式は RFC 1144、*Compressing TCP/IP Headers for Low-Speed Serial Links*（低速シリアル リンク向け TCP/IP ヘッダー圧縮）の記述に従います。

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	変更箇所
10.0	このコマンドが導入されました。
12.0	このコマンドが Cisco IOS Release 12.0 に統合されました。**iphc-format** キーワードが含まれるように、このコマンドが変更されました。
12.3(4)T	このコマンドが、Cisco IOS Release 12.3(4)T に統合されました。このコマンドは、**ietf-format** キーワードを含むように変更されました。
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。

使用上のガイドライン

TCP/IP パケットのヘッダーを圧縮してパケットのサイズを小さくできます。TCP ヘッダー圧縮は、フレームリレー、HDLC、または PPP カプセル化を使用するシリアル回線上でサポート

されます。シリアル接続の両端で圧縮をイネーブルにする必要があります。TCPヘッダーを圧縮すると、Telnet 接続が大幅に高速化されます。

一般に、トラフィックが大きなパケットで構成されずに多数の小さなパケットで構成されている場合、TCPヘッダーを圧縮するとメリットがあります。トランザクション処理（通常は端末を使用）には小さなパケットが使用され、ファイル転送には大きなパケットが使用される傾向があります。この機能ではTCPヘッダーだけを圧縮するため、User Datagram Protocol（UDP）パケットまたは他のプロトコル ヘッダーには影響ありません。

passive キーワード

デフォルトでは、**ip tcpheader-compression** コマンドは発信 TCP トラフィックを圧縮します。**passive** キーワードを指定した場合、同じインターフェイス上の着信 TCP トラフィックが圧縮されている場合にだけ、発信 TCP トラフィックが圧縮されます。**passive** キーワードを指定しない場合、すべての発信 TCP トラフィックが圧縮されます。

PPP インターフェイスの場合、**passive** キーワードは無視されます。PPP インターフェイスでは、**passive** キーワードの指定の有無にかかわらず、ヘッダー圧縮の使用をネゴシエートします。したがって、**passive** キーワードはPPPインターフェイスのデフォルト形式であるIPHC形式に置き換えられます。

iphc-format キーワード

iphc-format キーワードは、ヘッダー圧縮にIPHC形式を使用することを意味します。PPPおよびHDLCインターフェイスの場合、**iphc-format** キーワードを指定すると、Real-Time Transport Protocol（RTP）ヘッダー圧縮も有効になります。このような理由から、**showrunning-config** コマンドの出力には、**iprtpheader-compression** コマンドが表示されます。TCP および RTP 両方のヘッダー圧縮がイネーブルになるため、TCP および UDP パケットの両方が圧縮されます。

iphc-format キーワードは、フレームリレー カプセル化を使用するインターフェイスに使用できません。

（注） ヘッダー圧縮形式（この場合はIPHC）は、ネットワークの両端で同じにする必要があります。つまり、ローカル ルータで **iphc-format** キーワードを指定する場合、リモート ルータでも **iphc-format** キーワードを指定する必要があります。

ietf-format キーワード

ietf-format キーワードは、ヘッダー圧縮に IETF 形式を使用することを意味します。HDLC インターフェイスの場合、**ietf-format** キーワードでTCPパケットのみが圧縮されます。PPPインターフェイスの場合、**ietf-format** キーワードを指定すると、RTPヘッダー圧縮も有効化されます。このような理由から、**showrunning-config** コマンドの出力には、**iprtpheader-compression** コマンドが表示されます。TCPおよびRTP両方のヘッダー圧縮がイネーブルになるため、TCPおよびUDPパケットの両方が圧縮されます。

ietf-formatキーワードは、フレームリレーカプセル化を使用するインターフェイスに使用できません。

（注） ヘッダー圧縮形式（この場合はIETF）は、ネットワークの両端で同じにする必要があります。つまり、ローカル ルータで **ietf-format** キーワードを指定する場合、リモート ルータでも **ietf-format** キーワードを指定する必要があります。

例

次に、最初のシリアル インターフェイスに、最大 10 個のキャッシュ エントリを使用するヘッダー圧縮を設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

次に、Serial1/0.0サブインターフェイスでRTPヘッダー圧縮を有効にし、RTPヘッダー圧縮接続数を10に制限する例を示します。この例では、**iptcpheader-compression** コマンドのオプションの **iphc-format** キーワードが指定されています。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression iphc-format
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

次に、Serial2/0.0サブインターフェイスでRTPヘッダー圧縮を有効にし、RTPヘッダー圧縮接続数を20に制限する例を示します。この例では、**iptcpheader-compression** コマンドのオプションの **ietf-format** キーワードが指定されています。

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression ietf-format
Router(config-if)# ip tcp compression-connections 20
Router(config-if)# end
```

関連コマンド

Command	Description
iptcpcompression-connections	インターフェイス上に存在できるTCPヘッダー圧縮接続数の合計数を指定します。
showiptcpheader-compression	TCP/IP ヘッダー圧縮統計情報を表示します。
showrunning-config	現在実行中のコンフィギュレーション ファイルまたは特定のインターフェイスのコンフィギュレーションの内容、またはマップ クラス情報を表示します。

iphc-profile

IP ヘッダー圧縮（IPHC）プロファイルを作成し、IPHC プロファイル コンフィギュレーション モードにするには、グローバル コンフィギュレーション モードで **iphc-profile** コマンドを使用します。既存の IPHC プロファイルをインターフェイスまたはサブインターフェイスにアタッチするには、インターフェイス コンフィギュレーション モードで **iphc-profile** コマンドを使用します。IPHC 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。

iphc-profile *profile-name* {**ietf**|**van-jacobson**}
no iphc-profile *profile-name*

構文の説明

profile-name	作成またはアタッチされる IPHC プロファイルの名前です。この IPHC プロファイルの名前には最大 32 文字まで指定できます。この名前に、引用符、空白、または特殊文字を含めることはできません。
ietf	IPHC プロファイルが Internet Engineering Task Force（IETF）ヘッダー圧縮用であることを指定します。
van-jacobson	IPHC プロファイルが Van Jacobson ヘッダー圧縮用であることを指定します。

コマンド デフォルト

IPHC プロファイルは作成またはアタッチされません。

コマンド モード

グローバル コンフィギュレーション（IPHC プロファイルを作成するため）
インターフェイス コンフィギュレーション（既存の IPHC プロファイルをインターフェイスまたはサブインターフェイスに接続するため）

コマンド履歴

リリース	変更箇所
12.4(9)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

iphc-profile コマンドは、ヘッダー圧縮を有効にするために使用される IPHC プロファイルを作成し、IPHC プロファイル コンフィギュレーション モード（config-iphcp）にします。IPHC プロファイルはテンプレートで、使用するヘッダー圧縮のタイプを設定したり、オプション機能やヘッダー圧縮の設定を有効にして、そのプロファイルをインターフェイス、サブインターフェイス、またはフレーム リレー相手先固定接続（PVC）に適用できます。

IPHC プロファイル タイプの指定

IPHC プロファイルを作成するときは、**ietf** キーワードまたは **van-jacobson** キーワードを使用して IPHC プロファイル タイプを指定する必要があります。IETF プロファイル タイプは、RFC 2507、RFC 2508、RFC 3544、および RFC 3545 により確立されている標準規格に準拠し、この標準規格をサポートしています。通常、TCP 以外のヘッダー圧縮（RTP ヘッダー圧縮など）に関連付けられます。Van Jacobson プロファイル タイプは、RFC 1144 により確立されている標

準規格に準拠し、この標準規格をサポートしています。通常、TCPヘッダー圧縮に関連付けられます。

（注） フレーム リレー カプセル化を使用する場合は、（**van-jacobson** キーワードではなく）**ietf** キーワードを指定する必要があります。

IPHC プロファイル タイプを指定するときの検討事項

IPHC プロファイル タイプを指定するときは、TCP トラフィックを圧縮するのか、TCP 以外のトラフィック（つまり、RTP トラフィック）を圧縮するのかを検討します。また、トラフィックを受信するリモート ネットワーク リンクのヘッダー圧縮形式の機能についても検討します。指定する IPHC プロファイル タイプは、IPHC プロファイルを適用するリモート ネットワーク リンクで使用するヘッダー圧縮フォーマットに直接影響します。Van Jacobson IPHC プロファイルを使用すると TCP トラフィックのみがリモート ネットワーク リンクで圧縮されるのに対して、IETF IPHC プロファイルを使用すると TCP トラフィックまたは TCP 以外のトラフィック（RTP トラフィックなど）がリモート ネットワーク リンクで圧縮されます。

（注） 設定するルータで使用されているヘッダー圧縮形式と、リモート ネットワーク リンクで使用されているヘッダー圧縮形式が一致している必要があります。

設定可能なヘッダー圧縮の機能と設定

IPHC プロファイルの作成時に指定する IPHC プロファイル タイプ（IETF または Van Jacobson）によって、設定可能な（つまり、有効化や変更ができる）ヘッダー圧縮の機能と設定の固有のセットが決まります。両方のセットを次に示します。

IPHC プロファイル タイプとして Van Jacobson を指定した場合は、TCP ヘッダー圧縮を有効にして、TCP コンテキストの数を設定することができます。次の表に、使用可能な Van Jacobson IPHC プロファイル タイプのヘッダー圧縮の機能と設定、およびそれを有効にするために使用するコマンドを示します。

表 *8 : Van Jacobson IPHC* プロファイル タイプのヘッダー圧縮の機能と設定

コマンド	機能または設定
tcp	TCP ヘッダー圧縮をイネーブルにします。
tcpcontexts	TCPヘッダー圧縮で使用可能なコンテキスト数を設定します。

IPHC プロファイル タイプとして IETF を指定した場合は、TCP 以外のヘッダー圧縮（つまり、RTP ヘッダー圧縮）を有効にして、多数の追加の機能や設定を有効にすることができます。次の表に、使用可能な IETF IPHC プロファイル タイプのヘッダー圧縮の機能と設定、およびそれを有効にするために使用するコマンドを示します。

表 *9 : IETF IPHC* プロファイル タイプのヘッダー圧縮の機能と設定

コマンド	機能または設定
feedback	インターフェイスまたはリンクからのコンテキスト ステータスのフィードバック メッセージを有効にします。
maximumheader	圧縮された IP ヘッダーの最大サイズを設定します。
non-tcp	TCP 以外のヘッダー圧縮を有効にします。
non-tcpcontexts	TCP 以外のヘッダー圧縮で使用可能なコンテキスト数を設定します。
rtp	RTP ヘッダー圧縮をイネーブルにします。
recoverable-loss	インターフェイスで Enhanced Compressed Real-Time Transport Protoco（ECRTP）を有効にします。
refreshmax-period refreshmax-time refreshrtp	フル ヘッダーがリフレッシュされる前に待機する時間などの、コンテキスト リフレッシュ（フルヘッダー リフレッシュ）オプションを設定します。
tcp	TCP ヘッダー圧縮をイネーブルにします。
tcpcontexts	TCP ヘッダー圧縮で使用可能なコンテキスト数を設定します。

IPHC プロファイルの詳細について

IPHC プロファイルを使用したヘッダー圧縮の設定の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、Release 12.4T の「Header Compression」モジュールと「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

例

次の例では、profile1 という名前の IPHC プロファイルが作成され、Van Jacobson IPHC プロファイル タイプが指定されます。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile1 van-jacobson
Router(config-iphcp)# end
```

次の例では、profile2 という名前の 2 番目の IPHC プロファイルが作成されます。この IPHC プロファイルには、IETF IPHC プロファイル タイプが指定されます。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# end
```

次の例では、profile2 という名前の既存の IPHC プロファイルをシリアル インターフェイス 3/0 にアタッチします。この IPHC プロファイルには、profile2 の IPHC プロファイル タイプ（この例では IETF）が指定されます。

```
Router> enable
Router# configure terminal
Router(config)# interface serial 3/0
Router(config-if)# iphc-profile profile2 ietf
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
feedback	インターフェイスまたはリンクからのコンテキスト ステータスのフィードバック メッセージを有効にします。
maximumheader	圧縮された IP ヘッダーの最大サイズを指定します。
non-tcp	IPHC プロファイルの非 TCP ヘッダー圧縮を有効にします。
non-tcpcontexts	TCP 以外のヘッダー圧縮で使用可能なコンテキスト数を設定します。
recoverable-loss	インターフェイスで ECRTP をイネーブルにします。
refreshmax-period	フルヘッダー リフレッシュが発生する間に送信するパケット数を設定します。
refreshmax-time	フルヘッダー リフレッシュが発生するまでに待機する時間を設定します。
refreshrtp	RTP ヘッダー圧縮のコンテキストのリフレッシュの発生を有効にします。
rtp	IPHC プロファイル内の RTP ヘッダー圧縮を有効にします。
showiphc-profile	1 つまたは複数の IPHC プロファイルの設定情報を表示します。
tcp	IPHC プロファイル内の TCP ヘッダー圧縮を有効にします。
tcpcontexts	TCP ヘッダー圧縮で使用可能なコンテキスト数を設定します。

lacp max-bundle

ポート チャネルで QoS 適用ポリシーを有効にするには、グローバル コンフィギュレーション モードで **platform qos-port-channel_aggregator** コマンドとともに **lacp max-bundle** コマンドを使用します。

lacp max-bundle *port-channel-number***bundle-number**

構文の説明

bundle-number	バンドル情報を表示します。

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

グローバル設定

コマンド履歴

リリース	変更箇所
XE 3.18 SP	このコマンドのサポートが ASR 900 シリーズ ルータに追加されました。

例

次の例は、イーサネット フロー ポイントがあるメイン インターフェイスでポート レベルのシェーピングを設定する方法を示しています。

```
enable
configure terminal
interface port-channel 1
no ip address
negotiation auto
lacp max-bundle 1
service-policy output parent-llq
service instance 1 ethernet

encapsulation dot1q 100
bridge-domain 100
end
```

関連コマンド

コマンド	説明
show policy-map interface port-channel	EFP のポリシー マップ コンフィギュレーションを検証します。

lane client qos

LANエミュレーション（LANE）Quality of Service（QoS）データベースをインターフェイスに適用するには、サブインターフェイス コンフィギュレーション モードで **laneclient** qos コマンドを使用します。インターフェイスからQoS over LANE機能を削除するには、このコマンドの **no** 形式を使用します。

lane client qos *database-name*
no lane client qos *database-name*

構文の説明

database-name	QoSデータベースの名前です。

コマンド デフォルト

デフォルトではこのコマンドは設定されていません。

コマンド モード

サブインターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(2)E	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
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。

例

次に、LANE QoS データベースをサブインターフェイスに適用する例を示します。

```
Router(config-subif)# lane client qos user1
```

関連コマンド

コマンド	説明
atm-address	特定のATMアドレスに関連付けられたQoSパラメータを指定します。
laneqosdatabase	QoS over LANE データベースを構築するプロセスを開始します。
showlaneqosdatabase	特定の QoS over LANE データベースの内容を表示します。
ubr+cos	CoS 値を UBR+ VCC にマップします。

lane qos database

LAN エミュレーション（LANE）Quality of Service データベースを構築するには、グローバル コンフィギュレーション モードで **laneqosdatabase** コマンドを使用します。LANE QoS データベース名を削除するには、このコマンドの **no** 形式を使用します。

lane qos database 名前
no lane qos database 名前

構文の説明

名前	LANE QoS データベースの名前です。

コマンド デフォルト

デフォルトではこのコマンドは設定されていません。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.1(2)E	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
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。

使用上のガイドライン

このコマンドは、QoS パラメータの名前付きデータベースを指定します。データベースは、LANE クライアントが設定されているサブインターフェイスに適用できます。

例

次に、Catalyst 5000 ファミリ ATM スイッチで user1 という名前の QoS over LANE データベースの設定を開始する例を示します。

```
ATM# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ATM(config)# lane qos database user1
```

次に、ルータで user2 という名前の QoS over LANE データベースの設定を開始する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# lane qos database user2
```

関連コマンド

コマンド	説明
atm-address	特定の ATM アドレスに関連付けられた QoS パラメータを指定します。
laneclientqos	QoS over LANE データベースをインターフェイスに適用します。
showlaneqosdatabase	特定の QoS over LANE データベースの内容を表示します。
ubr+cos	CoS 値を UBR+ VCC にマップします。

load protocol

プロトコルヘッダー説明ファイル（PHDF）をルータにロードするには、グローバルコンフィギュレーションモードで**loadprotocol**コマンドを使用します。指定された場所のすべてのプロトコルまたは単一のプロトコルをアンロードするには、このコマンドの**no**形式を使用します。

load protocol *location* **:** *filename*
no load protocol {*location* **:** *filenameprotocol-name*}

構文の説明

location **:** *filename*	ルータにロードされる PHDF の場所です。 このコマンドのnoバージョンで使用すると、指定されたファイル名からロードされたすべてのプロトコルがアンロードされます。 （注） この場所は、ルータのローカルにする必要があります。
protocol-name	指定されたプロトコルのみをアンロードします。 （注） フィルタによって参照されているプロトコルをアンロードしようとすると、エラーが発生します。

コマンド デフォルト

このコマンドが発行されていない場合、PHDF はルータにロードされません。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。
12.2(18)ZY	このコマンドが、Catalyst 6500 シリーズの Programmable Intelligent Services Accelerator（PISA）が搭載されているスイッチの Cisco IOS Release 12.2(18)ZY に統合されました。

使用上のガイドライン

Flexible Packet Matching により、プロトコル フィールド、長さ、およびパターンが指定されたパケットヘッダーの任意の部分に基づいてトラフィックを分類できます。プロトコルヘッダーは、PHDF という個別のファイルで定義されます。PHDF 内に定義されているフィールド名は、パケット フィルタの定義に使用されます。PHDF は、Extensible Markup Language（XML）の柔軟性を活用して、ほぼすべてのプロトコルヘッダーを説明できるファイルです。PHDF の重要なコンポーネントは、バージョン、XML ファイル スキーマの場所、およびプロトコル フィールド定義です。プロトコル フィールド定義では、プロトコル ヘッダーの適切なフィールドに名前を付け、フィールドを説明するコメントを考慮し、ヘッダーのプロトコルヘッダー フィールドの場所を提供し（オフセットはプロトコルヘッダーの開始に相対的です）、フィールドの長さを提供します。バイト単位またはビット単位を指定できます。

（注） ヘッダーの合計の長さは、各 PHDF の末尾で指定する必要があります。

冗長設定の場合、Flexible Packet Matching 設定で使用されるすべての PHDF が、対応するスタンバイ ディスクに存在することを確認する必要があります。PHDF がスタンバイ ディスクにない場合は、その PHDF を使用しているすべての Flexible Packet Matching ポリシーが破損します。

ユーザは、独自のカスタム PHDF を XML で作成することができます。ただし、ip.phdf、ether.phdf、tcp.phdf、および udp.phdf の標準 PHDF もルータにロードすることができます。

標準 PHDF は、Cisco.com（URL：http://www.cisco.com/cgi-bin/tablebuild.pl/fpm）で入手できます。

PHDF は XML を介して定義するため、実行コンフィギュレーションでは表示されません。

loadprotocol コマンドを発行して、プロトコル ヘッダー用の PHDF を定義およびロードすることにより、プロトコルにフィルタを適用します。

例

次に、ブラスタ パケット用に FPM を設定する方法の例を示します。このクラス マップには、TCP ポート 135、4444 または UDP ポート 69、および IP ヘッダーの開始から 3 バイトでのパターン 0x0030 という一致基準が含まれています。

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

次の例は、PHDF「ip.phdf」の XML 設定です。

```
<?xml version="1.0" encoding="UTF-8"?>
<phdf xsi:noNamespaceSchem
aLocation="D:\harinadh\Doc\Projects\FPME\XML\ex.xsd">
<protocol name="ip" description="Definition-for-the-IP-protocol">
<field name="version" description="IP-version">
<offset type="fixed-offset" units="bits"> 0 </offset>
<length type="fixed" units="bits">4</length>
</field>
<field name="ihl" description="IP-Header-Length">
<offset type="fixed-offset" units="bits">4</offset>
<length type="fixed" units="bits">4</length>
</field>
<field name="tos" description="IP-Type-of-Service">
<offset type="fixed-offset" units="bits">8</offset>
<length units="bits" type="fixed">8</length>
</field>
<field name="length" description="IP-Total-Length">
<offset type="fixed-offset" units="bytes">2</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="identification" description="IP-Identification">
<offset type="fixed-offset" units="bytes">4</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="flags" description="IP-Fragmentation-Flags">
<offset type="fixed-offset" units="bytes">6</offset>
<length type="fixed" units="bits">3</length>
</field>
<field name="fragment-offset" description="IP-Fragmentation-Offset”>
<offset type="fixed-offset" units="bits">51</offset>
<length type="fixed" units="bits">13</length>
</field>
<field name="ttl" description="Definition-for-the-IP-TTL">
<offset type="fixed-offset" units="bytes">8</offset>
<length type="fixed" units="bytes">1</length>
</field>
<field name="protocol" description="IP-Protocol">
<offset type="fixed-offset" units="bytes">9</offset>
<length type="fixed" units="bytes">1</length>
</field>
<field name="checksum" description="IP-Header-Checksum">
<offset type="fixed-offset" units="bytes">10</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="source-addr" description="IP-Source-Address">
<offset type="fixed-offset" units="bytes">12</offset>
<length type="fixed" units="bytes">4</length>
</field>
<field name="dest-addr" description="IP-Destination-Address">
<offset type="fixed-offset" units="bytes">16</offset>
<length type="fixed" units="bytes">4</length>
</field>
<headerlength type="fixed" value="20"></headerlength>
</protocol>
</phdf>
```

match access-group から mls ip pbr

- mac packet-classify （451 ページ）
- mac packet-classify use vlan （453 ページ）
- map ip （455 ページ）
- map ipv6 （458 ページ）
- map mpls （460 ページ）
- match access-group （462 ページ）
- match application（クラスマップ） （466 ページ）
- match any （470 ページ）
- match atm-clp （472 ページ）
- match atm oam （474 ページ）
- match atm-vci （476 ページ）
- match class-map （478 ページ）
- match cos （481 ページ）
- match cos inner （485 ページ）
- match destination-address mac （486 ページ）
- match discard-class （488 ページ）
- match dscp （490 ページ）
- match field （494 ページ）
- match flow pdp （497 ページ）
- match fr-dlci （499 ページ）
- match input vlan （501 ページ）
- match input-interface （505 ページ）
- match ip dscp （508 ページ）
- match ip precedence （509 ページ）
- match ip rtp （510 ページ）
- match mpls experimental （512 ページ）
- match mpls experimental topmost （515 ページ）
- match not （517 ページ）
- match packet length (class-map) （519 ページ）

- match port-type （522 ページ）
- match precedence （523 ページ）
- match protocol （528 ページ）
- match protocol attribute application-group （541 ページ）
- match protocol attribute category （544 ページ）
- match protocol attribute sub-category （546 ページ）
- match protocol attribute encrypted （549 ページ）
- match protocol attribute tunnel （551 ページ）
- match protocol (NBAR) （553 ページ）
- match protocol potentially (NBAR) （625 ページ）
- match protocol citrix （696 ページ）
- match protocol fasttrack （698 ページ）
- match protocol gnutella （700 ページ）
- match protocol http （702 ページ）
- match protocol pppoe-discovery （709 ページ）
- match protocol rtp （711 ページ）
- match qos-group （713 ページ）
- match source-address mac （716 ページ）
- match start （718 ページ）
- match tag (class-map) （721 ページ）
- match vlan (QoS) （722 ページ）
- match vlan inner （724 ページ）
- maximum（ローカル ポリシー） （726 ページ）
- maximum bandwidth ingress （728 ページ）
- maximum bandwidth percent （730 ページ）
- maximum header （732 ページ）
- max-reserved-bandwidth （734 ページ）
- metadata application-params （738 ページ）
- metadata flow （741 ページ）
- metadata flow (troubleshooting) （743 ページ）
- mls ip pbr （746 ページ）

mac packet-classify

レイヤ 3 パケットをレイヤ 2 パケットとして分類するには、インターフェイス コンフィギュレーション モードで **macpacket-classify** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac packet-classify [bpdu]
no mac packet-classify [bpdu]

構文の説明

bpdu	（任意）BPDUパケットへのレイヤ2ポリシーの適用を指定します。

コマンド デフォルト

レイヤ 3 パケットはレイヤ 2 パケットとして分類されません。

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	変更箇所
12.2(18)SXD	このコマンドのサポートが Supervisor Engine 720 に追加されました。
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。
12.2(50)SY	BPDU パケットでの MAC ACL のサポートが追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

マルチレイヤ MAC アクセス コントロール リスト（ACL）Quality of Service（QoS）のフィルタリングには、次のインターフェイス タイプを設定できます。

- レイヤ 3 アドレスが設定されていない VLAN インターフェイス
- Ethernet over Multiprotocol Label Switching（EoMPLS）をサポートするよう設定された物理 LAN ポート
- EoMPLS をサポートするよう設定された論理 LAN サブインターフェイス

マルチレイヤ MAC ACL QoS のフィルタリングを設定されたインターフェイス上で、MAC ACL により許可または拒否された入力トラフィックは、出力インターフェイスにより MAC 層トラフィックとして処理されます。マルチレイヤ MAC ACL QoS のフィルタリングを設定されたインターフェイス上で、MAC ACL により許可または拒否されたトラフィックに、出力 IP ACL を適用することはできません。

マイクロフロー ポリシングは、**macpacket-classify** コマンドが有効に設定されたインターフェイスでは機能しません。

macpacket-classify コマンドにより、レイヤ 3 パケットはレイヤ 2 パケットとして分類され、IP 分類は無効になります。

トラフィックは、802.1Q サービス クラス（CoS）、トランク VLAN、EtherType、および MAC アドレスに基づいて分類されます。

例

次に、着信および送信レイヤ 3 パケットをレイヤ 2 パケットとして分類する例を示します。

```
Router(config-if)# mac packet-classify
Router(config-if)#
```

次に、着信および送信レイヤ 3 パケットのレイヤ 2 パケットとしての分類を無効にする例を示します。

```
Router(config-if)# no mac packet-classify
Router(config-if)#
```

次に、BPDU パケットにレイヤ 2 ポリシーを適用する例を示します。

```
Router(config-if)# mac packet-classify bpdu
Router(config-if)#
```

次に、BPDU パケットでのレイヤ 2 ポリシーを無効にする例を示します。

```
Router(config-if)# no mac packet-classify bpdu
Router(config-if)#
```

関連コマンド

コマンド	説明
macpacket-classifyusevlan	VLAN ベースの QoS フィルタリングを MAC ACL でイネーブルにします。

mac packet-classify use vlan

MAC アクセス コントロール リスト（ACL）で VLAN ベースの Quality of Service（QoS）フィル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 **macpacket-classifyusevlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac packet-classify use vlan
no mac packet-classify use vlan

構文の説明

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 ACL での VLAN ベースの QoS フィルタリング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	変更箇所
12.2(18)SXD	このコマンドのサポートが、Supervisor Engine 720 および Supervisor Engine 2 に導入されました。
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。

使用上のガイドライン

このコマンドをサポートするのは、PFC3BXL または PFC3B モードだけです。

このコマンドは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

レイヤ 2 の Service Advertising Protocol（SAP）でエンコードされたパケット（Intermediate System-to-Intermediate System（IS-IS）および Internet Packet Exchange（IPX）など）に QoS を適用する場合は、**nomacpacket-classifyusevlan** コマンドを使用してレイヤ 2 のキーの VLAN フィールドを無効にする必要があります。

VLAN フィールドが有効な場合、QoS は非 Advanced Research Projects Agency（ARPA）レイヤ 2 パケット（IS-IS および IPX など）のポリシングを許可しません。

例

次に、IP パケットのレイヤ 2 の分類を有効にする例を示します。

```
Router(config)# mac packet-classify use vlan
Router(config)
```

次に、IP パケットのレイヤ 2 の分類を無効にする例を示します。

```
Router(config)# no mac packet-classify use vlan
Router(config)
```

関連コマンド

コマンド	説明
macpacket-classify	レイヤ2パケットとしてレイヤ3パケットを分類します。

map ip

POS SPA、チャネライズド SPA、およびクリアチャネル SPA 用に、すべての IPv4 パケット、またはDiffServ コードポイント（DSCP）値または優先順位値に基づく IPv4 パケットを高優先順位または低優先順位に分類するには、入力クラスマップ モードで **mapip** コマンドの次の形式を使用します。IPv4 設定を削除するには、ここに記載されているこのコマンドの **no** 形式を使用します。

すべての IPv4 パケットを分類するためのコマンド
map ip all queue {**strict-priority**|**0**}
no map ip all queue {**strict-priority**|**0**}

DSCP 値に基づいて IPv4 パケットを分類するためのコマンド
map ip {**dscp-based**|**dscp** {*dscp-valuedscp-range*} **queue** {**strict-priority**|**0**}}
no map ip {**dscp-based**|**dscp** {*dscp-valuedscp-range*} **queue** {**strict-priority**|**0**}}

優先順位値に基づいて IPv4 パケットを分類するためのコマンド
map ip {**precedence-based**|**precedence** {*precedence-valueprecedence-range*} **queue strict-priority**|**0**}
no map ip {**precedence-based**|**precedence** {*precedence-valueprecedence-range*} **queue strict-priority**|**0**}

構文の説明

allqueue	すべての IPv4 パケットの高優先順位または低優先順位の設定を暗黙的に指定します。
strict-priority	すべての IPv4 パケットを高優先順位（絶対優先）として分類します。
0	すべての IPv4 パケットを低優先順位として分類します。
dscp-based	IPv4 の DSCP 値に基づく分類を有効にします。
dscp	IPv4 パケット用に、DSCP 値または範囲を高優先順位または低優先順位として設定できます。
dscp-value	優先順位が高い、または低いと設定される DSCP 値です。
dscp-range	優先順位が高い、または低いと設定される dscp-value の範囲です。
queue	キュー全体、DSCP 値、または優先順位値の、高優先順位または低優先順位としての分類を有効にします。
precedence-based	IPv4 優先順位値に基づく分類を有効にします。
precedence	IPv4 パケット用に、IPv4 優先順位値または範囲を高優先順位または低優先順位として設定できます。
precedence-value	優先順位が高い、または低いと設定される優先順位値です。
precedence-range	優先順位が高い、または低いと設定される precedence-value の範囲です。

コマンド デフォルト

高優先順位にマッピングするIPv4DSCP値または優先順位値の設定が指定されていない場合、システムは DSCP 範囲 EF のパケットを高優先順位として扱い、優先順位範囲 6 ～ 7 を高優先順位として扱います。

コマンド モード

入力クラスマップ コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
3.1S	POS SPA、チャネライズド SPA、およびクリアチャネル SPA 用に、すべての IPv4 パケット、またはDSCP 値または優先順位値に基づく IPv4 パケットを高優先順位または低優先順位に分類するために、このコマンドが導入されました。

使用上のガイドライン

POS SPA、チャネライズド SPA、またはクリアチャネル SPA 用に、すべての IPv4 パケットを高優先順位または低優先順位に分類するには、**mapipallqueue** コマンドを使用します。

IPv4 パケットを特定の DSCP 値で分類するには、**mapipdscp-based** コマンドを使用して DSCP 分類を有効にします。IPv4パケットを特定のDSCP値で高優先順位または低優先順位に分類するには、**mapipdscp** {{*dscp-value*|*dscp-range*} **queue** {**strict-priority**|**0**}} コマンドを使用します。

IPv4 パケットを特定の優先順位値で分類するには、**mapipprecedence-based** コマンドを使用して優先順位分類を有効にします。IPv4パケットを特定の優先順位値で高優先順位または低優先順位に分類するには、**mapipprecedence** {{*precedence-value*|*precedence-range*} **queue** {**strict-priority**|**0**}} コマンドを使用します。

例

次に、**mapipallqueuestrict-priority** コマンドを使用してすべての IPv4 パケットを高優先順位として分類する例を示します。

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip all queue strict-priority
```

次に、DSCP 値が cs1 の IPv4 パケットを高優先順位として分類する例を示します。

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip dscp-based
Router(config-ing-class-map)# map ip dscp cs1 queue strict-priority
```

次に、優先順位値が 3 および 5 の IPv4 パケットを高優先順位として分類する例を示します。

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip precedence-based
Router(config-ing-class-map)# map ip precedence 3 5 queue strict-priority
```

関連コマンド

Command	Description
plimqosinputclass-map	分類テンプレートをインターフェイスにアタッチします。

map ipv6

POS SPA、チャネライズド SPA、およびクリアチャネル SPA のコンテキストで、すべての IPv6 パケット、または特定のトラフィック クラス（TC）値に基づく IPv6 パケットを高優先順位または低優先順位に分類するには、入力クラスマップ モードで **mapipv6** コマンドを使用します。IPv6 設定を削除するには、ここに記載されているこのコマンドの **no** 形式を使用します。

すべての IPv6 パケットを分類するためのコマンド
map ipv6 all queue {**strict-priority**|**0**}
no map ipv6 all queue {**strict-priority**|**0**}

IPv6 トラフィック クラス値を高優先順位または低優先順位に分類するためのコマンド
map ipv6 tc {*tc-valuetc-range*} **queue** {**strict-priority**|**0**}
no map ipv6 tc {*tc-valuetc-range*} **queue** {**strict-priority**|**0**}

構文の説明

allqueue	すべての IPv6 パケットの高優先順位または低優先順位の設定を暗黙的に指定します。
strict-priority	すべての IPv6 パケットを高優先順位（絶対優先）として分類します。
0	すべての IPv6 パケットを低優先順位として分類します。
tc	IPv6 パケット用に、トラフィック クラス値または範囲を高優先順位または低優先順位として設定できます。
tc-value	優先順位が高い、または低い（0）と設定される特定のトラフィック クラス値です。
tc-range	優先順位が高い、または低い（0）と設定されるトラフィック クラス値の範囲です。
queue	キュー全体、トラフィック クラス値、またはトラフィック クラス値の範囲の、高優先順位または低優先順位としての分類を有効にします。

コマンド デフォルト

どの IPv6 トラフィック クラス値を高優先順位にマッピングするかをユーザが設定していない場合、システムはトラフィック クラス EF のパケットを高優先順位として扱います。

コマンド モード

入力クラスマップ コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
3.1S	POS SPA、チャネライズド SPA、およびクリア チャネル SPA 用に、すべての IPv6 パケット、またはトラフィック クラス値に基づく IPv6 パケットを高優先順位または低優先順位に分類するために、このコマンドが導入されました。

使用上のガイドライン

POS SPA、チャネライズドSPA、またはクリアチャネルSPAのコンテキストで、すべてのIPv6パケットを高優先順位または低優先順位に分類するには、**mapipv6allqueue** コマンドを使用します。

IPv6パケットを特定のトラフィック クラス値で分類するには、**mapipv6tccs2queuestrict-priority** コマンドを使用します。

例

次に、**mapipv6allqueuestrict-priority** コマンドを使用してすべてのIPv6パケットを高優先順位として分類する例を示します。

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ipv6 all queue strict-priority
```

次に、トラフィック クラス値がcs2のIPv6パケットを高優先順位として分類する例を示します。

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip tc cs2 queue strict-priority
```

関連コマンド

Command	Description
plimqosinputclass-map	分類テンプレートをインターフェイスにアタッチします。

map mpls

POS SPA、チャネライズド SPA、およびクリアチャネル SPA 用に、すべてのマルチプロトコルラベルスイッチング（MPLS）パケット、または指定された EXP 値または範囲を持つ MPLS パケットを高優先順位または低優先順位に分類するには、入力クラスマップ モードで **mapmpls** コマンドの次の形式を使用します。MPLS 設定を削除するには、ここに記載されているこのコマンドの **no** 形式を使用します。

すべての MPLS EXP 値を高優先順位または低優先順位に分類するためのコマンド
map mpls all queue {**strict-priority|0**}
no map mpls all queue

MPLS EXP 値を高優先順位または低優先順位に分類するためのコマンド
map mpls exp {*exp-valueexp-range*} **queue** {**strict-priority|0**}
no map mpls exp {*exp-valueexp-range*} **queue** {**strict-priority|0**}

構文の説明

allqueue	すべての MPLS パケットの高優先順位または低優先順位の設定を暗黙的に指定します。
strict-priority	すべての MPLS パケットまたは特定の EXP 値を持つ MPLS パケットを高優先順位（絶対優先）として分類します。
0	MPLS パケットを低優先順位として分類します。
exp	MPLS パケット用に、EXP 値または EXP 値の範囲を高優先順位または低優先順位として設定できます。EXP 値の有効範囲は 0 ～ 7 です。
exp-value	優先順位が高い、または低い（0）と設定される特定の EXP 値です。
exp-range	優先順位が高い、または低い（0）と設定される EXP 値の範囲です。EXP 値の有効範囲は 0 ～ 7 です。
queue	キュー全体、EXP 値、または EXP 値の範囲の、高優先順位または低優先順位としての優先順位の分類を有効にします。

コマンド デフォルト

どの MPLS EXP 値を高優先順位にマッピングするかをユーザが設定していない場合、システムは EXP 値が 6 ～ 7 のパケットを高優先順位として扱います。

コマンド モード

入力クラスマップ コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
3.1S	POS SPA、チャネライズド SPA、およびクリアチャネル SPA 用に、すべての MPLS パケット、または EXP 値に基づく MPLS パケットを高優先順位または低優先順位に分類するために、このコマンドが導入されました。

使用上のガイドライン

POS SPA、チャネライズド SPA、またはクリアチャネル SPA 用に、すべての MPLS パケットを高優先順位または低優先順位に分類するには、**mapmplsallqueue** コマンドを使用します。

MPLS パケットを特定の EXP 値で分類するには、**mapmplsexp{exp-value|exp-range}queue{strict-priority|0}** コマンドを使用します。

例

次に、**mapmplsallqueuestrict-priority** コマンドを使用して、すべての MPLS パケットを高優先順位として分類する例を示します。

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map mpls all queue strict-priority
```

次に、EXP 値が 4 の MPLS パケットを高優先順位として分類する例を示します。

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map mpls exp 4 queue strict-priority
```

関連コマンド

Command	Description
plimqosinputclass-map	分類テンプレートをインターフェイスにアタッチします。

match access-group

指定されたアクセス コントロール リスト（ACL）に基づいてクラス マップの一致基準を設定するには、QoS クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **match access-group** コマンドを使用します。ACL 一致基準をクラス マップから削除するには、このコマンドの **no** 形式を使用します。

match access-group {*access-group*|**name** *access-group-name*}
no match {*access-group*|**name** *access-group-name*}

構文の説明

access-group	パケットが同じクラスに属するかどうかを判定するための一致基準として使用される番号付き ACL です。範囲は 1 ～ 2699 です。
name *access-group-name*	パケットが同じクラスに属するかどうかを判定するための一致基準として使用される名前付き ACL を指定します。名前には 40 文字以内の英数字を使用できます。

コマンド デフォルト

一致基準は設定されません。

コマンド モード

QoS クラスマップ コンフィギュレーション（config-cmap）

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

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。
12.0(7)S	このコマンドが、Cisco IOS Release 12.0(7)S に統合されました。
12.0(17)SL	このコマンドが変更されました。このコマンドが拡張され、Cisco 10000 シリーズ ルータでのアクセス リストの照合を含むようになりました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.4(6)T	このコマンドが変更されました。このコマンドが拡張され、ゾーンベース ポリシー ファイアウォールをサポートするようになりました。
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。

リリース	変更箇所
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。
12.2SX	このコマンドが Cisco IOS Release 12.2SX トレインに統合されました。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 Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

match access-group コマンドは、クラス マップで指定されたクラスに属しているかどうかを確認するパケットに対して、その内容が一致基準として使用される番号付き ACL または名前付き ACL を指定します。

アクセス グループに一致するパケットのトラフィック レートが生成されます。ゾーンベース ポリシーファイアウォールでは、設定されたポリシーと一致するのは、セッションを作成した最初のパケットのみです。このフローの後続パケットは、設定されたポリシー内のフィルタと一致しませんが、セッションとは直接一致します。後続パケットに関連する統計情報は、検査アクションの一部として表示されます。

ゾーンベース ポリシー ファイアウォールは、**match access-group**、**match class-map**、および **match protocol** コマンドのみをサポートしています。クラス マップで **match** コマンドを複数指定した場合は、最後に指定したコマンドのみがクラス マップに適用されます。最後の **match** コマンドにより、それ以前に入力された **match** コマンドが上書きされます。

match access-group コマンドは、クラス マップで指定された基準と一致するかどうかを判断するために、その内容のパケットが確認される番号付きアクセス リストを指定します。**access-list** コマンドの **log** キーワードで設定されたアクセス リストは、一致基準を設定するときにはサポートされません。**access-list** コマンドの詳細については、『*Cisco IOS IP Application Services Command Reference*』を参照してください。

このコマンドが Cisco IOS Release 15.0(1)M 以降のリリースで設定されている場合、ファイアウォールはレイヤ 4 ポリシー マップのみを検査します。Cisco IOS Release 15.0(1)M より前のリリースでは、ファイアウォールはレイヤ 4 およびレイヤ 7 ポリシー マップの両方を検査します。

クラスベース重み付け均等化キューイング（CBWFQ）の場合は、ACL、Experimental（EXP）フィールド値、入力インターフェイス、プロトコル、および Quality of Service（QoS）ラベル

を含む一致基準に基づいて、トラフィック クラスを定義できます。クラスの一致基準を満たすパケットは、そのクラスのトラフィックの一部となります。

（注） ゾーンベース ポリシー ファイアウォールでは、このコマンドはCBWFQには適用できません。

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行できるコンフィギュレーション モードにします。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

match access-group コマンドを使用するには、**service-policy type performance-monitor inline** コマンドを設定する必要があります。

Cisco 10000 シリーズ ルータ以外でサポートされるプラットフォーム

match access-group コマンドを使用するには、**class-map** コマンドを設定して、一致基準を確立するクラスの名前を指定する必要があります。クラスを指定したら、次のいずれかのコマンドを使用してそのクラスの一致基準を設定できます。

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

Cisco 10000 シリーズ ルータ

match access-group コマンドを使用するには、最初に **class-map** コマンドを入力し、一致基準を確立するクラスの名前を指定する必要があります。

（注） **match access-group** コマンドは、クラス マップで指定された基準と一致するかどうかを判断するために、その内容のパケットが確認される番号付きアクセス リストを指定します。**access-list** コマンドの **log** キーワードで設定されたアクセス リストは、一致基準を設定するときにはサポートされません。

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ

Cisco ASR 1000 シリーズ ルータは、クラス マップごとに 16 を超えるマッチング ステートメントはサポートしていません。16 を超えるマッチング ステートメントを持つインターフェイスは、サービス ポリシーを拒否します。

例

次に、acl144 という名前のクラス マップを指定し、144 という番号が付いた ACL をそのクラスの一致基準として使用するように設定する例を示します。

```
Device(config)# class-map acl144
Device(config-cmap)# match access-group 144
```

次に、c1 という名前のクラス マップを定義し、144 という番号が付いた ACL をそのクラスの一致基準として使用するように設定する例を示します。

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match access-group 144
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードで Performance Monitor 用のサービス ポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過するパケットが ACL144 と一致する必要があることを指定します。

```
Device(config)# interface ethernet 0/0
Device(config-if)# service-policy type performance-monitor inline input
Device(config-if-spolicy-inline)# match access-group name ACL144
Device(config-if-spolicy-inline)# exit
```

関連コマンド

コマンド	説明
access-list (IP extended)	拡張 IP アクセス リストを定義します。
access-list (IP standard)	標準 IP アクセス リストを定義します。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
match access-group	指定した ACL をベースにクラス マップに対して一致基準を設定します。
match class-map	トラフィック クラスを分類ポリシーとして使用します。
match input-interface	指定された入力インターフェイスを一致基準として使用するクラス マップを設定します。
match mpls experimental	指定した EXP フィールド値を一致基準として使用するクラス マップを設定します。
match protocol	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。
service-policy type performance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。

match application（クラスマップ）

コントロールプレーンの分類の一致基準としてメタデータ アプリケーションを使用するには、QoS クラスマップ コンフィギュレーション モードで **match application** コマンドを使用します。以前に設定されたメタデータ アプリケーションを削除して、コントロール プレーンの分類の一致基準として使用されないようにするには、このコマンドの **no** 形式を使用します。

match application {**application-group** *application-group-name*| **attribute** {**category** {**business-and-productivity-tools**|**voice-and-video**}|**device-class** *device-class-type*|**media-type** *media-type*|**sub-category** {**remote-access-terminal**|**voice-video-chat-collaboration**}}|*application-name*[{**source** {**msp** |**nbar** |**rsvp**}|**vendor** *vendor-name***version** *version-number*}]}

no match application {**application-group** *application-group-name*| **attribute** {**category** {**business-and-productivity-tools**|**voice-and-video**}|**device-class** *device-class-type*|**media-type** *media-type*|**sub-category** {**remote-access-terminal**|**voice-video-chat-collaboration**}}|*application-name*[{**source** {**msp** |**nbar** |**rsvp**}|**vendor** *vendor-name***version** *version-number*}]}

構文の説明

application-group *application-group-name*	コントロール プレーンの分類エンジンが照合する必要があるアプリケーション グループを指定します。**telepresence-group**、**vmware-group**、および **webex-group** のいずれかの値を使用して、関連するアプリケーション グループを指定します。
attribute	照合する関連属性を指定します。
category	コントロール プレーンの分類エンジンが照合する必要があるカテゴリ タイプを指定します。
business-and-productivity-tools	ビジネス ツールと生産性ツールを指定します。
voice-and-video	音声とビデオのカテゴリを指定します。
device-class *device-class-type*	照合するデバイス クラスを指定します。**desktop-conferencing**、**desktop-virtualisation**、**physical-phone**、**room-conferencing**、**software-phone**、および **surveillance** のいずれかの値を使用して、関連するデバイス クラスを指定します。
media-type *media-type*	照合するメディアのタイプを指定します。**audio**、**audio-videocontrol**、**data**、および **video** のいずれかの値を使用して、関連するメディア タイプを指定します。
sub-category	照合するサブカテゴリを指定します。
remote-access-terminal	リモート アクセス端末のサブカテゴリを指定します。
voice-video-chat-collaboration	音声、ビデオ、およびコラボレーションのサブカテゴリを指定します。

application-name	コントロール プレーンの分類エンジンが照合する必要があるアプリケーションの名前です。**cisco-phone**、**citrix**、**h323**、**jabber**、**rtp**、**rtsp**、**sip**、**telepresence-control**、**telepresence-data**、**telepresence-media**、**vmware-view**、**webex-data**、**webex-meeting**、**webex-streaming**、**webex-video**、**webex-voice**、および **wyze-zero-client** のアプリケーションがサポートされています。
source	（任意）アプリケーションのソースを指定します。
msp	アプリケーション ソースを Media-Proxy Service（MSP）として指定します。
nbar	アプリケーション ソースを Network Based Application Recognition（NBAR）として指定します。
rsvp	アプリケーション ソースをリソース予約プロトコル（RSVP）として指定します。
vendor *vendor-name*	（任意）ベンダーの名前を指定します。それぞれのアプリケーション名のサポートされているベンダーのリストを取得するには、**vendor** キーワードの後に ? を入力します。
version *version-number*	（任意）バージョン番号を指定します。

コマンド デフォルト

メタデータベースのコントロール プレーンの分類は無効になっています。

コマンド モード

QoS クラスマップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
15.2(1)T	このコマンドが導入されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。
15.3(1)T	このコマンドが変更されました。**source**、**msp**、**nbar**、および **rsvp** キーワードが追加されました。

使用上のガイドライン

Quality of Service（QoS）ポリシー用に、プラットフォーム単位、ライン カード単位でのメタデータベースのコントロールプレーンの分類を有効にするには、次の重要な手順が必要です。

- メタデータベースのフィルタを使用してクラス マップを作成します。
- クラスを使用するポリシー マップを作成します。
- ターゲットにポリシー マップをアタッチします。

match application コマンドを使用して、クラスマップに適用できるメタデータベースのフィルタを有効にできます。必要なアプリケーション名を指定すると、そのアプリケーション名と一致するフローにのみ、それぞれのポリシーを適用できるようになります。分類エンジンが最初の照合を行います。

match application コマンドをその他の **match** コマンドと組み合わせて使用して、クラスの一致基準を指定することができます。たとえば、**match application** コマンドと一緒に、フローの分類基準として **match dscp** コマンドを使用することができます。

show metadata flow classification table コマンドを使用して、メタデータベースの分類の情報をチェックすることができます。

debug metadata flow all コマンドを使用して、特定の分類が正常に作成されたかどうかをチェックすることができます。

（注） CSCub24690 では、**webex-data**、**webex-streaming**、**webex-video**、および **webex-voice** キーワードは **match application** *application-name* コマンドでサポートされていません。

例

次に、クラス マップ c1 を設定し、一致基準としてメタデータ アプリケーション webex-meeting を指定して、コントロールプレーンの分類を実現する例を示します。メタデータ アプリケーション webex-meeting と一致するフローのみが、適切なアクションのために考慮されます。

```
Device(config)# class-map c1
Device(config-cmap)# match application webex-meeting
```

この例の完全性のために、次の設定が提供されています。

以前に設定されたクラス c1 を使用するポリシー マップ p1 が作成されます。この例の要件は、クラス c1 に定義された基準に一致するすべてのフローに、1 Mbps の保証帯域幅を提供することです。

```
Device(config)# policy-map p1
Device(config-pmap)# class c1
Device(config-pmap-c)# priority 1
```

次に、ターゲット インターフェイスにポリシーをアタッチする設定例を示します。

```
Device(config)# interface gigabitethernet 0/0
Device(config-if)# service-policy output p1
```

関連コマンド

コマンド	説明
class (policy-map)	ポリシーを作成または変更するクラスの名前を指定します。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
debug metadata	メタデータ フローのデバッグを有効にします。

コマンド	説明
metadata application-params	メタデータ アプリケーション エントリ コンフィギュレーション モードにして、新しいメタデータ アプリケーション パラメータを作成します。
policy-map	ポリシーマップ コンフィギュレーション モードを開始し、サービス ポリシーを指定するため 1 つ以上のインターフェイスに適用できるポリシー マップを作成または修正します。
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与えます。
service-policy	入力インターフェイス、VC、出力インターフェイス、またはインターフェイスや VC のサービス ポリシーとして使用される VC にポリシー マップを適用します。
show metadata flow	メタデータ フロー情報を表示します。

match any

すべてのパケットの成功する一致基準とするクラスマップの一致基準を設定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchany** コマンドを使用します。成功する一致基準としてのすべての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 any
no match any

構文の説明

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

一致基準が指定されていません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.0(5)T	このコマンドが Cisco IOS Release 12.0(5)T に統合されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
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 Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーション モードにします。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、s**ervice-policytypeperformance-monitorinline** コマンドを入力する必要があります。

例

次のコンフィギュレーションでは、イーサネット インターフェイス 1/1 を通過するすべてのパケットが、ポリシーマップ クラス コンフィギュレーション モードで指定されたパラメータに基づいてポリシー処理されます。

```
Router(config)# class-map matchany
Router(config-cmap)# match any
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
Router(config)# interface ethernet1/1
Router(config-if)# service-policy output policy1
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor用のサービス ポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過するすべてのパケットが、**fm-2** という名前のフロー モニタ設定で指定されたパラメータに基づいて照合され、モニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match any
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。
matchinput-interface	指定された入力インターフェイスを一致基準として使用するクラス マップを設定します。
matchprotocol	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。

match atm-clp

ATM セル損失率優先度（CLP）に基づいたパケット照合を有効にするには、クラスマップ コンフィギュレーション モードで **matchatm-clp** コマンドを使用します。ATM CLP に基づいたパケット照合を無効にするには、このコマンドの **no** 形式を使用します。

match atm-clp
no match atm-clp

構文の説明

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

パケットは、ATM CLP に基づいては照合されません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
12.0(28)S	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
12.2(33)SRC	Cisco 7600 シリーズ ルータのサポートが追加されました。
12.4(15)T2	このコマンドが Cisco IOS Release 12.4(15)T2 に統合されました。
12.2(33)SB	Cisco 7300 シリーズ ルータのサポートが追加されました。
Cisco IOS XE リリース 2.3	このコマンドが、Cisco IOS XE Release 2.3 に統合されました。

使用上のガイドライン

このコマンドは、ATM メイン インターフェイス、ATM サブインターフェイス、または ATM 相手先固定接続（PVC）にアタッチされているポリシーマップでサポートされています。ただし、これらのタイプの ATM インターフェイスにアタッチされたポリシーマップ（**matchatm-clp** コマンドを含む）になれるのは、入力ポリシー マップだけです。

このコマンドは、PA-A3 アダプタでしかサポートされています。

例

次の例では、**class-map** コマンドを使用して「class-c1」という名前のクラスが作成され、そのクラス内で **matchatm-clp** コマンドが設定されます。したがって、パケットは ATM CLP に基づいて照合され、このクラスに置かれます。

```
Router> enable
Router# configure terminal
Router(config)# class-map class-c1
```

```
Router(config-cmap)# match atm-clp
Router(config-cmap)# end
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
showatmpvc	すべての ATM PVC およびトラフィック情報を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

match atm oam

ATMインターフェイスで制御トラフィック分類を有効にするには、クラスマップ コンフィギュレーション モードで **matchatmoam** コマンドを使用します。制御トラフィック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。

match atm oam
no match atm oam

構文の説明

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

デフォルトの動作または値はありません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(30)S	このコマンドが導入されました。

使用上のガイドライン

ATM インターフェイスまたは ATM 相手先固定接続（PVC）にアタッチされたポリシー マップに、このコマンドを使用します。**matchatmoam** コマンドを含む、ATM インターフェイスまたは ATM PVC にアタッチされたポリシー マップには、入力ポリシー マップのみを使用できます。

例

次に、クラスマップ内の一致基準として設定される制御トラフィック分類の例を示します。このクラス マップを含むポリシー マップが ATM インターフェイスに適用されます。

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map class-oam

Router(config-cmap)# match atm oam

Router(config-cmap)# exit
```

関連コマンド

コマンド	説明
showclass-map	すべてのクラス マップおよびその一致基準を表示します。
showpolicy-map	すべてのポリシー マップを表示します。

コマンド	説明
showpolicy-mapinterface	指定したATMインターフェイス上か、インターフェイス上の特定のPVCに対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

match atm-vci

ATM 仮想回線インターフェイス（VCI）に基づいたパケット照合を有効にするには、クラス マップ コンフィギュレーション モードで **matchatm-vci** コマンドを使用します。ATM VCI に基づいたパケット照合を無効にするには、このコマンドの **no** 形式を使用します。

match atm-vci *vc-id* [-*vc-id*]
no match atm-vci

構文の説明

vc-id	2 台のプロバイダー エッジ ルータ間の仮想回線に割り当てられる VC 番号です。1 つの VC または VC の範囲を指定できます。
-*vc-id*	（任意）最初の VC 番号からハイフンで区切られた 2 番目の VC 番号です。2 つの VC 番号を指定する場合、範囲は 32 ～ 65535 です。

コマンド デフォルト

一致基準は設定されません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 2.3	このコマンドが導入されました。
12.2(33)SRE	このコマンドが変更されました。このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。

使用上のガイドライン

matchatm-vci コマンドをクラス マップ コンフィギュレーション モードで設定する場合、このクラス マップは、ATM 相手先固定パス（PVP）だけにアタッチできるポリシー マップに追加できます。

（注） Cisco 7600 シリーズ ルータでは、**matchatm-vci** コマンドは、ATM VP の入力方向だけでサポートされます。

matchnot コマンドを使用すると、コマンドで指定した VC 以外の VC と照合できます。

例

次の例では、VC ID 50 での照合を有効にします。

```
Router(config)# class-map map1
Router(config-cmap)# match atm-vci 50
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラスマップを作成します。
matchnot	成功しない一致基準として使用する単一の一致基準値を指定します。

match class-map

トラフィック クラスを分類ポリシーとして使用するには、クラス マップまたはポリシー インライン コンフィギュレーション モードで **match class-map** コマンドを使用します。一致基準としての特定のトラフィック クラスを削除するには、このコマンドの **no** 形式を使用します。

match class-map *class-map-nam e*
no match class-map *class-map-name*

構文の説明

class-map-name	一致基準として使用するトラフィック クラスの名前。

コマンド デフォルト

一致基準が指定されていません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.4(6)T	このコマンドが拡張され、ゾーンベース ポリシー ファイアウォールをサポートするようになりました。
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。
12.2(31)SB	このコマンドは、Cisco 10000 シリーズに実装されました。
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。
Cisco IOS XE Release 3.2S	このコマンドが、Cisco IOS XE Release 3.2S に統合されました。

使用上のガイドライン

1 つのトラフィック クラスに match-any 特性と match-all 特性の両方を使用する唯一の方法は、**match class-map** コマンドを使用する方法です。match-any 特性と match-all 特性を結合して 1 つのクラスにするには、次のいずれかを実行します。

- match-any 指示を使用してトラフィック クラスを作成し、一致基準として match-all 指示を使用して設定したクラスを使用します（**match class-map** コマンドを使用）。

- match-all 指示を使用してトラフィック クラスを作成し、一致基準として match-any 指示を使用して設定したクラスを使用します（**match class-map** コマンドを使用）。

また、**match class-map** コマンドを使用してトラフィック クラスを別のクラス内にネストすることもできます。これにより、以前に設定したトラフィック クラスにほとんどの情報が存在している場合に、ユーザが新しいトラフィック クラスを再作成するオーバーヘッドが削減されます。

パケットがクラス マップに一致すると、それらのパケットのトラフィック レートが生成されます。ゾーンベース ファイアウォール ポリシーでは、ポリシーと一致するのは、セッションを作成した最初のパケットのみです。このフローの後続パケットは、設定されたポリシー内のフィルタと一致しませんが、セッションとは直接一致します。後続パケットに関連する統計情報は、検査アクションの一部として表示されます。

例

Non-Zone-BasedPolicyFirewallExamples

次の例で、トラフィック クラス class1 の特性は、トラフィック クラス class2 の特性とほぼ同じですが、トラフィック クラス class1 では、一致基準として宛先アドレスが追加されています。トラフィック クラス class1 をゼロから設定する代わりに、**match class-map class2** コマンドを使用できます。このコマンドを使用すると、トラフィック クラス class2 のすべての特性をトラフィック クラス class1 に取り込み、トラフィック クラスを再設定することなく、新しい宛先アドレスの一致条件を追加できます。

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# exit
```

次に、2 つのトラフィック クラスの特性を組み合わせる例を示します。1 つは match-any 特性を使用し、1 つは match-all 特性を使用しています。これを、**match class-map** コマンドで 1 つのトラフィック クラスとして設定します。class4 というトラフィック クラスの場合、パケットが class4 トラフィック クラスのメンバーとして見なされるためには、3 つの一致基準（IP プロトコルかつ QoS グループ 4、宛先 MAC アドレス 1.1.1、またはアクセス グループ 2）のいずれかを満たしている必要があります。一致基準である IP プロトコルかつ QoS グループ 4 は、トラフィック クラス class3 の定義で必要であり、**match class-map class3** コマンドによって、トラフィック クラス class4 の定義に可能な一致として含まれています。

この例では、トラフィック クラス class4 だけがサービス ポリシー policy1 に使用されています。

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
```

```
Router(config-cmap)# exit
Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラスマップを作成します。

match cos

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するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchcos** コマンドを使用します。一致基準としての特定のレイヤ 2 CoS/ISL マーキングを削除するには、このコマンドの **no** 形式を使用します。

match cos cos-value [**cos-value** [**cos-value** [**cos-value**]]]
no match cos cos-value [**cos-value** [**cos-value** [**cos-value**]]]

構文の説明

Cisco 10000 シリーズ ルータ以外でサポートされるプラットフォーム	
cos-value	具体的な IEEE 802.1Q/ISL CoS 値。*cos-value* は 0 ～ 7 です。最大で 4 つのスペースで区切られた CoS 値を 1 つの **matchcos** ステートメントで指定できます。
Cisco 10000 シリーズ ルータ	特定のパケット CoS ビット値です。パケット CoS ビット値が、指定された CoS 値と一致する必要があることを指定します。*cos-value* は 0 ～ 7 です。最大で 4 つのスペースで区切られた CoS 値を 1 つの **matchcos** ステートメントで指定できます。
cos-value	

コマンド デフォルト

パケットのレイヤ 2 CoS/ISL マーキングに基づいた照合は行われません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.1(5)T	このコマンドが導入されました。
12.0(25)S	このコマンドが、Cisco IOS Release 12.0(25)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。

リリース	変更箇所
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。
12.2(33)SRC	このコマンドが Cisco IOS Release 12.2(33)SRC に統合され、Cisco 7600 シリーズ ルータのサポートが追加されました。
12.4(15)T2	このコマンドが Cisco IOS Release 12.4(15)T2 に統合されました。
12.2(33)SB	このコマンドが Cisco IOS Release 12.2(33)SB に統合され、Cisco 7300 シリーズ ルータのサポートが追加されました。
15.1(3)T	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。
12.2(33)SCF	このコマンドが、Cisco IOS リリース 12.2(33)SCF に統合されました。
3.2SE	このコマンドが、Cisco IOS XE リリース 3.2SE に統合されました。
15.1(2)SNG	このコマンドが、Cisco ASR 901 シリーズ アグリゲーション サービス ルータに統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーション モードにします。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、**service-policytypeperformance-monitorinline** コマンドを入力する必要があります。

例

次に、1、2、および3のCoS値を、cosという名前の分類ポリシーを含むインターフェイスの成功する一致基準とする例を示します。

```
Router(config)# class-map cos
Router(config-cmap)# match cos 1 2 3
```

次の例では、CoS値に基づいてトラフィックを分類するために、voiceおよびvideo-n-dataという名前のクラスを作成しています。その後、cos-based-treatmentポリシーマップ内で該当パケットへの QoS 処理を指定しています（この例では、QoS 処理は priority が 64、bandwidth が 512）。この例で設定したサービス ポリシーは、ファスト イーサネット インターフェイス 0/0.1 から出て行くすべてのパケットにアタッチされます。サービス ポリシーは、サービス ポリシーをサポートする任意のインターフェイスにアタッチできます。

```
Router(config)# class-map voice
Router(config-cmap)# match cos 7
Router(config)# class-map video-n-data
Router(config-cmap)# match cos 5
Router(config)# policy-map cos-based-treatment
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 64
Router(config-pmap-c)# exit
Router(config-pmap)# class video-n-data
Router(config-pmap-c)# bandwidth 512
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet0/0.1
Router(config-if)# service-policy output cos-based-treatment
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor 用のサービス ポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過する、CoS 値 2 の基準に一致するパケットが、**fm-2** という名前のフロー モニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match cos 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Cisco IOS Release 12.2(33)SCF で CoS 値により 802.1p ドメイン内のトラフィック クラスを照合するための match cos コマンドの例

次に、パケット CoS 値で 802.1p ドメインのトラフィック クラスを照合する例を示します。

```
Router> enable
Router# config terminal
Router(config)# class-map cos7
Router(config-cmap)# match cos 2
Router(config-cmap)# exit
```

関連コマンド

Command	Description
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。

Command	Description
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシーマップを対応付けます。
setcos	発信パケットのレイヤ 2 CoS 値を設定します。
showclass-map	すべてのクラス マップおよびその一致基準を表示します。

match cos inner

レイヤ 2 サービス クラス（CoS）マーキングで QinQ パケットの内部 cos 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 **matchcosinner** コマンドを使用します。特定のレイヤ 2 CoS 内部タグ マーキングを削除するには、このコマンドの **no** 形式を使用します。

match cos cos-value
no match cos cos-value

構文の説明

cos-value	具体的な IEEE 802.1Q/ISL CoS 値。*cos-value* は 0 ～ 7 です。最大で 4 つの CoS 値を 1 つの **matchcos** ステートメントで指定できます。

コマンド デフォルト

一致基準が指定されていません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(18)SXE	このコマンドが導入されました。
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。

例

次に、1、2、および 3 の内部 CoS 値を、cos という分類ポリシーを含むインターフェイスの成功する一致基準とする例を示します。

```
Router(config)# class-map cos

Router(config-cmap)# match cos inner 1 2 3
```

関連コマンド

Command	Description
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
setcos	発信パケットのレイヤ 2 CoS 値を設定します。
showclass-map	すべてのクラス マップおよびその一致基準を表示します。

match destination-address mac

一致基準として宛先 MAC アドレスを使用するには、クラスマップ コンフィギュレーション モードまたはポリシーインライン コンフィギュレーションモードで**matchdestination-addressmac** コマンドを使用します。以前に一致基準として指定していた宛先 MAC アドレスを削除するには、このコマンドの **no** 形式を使用します。

match destination-address mac *address*
no match destination-address mac *address*

構文の説明

address	一致基準として使用される宛先MACアドレスです。

コマンド デフォルト

宛先 MAC アドレスは指定されません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズに実装されました。
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 Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーションモードにします。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、s**ervice-policytypeperformance-monitorinline** コマンドを入力する必要があります。

例

次の例では、macaddress という名前のクラス マップを指定し、このクラスの一致基準として使用される宛先 MAC アドレスを指定します。

```
Router(config)# class-map macaddress
Router(config-cmap)# match destination-address mac 00:00:00:00:00:00
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor用のサービス ポリシーを設定する例を示します。このポリシーは、イーサネットインターフェイス0/0を通過する、指定された宛先MACアドレスに一致するパケットが、**fm-2** という名前のフローモニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
destination-address mac 00:00:00:00:00:00
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。

match discard-class

一致基準として廃棄クラスを指定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchdiscard-class** コマンドを使用します。以前に一致基準として指定していた廃棄クラスを削除するには、このコマンドの **no** 形式を使用します。

match discard-class *class-number*
no match discard-class *class-number*

構文の説明

class-number	照合される廃棄クラスの番号です。有効な値は0～7です。

コマンド デフォルト

パケットは期待どおりに分類されません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
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 Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーション モードにします。

discard-class 値に数学的な意味はありません。たとえば、discard-class 値 2 が 1 より大きいわけではありません。この値は単に、discard-class 2 でマークされたパケットは、discard-class 1 でマークされたパケットとは異なる扱いをする必要があることを示しています。

指定された discard-class 値と一致するパケットは、他の discard-class 値でマークされたパケットとは異なる扱いを受けます。discard-class は一致基準のみで、ドロップするトラフィックに対して Per-Hop Behavior（PHB）を定義する際に使用されます。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、s**ervice-policytypeperformance-monitorinline** コマンドを入力する必要があります。

例

次に、廃棄クラス 2 のパケットが照合される例を示します。

```
Router(config)# class-map d-class-2
Router(config-cmap)# match discard-class 2
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor 用のサービス ポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過する、discard-class 2 によって指定された基準と一致するパケットが、**fm-2** という名前のフロー モニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
discard-class 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。
setdiscard-class	discard-class 値でパケットをマークします。

match dscp

Differentiated Services Code Point（DSCP; DiffServ コードポイント）、相対的優先転送（AF）、および証明書サーバ（CS）の値の1つまたは複数を一致基準として指定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchdscp** コマンドを使用します。クラス マップから特定の 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。

match [ip] dscp *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]
no match [ip] dscp *dscp-value*

構文の説明

ip	（任意）IPv4パケットのみを照合するように指定します。使用しない場合、IPv4とIPv6パケットの両方が照合されます。 （注） Cisco 10000 シリーズ ルータの場合は、**ip** キーワードが必要です。
dscp-value	DSCP 値の識別に使用する DSCP 値。有効な値については、「使用上のガイドライン」セクションを参照してください。

コマンド デフォルト

一致基準は設定されません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。このコマンドで **matchipdscp** コマンドが置き換えられます。
12.0(28)S	このコマンドが IPv6 におけるサポート用に Cisco IOS Release 12.0(28)S に統合されました。
12.0(17)SL	このコマンドが Cisco IOS Release 12.0(17)SL に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ ルータに実装されました。
15.1(3)T	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。

リリース	変更箇所
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーションモードにします。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、**service-policytypeperformance-monitorinline** コマンドを入力する必要があります。

DSCP 値

1 つまたは複数の Diffserv コード ポイント（DSCP）値を入力する必要があります。コマンドには、次の任意の組み合わせを含めることができます。

- DiffServ コード ポイント値を表す数字（0 ～ 63）
- 特定の AF DSCP を識別する AF 番号（af11 など）
- 特定の CS DSCP を識別する CS 番号（cs1 など）
- **default**：デフォルト DSCP を持つパケットに一致します。
- **ef**：EF DSCP を持つパケットに一致します。

たとえば、0、1、2、3、4、5、6、または 7 の DCSP 値が必要な場合（指定したすべての IP DSCP 値ではなく、1 つの IP DSCP 値だけが正常な一致基準であることに注意）、**matchdscp01234567** コマンドを入力します。

このコマンドはクラス マップで使用され、パケット上の特定の DSCP 値マーキングを識別します。このコンテキストでは、*dscp-value* 引数はマーキングとしてだけ使用され、数学的な意味はありません。たとえば、*dscp-value* の 2 という値は、1 より大きいわけではありません。値は単に 2 という *dscp-value* でマーキングされているパケットが、1 という *dscp-value* でマーキングされているパケットとは異なるということを示しているに過ぎません。これらのマーキングされたパケットの処理は、ユーザが、ポリシー マップ クラス コンフィギュレーション モードでの Quality of Service（QoS）ポリシーの設定を通じて定義します。

DSCP 値での一致パケット

DSCP 値を IPv6 パケットだけに照合させるには、**matchprotocolipv6** コマンドも使用する必要があります。このコマンドを使用しないと、DSCP での照合はデフォルトで IPv4 パケットと IPv6 パケットの両方に対して行われます。

DSCP 値を IPv4 パケットだけに照合させるには、**ip** キーワードを使用します。**ip** キーワードを指定しないと、照合は IPv4 パケットと IPv6 パケットの両方に行われます。または、**matchprotocolip** コマンドを **matchdscp** とともに使用して、IPv4 パケットのみを分類することができます。

DSCP ビットをセットした後は、その他の QoS 機能をビット設定で動作させることができます。

ネットワークは、マーキングされているトラフィックにプライオリティを与える（または何らかのタイプの優先処理を行う）ことができます。一般に、ネットワークのエッジ（または管理ドメイン）で優先順位の値を設定します。これにより、データが優先順位に従ってキューに格納されます。重み付け均等化キューイング（WFQ）で、輻輳ポイントでの優先順位の高いトラフィックの処理を高速化できます。重み付けランダム早期検出（WRED）で、輻輳時に、優先順位の高いトラフィックの損失率をその他のトラフィックより確実に低くすることができます。

Cisco 10000 シリーズ ルータ

Cisco 10000 シリーズ ルータは、IPv4 パケットの DSCP 照合のみをサポートしています。一致基準として使用する DSCP 値を指定する場合は、ip キーワードを含める必要があります。

同じパケットをマーク付けする場合に、set ip dscp コマンドを set ip precedence コマンドと組み合わせて使用することはできません。DSCP 値と precedence 値は、相互に排他的です。パケットにはどちらか一方の値を設定でき、両方を設定することはできません。

例

次に、複数の一致基準を設定する例を示します。この場合は、2 つの IP DSCP 値と 1 つの AF 値です。

```
Router(config)# class-map map1
Router(config-cmap)# match dscp 1 2 af11
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor用のサービスポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過する、DSCP 値 2 によって指定された基準と一致するパケットが、fm-2という名前のフローモニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match dscp 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# end
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
matchprotocolip	パケットの DSCP 値照合を行います。
matchprotocolipv6	IPv6 パケットの DSCP 値と照合します。

コマンド	説明
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシーマップを対応付けます。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。
setdscp	トラフィック クラス内のパケットの DSCP 値をマーク付けします。
showclass-map	すべてのクラス マップおよびその一致基準を表示します。

match field

（注） Cisco IOS Release 15.2(4)M では、Cisco IOS ソフトウェアで **match field** コマンドを使用できません。

プロトコルヘッダー記述ファイル（PHDF）で定義されたフィールドに基づいてクラスマップの一致基準を設定するには、クラスマップ コンフィギュレーション モードで **match field** コマンドを使用します。指定した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 field *protocol protocol-field* {**eq [mask]**|**neq [mask]**|**gt**|**lt**|**range** *range*|**regex** *string*} *value* [**next** *next-protocol*]
no match field *protocol protocol-field* {**eq [mask]**|**neq [mask]**|**gt**|**lt**|**range** *range*|**regex** *string*} *value* [**next** *next-protocol*]

構文の説明

プロトコル	PHDF がルータにロードされているプロトコルの名前です。
protocol field	一致基準は、ロードされたプロトコル内で指定されているフィールドに基づきます。
eq	パケットが指定された値またはマスクと等しい場合に、一致基準が満たされます。
neq	パケットが指定された値またはマスクと等しくない場合に、一致基準が満たされます。
mask *mask*	（任意）**eq** または **neq** キーワードが発行された場合に使用できます。
gt	パケットが指定された値を超えない場合に、一致基準が満たされます。
lt	パケットが指定された値未満の場合に、一致基準が満たされます。
range *range*	一致基準は、下限および上限のプロトコルのフィールド範囲に基づきます。
regex *string*	一致基準は、照合される文字列に基づきます。
value	パケットが一致する必要がある値です。
next *next-protocol*	一致基準として使用される、プロトコルのスタック内の次のプロトコルを指定します。

コマンド デフォルト

一致基準は設定されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。
12.2(18)ZY	このコマンドが、Catalyst 6500 シリーズの Programmable Intelligent Services Accelerator（PISA）が搭載されているスイッチの Cisco IOS Release 12.2(18)ZY に統合されました。
Cisco IOS XE 2.2	このコマンドが、Cisco IOS XE Release 2.2 に統合されました。
15.2(4)M	このコマンドは Cisco IOS ソフトウェアから削除されました。

使用上のガイドライン

match-field コマンドを発行する前に、**load protocol** コマンドによりルータに PHDF をロードする必要があります。その後、最初に **class-map** コマンドを入力し、一致基準を確立するクラスの名前を指定する必要があります。

一致基準は、開始点、オフセット、サイズ、照合する値、およびマスクにより定義されます。任意のプロトコル フィールドを持つパターンで一致を定義できます。

例

次に、ブラスタ パケット用に FPM を設定する方法の例を示します。このクラス マップには、TCP ポート 135、4444 または UDP ポート 69、および IP ヘッダーの開始から 3 バイトでのパターン 0x0030 という一致基準が含まれています。

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
load protocol	PHDF をルータにロードします。
match start	データグラム ヘッダー（レイヤ 2）またはネットワーク ヘッダー（レイヤ 3）に基づいてクラス マップの一致条件を設定します。

match flow pdp

クラスマップ内の一致基準としてパケットデータプロトコル（PDP）フローを指定するには、クラスマップ コンフィギュレーション モードで **matchflowpdp** コマンドを使用します。一致基準としての PDP フローを削除するには、このコマンドの **no** 形式を使用します。

match flow pdp
no match flow pdp

構文の説明

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

PDP フローは一致基準として指定されません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
12.3(8)XU	このコマンドが導入されました。
12.3(11)YJ	このコマンドが、Cisco IOS Release 12.3(11)YJ に組み込まれました。
12.3(14)YQ	このコマンドが、Cisco IOS Release 12.3(14)YQ に組み込まれました。
12.3(14)YU	このコマンドが、Cisco IOS Release 12.3(14)YU に組み込まれました。
12.4(2)XB	このコマンドが、Cisco IOS Release 12.4(2)XB に組み込まれました。
12.4(9)T	このコマンドが Cisco IOS Release 12.4(9)T に統合されました。

使用上のガイドライン

matchflowpdp コマンドにより、PDP フローに基づいてトラフィックを照合および分類できます。

matchflowpdp コマンドは、Cisco IOS Release 12.4(9)T で使用可能な Flow-Based QoS for GGSN 機能に含まれています。Flow-Based QoS for GGSN 機能は、Gateway General Packet Radio Service（GPRS）Support Node（GGSN）専用に設計されています。

PDP ごとのポリシング

Flow-Based QoS for GGSN 機能には、PDP ごとのポリシング（セッションベースのポリシング）が含まれています。

matchflowpdp コマンドにより（**class-map** コマンド、**policy-map** コマンド、**policeratepdp** コマンド、および **service-policy** コマンドと組み合わせて使用した場合）、GGSN のダウンリンクトラフィックに、PDP ごとのポリシング（セッションベースのポリシング）を設定できます。

PDP ごとのポリシングに関連する次の点に注意してください。

- **class-map** コマンドを使用して PDP フロー分類のクラスマップを定義するときは、**match-any** キーワードを使用しないでください。
- PDP ごとのポリシング機能を使用するには、Universal Mobile Telecommunications System（UMTS）Quality of Service（QoS）を設定する必要があります。UMTS QoS の設定の詳細については、『Cisco GGSN Release 6.0 Configuration Guide , Cisco IOS Release 12.4(2)XB』の「Configuring QoS on the GGSN」セクションを参照してください。
- PDP ごとのポリシングを設定するために作成されるポリシー マップには、**matchflowpdp** コマンドのみが指定されている複数のクラスを含めることはできません。言い換えると、ポリシーマップに複数のクラスがある場合には、少なくとも 1 つのクラスで、**matchflowpdp** コマンドを別のマッチング ステートメント（**matchprecedence** など）と組み合わせて使用する必要があります。

詳細情報

GGSN の詳細と、Flow-Based QoS for GGSN 機能の設定手順については、『Cisco GGSN Release 6.0 Configuration Guide , Cisco IOS Release 12.4(2)XB』を参照してください。

（注） Flow-Based QoS for GGSN 機能を設定するには、「Configuring Per-PDP Policing」セクションの手順に従います。

GGSN 固有のコマンドの詳細については、『Cisco GGSN Release 6.0 Command Reference , Cisco IOS Release 12.4(2)XB』を参照してください。

例

次に、PDP フローを、「class-pdp」という名前のクラス マップ内の一致基準として指定する例を示します。

```
class-map class-pdp
 match flow pdp
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
matchprecedence	IP precedence 値を一致基準として識別します。
policeratepdp	ポリシング レートを使用した PDP トラフィック ポリシングを設定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
service-policy	ポリシー マップをインターフェイスに付加します。

match fr-dlci

クラスマップでフレーム リレーデータリンク接続識別子（DLCI）番号を一致基準として指定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchfr-dlci** コマンドを使用します。以前に一致基準として指定していた DLCI 番号を削除するには、このコマンドの **no** 形式を使用します。

match fr-dlci *dlci-number*
no match fr-dlci *dlci-number*

構文の説明

dlci-number	パケットに関連付けられた DLCI の番号です。

コマンド デフォルト

DLCI 番号は指定されません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
15.1(3)T	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーション モードにします。

この一致基準は、フレーム リレー ネットワークのメイン インターフェイスとポイントツーマルチポイント サブインターフェイスで使用でき、階層型ポリシー マップでも使用できます。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、s**ervice-policytypeperformance-monitorinline** コマンドを入力する必要があります。

例

次の例では、「class1」という名前のクラスマップが作成され、フレーム リレー DLCI 番号 500 が一致基準として指定されています。この基準と一致するパケットが class1 に配置されます。

```
Router(config)# class-map class1
Router(config-cmap)# match fr-dlci 500
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor用のサービスポリシーを設定する例を示します。このポリシーは、イーサネットインターフェイス0/0を通過する、フレームリレーDLCI番号500と一致するパケットが、**fm-2**という名前のフローモニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
fr-dlci 500
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。
showclass-map	すべてのクラス マップおよびその一致基準を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定のPVCに対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

match input vlan

特定の仮想ローカル エリア ネットワーク（VLAN）ID を持つ着信パケットを照合するようにクラスマップを設定するには、クラスマップ コンフィギュレーション モードで**matchinputvlan** コマンドを使用します。VLAN ID の照合を削除するには、このコマンドの **no** 形式を使用します。

match input vlan *input-vlan-list*
no match input vlan *input-vlan-list*

構文の説明

input-vlan-list	照合する 1 つ以上の VLAN ID です。VLAN ID の有効範囲は 1 ～ 4094 で、VLAN ID のリストには次のいずれかまたはすべてを含めることができます。 • スペースで区切られた単一の VLAN ID。例：100 200 300 • スペースで区切られた 1 つ以上の VLAN ID の範囲。例：1-1024 2000-2499

コマンド デフォルト

デフォルトでは、VLAN ID の照合は行われません。

コマンド モード

クラス マップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(18)SXE	このコマンドが、Cisco Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータに導入されました。
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。

使用上のガイドライン

matchinputvlan コマンドにより、入力インターフェイスでパケットが受信されたときに、1 つ以上の特定の VLAN ID とパケットを照合するクラス マップを作成できます。これにより、Ethernet over MPLS（EoMPLS）仮想回線（VC）用の階層型 Quality of Service（HQoS）が有効になり、QoS クラス マップとポリシー マップの間の親子関係が使用できるようになります。これにより、サービス プロバイダーは、特定の EoMPLS ネットワークのトラフィックを簡単に分類および整形することができます。

EoMPLS アプリケーションでは、通常、親クラス マップが特定の EoMPLS ネットワーク内のすべての VC の最大帯域幅を指定します。その後、子クラスマップがこのトラフィックのサブセットに対して、その他の QoS 操作（トラフィック シェーピングなど）を実行します。

matchinputvlan コマンドと、クラスマップ コンフィギュレーション コマンドでもある **matchvlan** コマンドを混同しないでください。

- **matchvlan** コマンドは、ポリシーマップが適用される特定のインターフェイスのパケットで VLAN ID を照合します。**matchvlan** コマンドを使用するポリシーマップは、**service-policy**

{**input**|**output**} コマンドを使用して、ルータの入力または出力インターフェイスに適用できます。

- **matchinputvlan** コマンドは、ルータの入力インターフェイスで受信されたパケットでVLAN ID を照合します。通常、**matchinputvlan** コマンドを使用するポリシー マップは、**service-policyoutput** コマンドを使用してルータの出力インターフェイスに適用されます。

また、**matchinputvlan** コマンドは、VLAN 間ルーティングに使用される論理 VLAN インターフェイスで受信されたパケットを照合する、**matchinput-interfacevlan** コマンドと混同されることもあります。

ヒント　クラス マップは **matchinput-interface** コマンドもサポートしているため、**matchinputvlan** コマンドを入力するときは **input** キーワードを省略することはできません。

（注）　**matchinputvlan** コマンドは、FlexWAN、拡張 FlexWAN、および Optical Service Module（OSM）ライン カード上のレイヤ 2 LAN ポートでのみ使用できません。

matchinputvlan コマンドを使用するときは、次の制限が適用されます。

- VLAN インターフェイス（**interfacevlan** コマンドで作成された論理インターフェイス）にサービス ポリシーをすでにアタッチしている場合には、インターフェイスに**matchinputvlan** を使用するポリシーをアタッチすることはできません。
- **matchinputvlan** コマンドを使用するクラス マップは、**match-any** オプションのみをサポートしています。**matchinputvlan** コマンドを使用するクラス マップで **match-all** オプションを使用することはできません。
- 親クラスに **matchinputvlan** コマンドを使用するクラス マップが含まれている場合は、子クラス マップで **matchexp** コマンドを使用することはできません。

例

次の例では、VLAN ID が 1000 のパケットを照合するクラス マップとポリシー マップを作成します。このポリシー マップは、このトラフィックを 10 Mbps（10,000,000 bps）の認定情報レート（CIR）値に整形します。その後、最後の行でこのポリシー マップを特定のギガビット イーサネット WAN インターフェイスに適用します。

```
Router# configure terminal

Router(config)# class-map match-any vlan1000

Router(config-cmap)# match input vlan 1000

Router(config-cmap)# exit

Router(config)# policy-map policy1000

Router(config-pmap)# class vlan1000
```

```
Router(config-pmap-c)# exit

Router(config-pmap)# shape average 10000000

Router(config-pmap)# interface GE-WAN 3/0

Router(config-if)# service-policy output policy1000

Router(config-if)#
```

次に、VLAN ID 100、200、および300と照合するように設定されるクラス マップの例を示します。

```
Router# configure terminal

Router(config)# class-map match-any hundreds

Router(config-cmap)# match input vlan 100 200 300

Router(config-cmap)#
```

次に、2000 ～ 2999 のすべての VLAN ID と照合するように設定されるクラス マップの例を示します。

```
Router# configure terminal

Router(config)# class-map match-any vlan2000s

Router(config-cmap)# match input vlan 2000-2999

Router(config-cmap)#
```

次に、VLAN ID の範囲と特定の VLAN ID の両方と照合するように設定されるクラス マップの例を示します。

```
Router# configure terminal

Router(config)# class-map match-any misc

Router(config-cmap)# match input vlan 1 5 10-99 2000-2499

Router(config-cmap)#
```

関連コマンド

コマンド	説明
clearceflinecard	1 つ以上のライン カード上の Cisco Express Forwarding（CEF）情報をクリアしますが、メイン ルート プロセッサ（RP）上の CEF 情報はクリアしません。これにより、ライン カード上の CEF 情報が RP 上の CEF 情報と同期されます。
matchqos-group	一致基準として特定の QoS グループ値を指定します。
mlsqostrust	保存する必要があるパケットの着信 QoS フィールドを決めるために、インターフェイスの信頼状態を設定します。

コマンド	説明
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービスポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。
showplatformqospolicy-map	ルータに設定されているポリシーマップのタイプと数を表示します。

match input-interface

指定された入力インターフェイスを一致基準として使用するようにクラスマップを設定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchinput-interface** コマンドを使用します。入力インターフェイスの一致基準をクラス マップから削除するには、このコマンドの **no** 形式を使用します。

match input-interface *interface-name*
no match input-interface *interface-name*

構文の説明

interface-name	一致基準として使用する入力インターフェイスの名前です。

コマンド デフォルト

一致基準が指定されていません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

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

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。
12.0(7)S	このコマンドが、Cisco IOS Release 12.0(7)S に統合されました。
12.0(17)SL	このコマンドが拡張され、入力インターフェイスでの一致を含むようになりました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
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 Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーションモードにします。

（注） CSCtx62310 では、このコマンドを一意に識別するために入力する必要がある最小文字列は **match input-** です。デバイスが、このコマンドの省略バージョンとして **match input** を受け入れなくなりました。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

ポリシー インライン コンフィギュレーション モードにするために、まず **service-policytypeperformance-monitorinline** コマンドを入力する必要があります。

Cisco 10000 シリーズ ルータ以外でサポートされるプラットフォーム

クラスベース重み付け均等化キューイング（CBWFQ）の場合は、入力インターフェイス、アクセス コントロール リスト（ACL）、プロトコル、Quality of Service（QoS）ラベル、Experimental（EXP）フィールドの値などの一致基準に基づいて、トラフィック クラスを定義します。クラスの一致基準を満たすパケットは、そのクラスのトラフィックの一部となります。

matchinput-interface コマンドは、クラス マップで指定されたクラスに属しているかどうかを確認するパケットに対して、一致基準として使用される入力インターフェイスの名前を指定します。

matchinput-interface コマンドを使用するには、まず **class-map** コマンドを入力して、一致基準を確立するクラスの名前を指定する必要があります。クラスを指定したら、次のいずれかのコマンドを使用してそのクラスの一致基準を設定できます。

- **matchaccess-group**
- **matchinput-interface**
- **matchmplsexperimental**
- **matchprotocol**

クラスマップで複数のコマンドを指定する場合、最後に入力されたコマンドだけが適用されます。最後のコマンドは、それ以前に入力されたコマンドを無効にします。

Cisco 10000 シリーズ ルータ

CBWFQ では、入力インターフェイス、ACL、プロトコル、QoS ラベル、EXP フィールド値などの一致基準に基づいて、トラフィック クラスを定義します。クラスの一致基準を満たすパケットは、そのクラスのトラフィックの一部となります。

matchinput-interface コマンドを使用するには、まず **class-map** コマンドを入力して、一致基準を確立するクラスの名前を指定する必要があります。

例

次の例では、ethernet1 という名前のクラス マップを指定し、このクラスの一致基準として使用される ethernet1 という名前の入力インターフェイスを設定します。

```
Router(config)# class-map ethernet1
Router(config-cmap)# match input-interface ethernet1
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor 用のサービス ポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過する、ethernet1 という名前の入力インターフェイスの基準と一致するパケットが、fm-2 という名前のフロー モニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match input-interface ethernet 1
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

Command	Description
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
matchaccess-group	指定した ACL に基づいてクラス マップの一致基準を設定します。
matchmplsexperimental	指定した EXP フィールド値を一致基準として使用するクラス マップを設定します。
matchprotocol	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。

match ip dscp

matchipdscp コマンドは、match dscp コマンドによって置き換えられます。詳細については、match dscp コマンドを参照してください。

match ip precedence

matchipprecedence コマンドは、match precedence コマンドによって置き換えられます。詳細については、match precedence コマンドを参照してください。

match ip rtp

Real-Time Protocol（RTP）ポートを一致基準として使用するようにクラスマップを設定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchiprtp** コマンドを使用します。RTP ポートの一致基準を削除するには、このコマンドの **no** 形式を使用します。

match ip rtp *starting-port-number port-range*
no match ip rtp

構文の説明

starting-port-number	開始 RTP ポート番号。値の範囲は 2000 ～ 65535 です。
port-range	RTP ポート番号の範囲です。値の範囲は 0 ～ 16383 です。

コマンド デフォルト

一致基準が指定されていません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.1(2)T	このコマンドが導入されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
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 Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーション モードにします。

このコマンドは、指定されたポート範囲内のIP RTPパケットを照合するために使用されます。*starting port number* 引数から *starting port number* 引数に *port range* 引数を加えた数までの範囲の、すべての偶数 User Datagram Port（UDP）ポート番号宛てのパケットを照合します。

RTP ポート範囲を一致基準として使用することは、音声やビデオなどの RTP を使用するアプリケーションに特に効果的です。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、s**ervice-policytypeperformance-monitorinline** コマンドを入力する必要があります。

例

次に、ethernet1 という名前のクラス マップを指定し、RTP ポート番号 2024 および範囲 1000 を、このクラスの一致基準として使用されるように設定する例を示します。

```
Router(config)# class-map ethernet1
Router(config-cmap)# match ip rtp 2024 1000
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor用のサービスポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過する、RTP ポート番号 2024 と範囲 1000 の基準に一致するパケットが、**fm-2** という名前のフローモニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
ip rtp 2024 1000
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

Command	Description
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。
iprtppriority	UDP 宛先ポートの範囲に属する RTP パケット フローセットについて、完全プライオリティ キューを予約します。
matchaccess-group	指定した ACL 番号に基づいてクラス マップの一致基準を設定します。

match mpls experimental

Experimental（EXP）フィールドに指定された値（複数可）を一致基準として使用するようにクラス マップを設定するには、クラスマップ コンフィギュレーション モードで **matchmplsexperimental** コマンドを使用します。EXP フィールドの一致基準をクラス マップから削除するには、このコマンドの **no** 形式を使用します。

match mpls experimental *number*
no match mpls experimental *number*

構文の説明

number	一致基準として使用する EXP フィールドの値（0 ～ 7 からの任意の値）。スペースで区切って複数の値を指定できます（3 4 7 など）。

コマンド デフォルト

一致基準が指定されていません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(7)XE1	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.2(4)T	このコマンドが Cisco MGX RPM-PR カードを持つ Cisco MGX 8850 スイッチおよび MGX 8950 スイッチに実装されました。
12.2(4)T2	このコマンドは、Cisco 7500 シリーズに実装されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズに実装されました。
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

Cisco 10000 シリーズ以外のサポートされているプラットフォーム

クラスベース重み付け均等化キューイング（CBWFQ）の場合は、入力インターフェイス、アクセス コントロール リスト（ACL）、プロトコル、Quality of Service（QoS）ラベル、Experimental（EXP）フィールドの値などの一致基準に基づいてトラフィック クラスを定義します。クラスの一致基準を満たすパケットは、そのクラスのトラフィックの一部となります。

matchmplsexperimental コマンドは、クラス マップで指定されたクラスに属しているかどうかを確認するパケットに対して、一致基準として使用される EXP フィールドの名前を指定します。

matchmplsexperimental コマンドを使用するには、まず **class-map** コマンドを入力して、一致基準を確立するクラスの名前を指定する必要があります。クラスを指定したら、次のいずれかのコマンドを使用してそのクラスの一致基準を設定できます。

- **matchaccess-group**
- **matchinput-interface**
- **matchmplsexperimental**
- **matchprotocol**

クラスマップで複数のコマンドを指定する場合、最後に入力されたコマンドだけが適用されます。最後のコマンドは、それ以前に入力されたコマンドを無効にします。

Cisco 10000 シリーズ

このコマンドは、ESR-PRE1 モジュールでのみ使用可能です。

CBWFQ では、入力インターフェイス、ACL、プロトコル、QoS ラベル、EXP フィールド値などの一致基準に基づいてトラフィック クラスを定義します。クラスの一致基準を満たすパケットは、そのクラスのトラフィックの一部となります。

matchmplsexperimental コマンドを使用するには、まず **class-map** コマンドを入力して、一致基準を確立するクラスの名前を指定する必要があります。

例

次に、ethernet1 というクラス マップを指定し、マルチプロトコル ラベル スイッチング（MPLS）Experimental 値の 1 および 2 をこのクラスの一致基準として使用するように設定する例を示します。

```
Router(config)# class-map ethernet1
Router(config-cmap)# match mpls experimental 1 2
```

関連コマンド

Command	Description
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
matchaccess-group	指定した ACL に基づいてクラス マップの一致基準を設定します。
matchinput-interface	指定された入力インターフェイスを一致基準として使用するクラス マップを設定します。
matchmplsexperimentaltopmost	topmost ラベルの EXP 値を一致基準とします。
matchprotocol	特定のプロトコルでトラフィックを照合します。

Command	Description
matchqos-group	指定したプロトコルに基づいてクラス マップの一致基準を設定します。

match mpls experimental topmost

最上位ラベル ヘッダーの Experimental（EXP）値と照合するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchmplsexperimentaltopmost** コマンドを使用します。EXP の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 mpls experimental topmost number
no match mpls experimental topmost number

構文の説明

number	最上位ラベル ヘッダーのマルチプロトコル ラベル スイッチング（MPLS）EXP フィールドです。有効な値は 0 ～ 7 です。

コマンド デフォルト

最上位ラベル ヘッダーに EXP の一致基準は設定されていません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。
Cisco IOS XE リリース 2.3	このコマンドが、Cisco IOS XE Release 2.3 に統合されました。
15.1(3)T	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。
12.2(33)SCF	このコマンドが、Cisco IOS リリース 12.2(33)SCF に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーション モードにします。

このコマンドは、入力インターフェイスと出力インターフェイスに対して入力できます。このコマンドは MPLS パケットでのみ照合します。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、**service-policytypeperformance-monitorinline** コマンドを入力する必要があります。

例

次に、最上位ラベル ヘッダーの EXP 値 3 が照合される例を示します。

```
Router(config)# class-map mpls exp
Router(config-cmap)# match mpls experimental topmost 3
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor用のサービス ポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過する、最上位ラベル ヘッダーの EXP 値 3 の基準に一致するパケットが、**fm-2** という名前のフローモニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match mpls experimental topmost 3
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。
setmplsexperimentaltopmost	入力インターフェイスまたは出力インターフェイスでの最上位 MPLS ラベル ヘッダーに、MPLS EXP フィールド値を設定します。

match not

単一の一致基準値を成功しない一致基準として使用するように指定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchnot** コマンドを使用します。以前に指定していたソース値を削除して一致基準として使用しないようにするには、このコマンドの **no** 形式を使用します。

match not *match-criterion*
no match not *match-criterion*

構文の説明

match-criterion	成功しない一致基準とする一致基準値です。指定した一致基準以外のすべての値は、成功する一致基準とみなされます。

コマンド デフォルト

成功しない一致基準は設定されていません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.0(5)T	このコマンドが Cisco IOS Release 12.0(5)T に統合されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
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 Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーション モードにします。

matchnot コマンドは、一致基準として使用されない Quality of Service（QoS）ポリシー値を指定するために使用されます。**matchnot** コマンドが使用された場合、その QoS ポリシー以外のすべての値は、成功する一致基準になります。

たとえば、QoS クラスマップ コンフィギュレーション モードで **matchnotqos-group4** コマンドが発行された場合、指定されたクラスは 4 以外のすべての QoS グループ値を成功する一致基準として受け入れます。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、s**ervice-policytypeperformance-monitorinline** コマンドを入力する必要があります。

例

次のトラフィック クラスでは、IP 以外のすべてのプロトコルが成功する一致条件と見なされます。

```
Router(config)# class-map noip
Router(config-cmap)# match not protocol ip
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor 用のサービス ポリシーを設定する例を示します。このポリシーは、IP 以外のすべてのプロトコルのイーサネット インターフェイス 0/0 を通過するパケットが、**fm-2** という名前のフロー モニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match not protocol ip
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。

match packet length (class-map)

IP ヘッダー内のレイヤ 3 パケット長をクラス マップ内の一致基準として指定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchpacketlength** コマンドを使用します。一致基準として指定済みのレイヤ 3 パケット長を取り消すには、このコマンドの **no** 形式を使用します。

match packet length {**max** *maximum-length-value* [**min** *minimum-length-value*]|**min** *minimum-length-value* [**max** *maximum-length-value*]}
no match packet length {**max** *maximum-length-value* [**min** *minimum-length-value*]|**min** *minimum-length-value* [**max** *maximum-length-value*]}

構文の説明

max	レイヤ 3 パケット長の最大値が指定されることを示します。
maximum-length-value	レイヤ 3 パケット長の最大長の値（バイト単位）です。範囲は 1 ～ 2000 です。
min	レイヤ 3 パケット長の最小値が指定されることを示します。
minimum-length-value	レイヤ 3 パケット長の最小長の値（バイト単位）です。範囲は 1 ～ 2000 です。

コマンド デフォルト

IP ヘッダー内のレイヤ 3 パケット長は、一致基準として使用されません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。
12.2(18)SXE	このコマンドが、Cisco IOS Release 12.2(18)SXE に統合されました。
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。
Cisco IOS XE Release 2.2	このコマンドが Cisco IOS XE Release 2.2 に統合され、Cisco ASR 1000 シリーズ ルータに実装されました。
15.1(3)T	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーションモードにします。

このコマンドでは、IP ヘッダー内のレイヤ 3 パケット長のみが考慮されます。IP ヘッダー内のレイヤ 2 パケット長は考慮されません。

このコマンドを使用する場合は、少なくとも最大値または最小値を指定する必要があります。ただし、両方の値を入力することもできます。

最小値のみが指定されている場合は、最小値よりも大きいレイヤ3パケット長を持つパケットが、基準に一致するとみなされます。

最大値のみが指定されている場合は、最大値よりも小さいレイヤ3パケット長を持つパケットが、基準に一致するとみなされます。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、**service-policytypeperformance-monitorinline** コマンドを入力する必要があります。

例

次の例では、「class 1」という名前のクラス マップが作成され、一致基準としてレイヤ 3 パケット長が指定されています。この例では、最小レイヤ 3 パケット長が 100 バイトで、最大レイヤ 3 パケット長が 300 バイトのパケットが、一致基準を満たしているとされています。

```
Router(config)# class-map match-all class1
Router(config-cmap)# match packet length min 100 max 300
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor用のサービスポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過する、100 バイトの最小レイヤ 3 パケット長と 300 バイトの最大レイヤ 3 パケット長の基準に一致するパケットが、**fm-2** という名前のフロー モニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match packet length min 100 max 300
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。

コマンド	説明
showclass-map	すべてのクラス マップおよびその一致基準を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定のPVCに対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

match port-type

クラス マップのポートに基づいてアクセス ポリシーを照合するには、クラス マップ コンフィギュレーション モードで **matchport-type** コマンドを使用します。ポート タイプを削除するには、このコマンドの **no** 形式を使用します。

match port-type {**routed**|**switched**}
no match port-type {**routed**|**switched**}

構文の説明

routed	ルーテッド インターフェイスを照合します。クラス マップをルーテッド インターフェイスにのみ関連付ける必要がある場合は、このキーワードを使用します。
switched	スイッチド インターフェイスを照合します。クラス マップをスイッチド インターフェイスにのみ関連付ける必要がある場合は、このキーワードを使用します。

コマンド デフォルト

アクセス ポリシーは照合されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.4(6)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

このコマンドは、ユーザが接続するポートに基づいて、適用されるアクセス ポリシーが異なる可能性がある場合に使用されます。

例

次に、クラス マップのポートに基づいてアクセス ポリシーが照合される例を示します。

Router(config-cmap)# **matchport-typerouted**

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
matchtag(class-map)	クラス マップのタグ タイプに照合されるタグを指定します。

match precedence

一致基準として使用する IP プレシデンス値を特定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchprecedence** コマンドを使用します。クラス マップから特定の IP プレシデンス値を削除するには、このコマンドの **no** 形式を使用します。

match [ip] precedence
{*precedence-criteria1precedence-criteria2precedence-criteria3precedence-criteria4*}
no match [ip] precedence
{*precedence-criteria1precedence-criteria2precedence-criteria3precedence-criteria4*}

構文の説明

ip	（任意）IPv4 パケットのみを照合するように指定します。使用しない場合、IPv4 と IPv6 パケットの両方が照合されます。 （注） Cisco 10000 シリーズ ルータの場合は、**ip** キーワードが必要です。
precedence-criteria1 *precedence-criteria2* *precedence-criteria3* *precedence-criteria4*	優先順位値を指定します。スペースで区切って、最大4つの異なる値を入力できます。有効な値については、「使用上のガイドライン」セクションを参照してください。

コマンド デフォルト

一致基準は設定されていません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。このコマンドで **matchipprecedence** コマンドが置き換えられます。
12.0(17)SL	このコマンドが Cisco IOS Release 12.0(17)SL に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.0(28)S	このコマンドが IPv6 用に Cisco IOS Release 12.0(28)S に統合されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。
15.1(3)T	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。

リリース	変更箇所
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。
Cisco IOS XE Release 3.6	このコマンドが Cisco ASR 903 ルータに実装されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーション モードにします。

数字の省略形（0 ～ 7）または基準名（critical、flash など）で、単一の マッチング ステートメントに最大 4 つの一致基準を入力できます。たとえば、0、1、2、または 3 のプレシデンス値が必要な場合（指定したすべてのプレシデンス値ではなく、1 つの値だけが正常な一致基準であることに注意）、**matchipprecedence0123** コマンドを入力します。*precedence-criteria* の数字には、数学的な意味はありません。つまり、2 という *precedence-criteria* は、1 より大きいわけではありません。これらの異なるパケットが処理される方法は、ポリシーマップ コンフィギュレーション モードで設定される Quality of Service（QoS）ポリシーによって決まります。

QoS ポリシーは、ネットワークに入ってくるパケットの IP 優先順位マーキングを含むように設定できます。これにより、ネットワーク内のデバイスは、新しくマーキングされた IP 優先順位値を使用してパケットの処理方法を決定することができます。たとえば、クラスベースの重み付けランダム早期検出（WRED）は、IP 優先順位値を使用して、パケットがドロップされる確率を判断します。また、音声パケットを特定の優先順位でマーキングすることもできます。そうすれば、低遅延キューイング（LLQ）を設定して、その優先順位のすべてのパケットをプライオリティ キューに入れることができます。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、**service-policytypeperformance-monitorinline** コマンドを入力する必要があります。

Cisco 7600 および 10000 シリーズ ルータでの IPv6 および IPv4 パケットのプレシデンスの照合

Cisco 7600 シリーズおよび 10000 シリーズ ルータで、**matchprotocol** コマンドと **ipv6** キーワードを使用して、IPv6 パケットのみのプレシデンス値に基づく一致基準を設定します。このキーワードを使用しないと、プレシデンスでの照合はデフォルトで IPv4 パケットと IPv6 パケットの両方に対して行われます。**ip** キーワードを使用して、IPv4 パケットのみのプレシデンス値に基づく一致基準を設定します。**ip** キーワードを指定しないと、照合は IPv4 パケットと IPv6 パケットの両方に行われます。

優先順位の値と名前

次の表に、すべての基準条件の値、名前、バイナリ値、および推奨用途を示します。スペースで区切って、最大 4 つの条件を入力できます。1 つの優先順位値だけが一致すれば、一致したと判断されます。次の表に、IP プレシデンス値を示します。

表 *10 : IP precedence* 値

precedence 値	優先順位の名前	バイナリ値	推奨用途
0	routine	000	デフォルトのマーキング値
1	priority	001	データ アプリケーション
2	immediate	010	データ アプリケーション
3	flash	011	コール シグナリング
4	flash-override	100	ビデオ会議およびストリーミング ビデオ
5	critical	101	音声
6	internet (control)	110	ネットワーク コントロール トラフィック（ルーティングなど、通常は優先順位 6 にします）
7	network (control)	111	

IP 優先順位 6 と 7 は、コントロール パケットをマーキングするのでないかぎり、パケットのマーキングに使用しないでください。

例

IPv4 専用のトラフィック一致

次に、priority50 というサービス ポリシーを設定し、サービス ポリシー priority50 をインターフェイスにアタッチして、IPv4 トラフィックだけを照合する例を示します。IPv4 と IPv6 の両方が稼働しているネットワークでは、照合とトラフィックの分離でプロトコル間の区別を行う必要がある場合もあるでしょう。この例では、ipprec5 というクラス マップで、ファスト イーサネット インターフェイス 1/0/0 に入ってきたすべての IPv4 パケットについて、プレシデンス値が 5 かどうかを評価します。受信 IPv4 パケットが優先順位値 5 でマーキングされていた場合、パケットはプライオリティ トラフィックとして扱われ、50 kbps の帯域幅が割り当てられます。

```
Router(config)# class-map ipprec5
Router(config-cmap)# match ip precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

IPv6 専用のトラフィック一致

次に、IPv6 トラフィックだけの優先順位を照合する、同じサービス ポリシーを示します。**ipv6** キーワードを持つ **matchprotocol** コマンドが、**matchprecedence** コマンドよりも優先されることに注意してください。IPv6 トラフィックだけの照合を行うには、**matchprotocol** コマンドが必要です。

```
Router(config)# class-map ipprec5
Router(config-cmap)# match protocol ipv6
Router(config-cmap)# match precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して、Performance Monitor 用のサービス ポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過する、match precedence 4 の基準に一致するパケットが、fm-2 という名前のフローモニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match precedence 4
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# end
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
matchprotocol	指定されたプロトコルを基づくクラス マップの一致基準を設定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシーマップを対応付けます。

コマンド	説明
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。
setipprecedence	IP ヘッダーに優先順位を設定します。
showclass-map	すべてのクラス マップとその一致基準を表示するか、または指定したクラス マップとその一致基準を表示します。

match protocol

指定されたプロトコルに基づいてクラス マップの一致基準を設定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchprotocol** コマンドを使用します。プロトコルベースの一致基準をクラス マップから削除するには、このコマンドの **no** 形式を使用します。

match protocol *protocol-name*
no match protocol *protocol-name*

構文の説明

protocol-name	一致基準として使用されるプロトコルの名前です（bgp など）。ほとんどのルータでサポートされているプロトコルのリストについては、「使用上のガイドライン」を参照してください。

コマンド デフォルト

一致基準は設定されていません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。
12.0(7)S	このコマンドが、Cisco IOS Release 12.0(7)S に統合されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(13)E	このコマンドが Cisco IOS Release 12.1(13)E に統合され、FlexWAN モジュールのない Catalyst 6000 ファミリ スイッチに実装されました。
12.2(8)T	このコマンドが Cisco IOS Release 12.2(8)T に統合されました。
12.2(13)T	このコマンドが変更され、一致基準として使用されるプロトコルのリストから **apollo**、**vines**、および **xns** が削除されました。Apollo Domain、Banyan VINES、および Xerox Network Systems（XNS）がこのリリースで削除されたため、これらのプロトコルは削除されました。IPv6 パケットでの照合をサポートするために、IPv6 プロトコルが追加されました。
12.0(28)S	このコマンドが IPv6 用に Cisco IOS Release 12.0(28)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。

リリース	変更箇所
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
12.2(18)SXE	このコマンドが Cisco IOS Release 12.2(18)SXE に統合され、Supervisor Engine 720 に実装されました。
12.4(6)T	このコマンドが変更されました。Napster プロトコルはサポートされなくなったため、削除されました。
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。
12.2(31)SB2	このコマンドが Cisco IOS Release 12.2(31)SB2 に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.2(18)ZY	このコマンドが、Cisco IOS Release 12.2(18)ZY に統合されました。このコマンドは、Supervisor 32/Programmable Intelligent Services Accelerator（PISA）エンジンが搭載された Catalyst 6500 シリーズ スイッチの Network-Based Application Recognition（NBAR）機能を拡張するため、変更されました。
12.4(15)XZ	このコマンドが、Cisco IOS Release 12.4(15)XZ に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合され、Cisco 1700、Cisco 1800、Cisco 2600、Cisco 2800、Cisco 3700、Cisco 3800、Cisco 7200、および Cisco 7300 シリーズ ルータに実装されました。
Cisco IOS XE Release 2.2	このコマンドが Cisco IOS XE Release 2.2 に統合され、Cisco ASR 1000 シリーズ ルータに実装されました。
Cisco IOS XE Release 3.1S	このコマンドが変更されました。より多くのプロトコルのサポートが追加されました。
15.1(3)T	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシーインライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーション モードにします。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、s**ervice-policytypeperformance-monitorinline** コマンドを入力する必要があります。

Cisco 7600 ルータおよび Cisco 10000 シリーズ ルータ以外でサポートされるプラットフォーム

クラスベース重み付け均等化キューイング（CBWFQ）の場合は、一致基準プロトコル、アクセス コントロール リスト（ACL）、入力インターフェイス、Quality of Service（QoS）ラベル、および Experimental（EXP）フィールドの値に基づいて、トラフィック クラスを定義します。クラスの一致基準を満たすパケットは、そのクラスのトラフィックの一部となります。

matchprotocol コマンドは、クラス マップで指定されたクラスに属しているかどうかを確認するパケットに対して、一致基準として使用されるプロトコルの名前を指定します。

matchprotocolipx コマンドは出力方向のパケットのみを照合します。

matchprotocol コマンドを使用するには、まず **class-map** コマンドを入力して、一致基準を確立するクラスの名前を指定する必要があります。クラスを指定したら、次のいずれかのコマンドを使用してそのクラスの一致基準を設定できます。

- **matchaccess-group**
- **matchinput-interface**
- **matchmplsexperimental**

クラスマップで複数のコマンドを指定する場合、最後に入力されたコマンドだけが適用されます。最後のコマンドは、それ以前に入力されたコマンドを無効にします。

NBAR トラフィックによりサポートされているプロトコル タイプを照合するように NBAR を設定するには、**matchprotocol(NBAR)** コマンドを使用します。

Cisco 7600 シリーズ ルータ

QoS クラスマップ コンフィギュレーションの **matchprotocol** コマンドは、NBAR を設定し、入力と出力両方のポート上のすべてのトラフィックを送信して、マルチレイヤ スイッチ フィーチャ カード 2（MSFC2）のソフトウェアで処理されるようにします。

CBWFQ の場合は、プロトコル、ACL、入力インターフェイス、QoS ラベル、およびマルチプロトコル ラベル スイッチング（MPLS）EXP フィールド値などの一致基準に基づいて、トラフィック クラスを定義します。クラスの一致基準を満たすパケットは、そのクラスのトラフィックの一部となります。

matchprotocol コマンドは、クラス マップで指定されたクラスに属しているかどうかを確認するパケットに対して、一致基準として使用されるプロトコルの名前を指定します。

matchprotocol コマンドを使用する場合は、まず **class-map** コマンドを入力して、一致基準を確立するクラスの名前を指定する必要があります。

クラスマップで複数のコマンドを指定する場合、最後に入力されたコマンドだけが適用されます。最後のコマンドは、それ以前に入力されたコマンドを無効にします。

このコマンドは、NBAR機能が認知するプロトコルを照合するのに使用されます。NBARがサポートするプロトコルの一覧については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classification」を参照してください。

Cisco 10000 シリーズ ルータ

CBWFQの場合は、プロトコル、ACL、入力インターフェイス、QoSラベル、およびEXPフィールド値などの一致基準に基づいて、トラフィック クラスを定義します。クラスの一致基準を満たすパケットは、そのクラスのトラフィックの一部となります。

matchprotocol コマンドは、クラス マップで指定されたクラスに属しているかどうかを確認するパケットに対して、一致基準として使用されるプロトコルの名前を指定します。

matchprotocolipx コマンドは出力方向のパケットのみを照合します。

matchprotocol コマンドを使用するには、まず **class-map** コマンドを入力して、一致基準を確立するクラスの名前を指定する必要があります。

NBAR プロトコルを照合する場合は、**matchprotocol** (NBAR) コマンドを使用します。

match protocol コマンドの制限（Catalyst 6500 シリーズ スイッチのみ）

ポリシー マップにはトラフィック クラスが含まれています。トラフィック クラスには、プロトコルタイプまたはアプリケーションに基づいてパケットを照合する（およびグループにまとめる）ために使用できる、1 つ以上の **match** コマンドが含まれています。必要に応じて任意の数のトラフィック クラスを作成できます。

Cisco IOS Release 12.2(18)ZY には、Supervisor 32/PISA エンジンが搭載された Catalyst 6500 シリーズスイッチ用のソフトウェアが含まれています。このリリースおよびプラットフォームでは、ポリシー マップと **matchprotocol** コマンドの使用に関する次の制限に注意してください。

- 1 つのトラフィック クラスは、最大 8 個のプロトコルまたはアプリケーションに一致するように設定できます。
- 複数のトラフィック クラスは、累積で最大 95 個のプロトコルまたはアプリケーションに一致するように設定できます。

サポートされるプロトコル

以下の表に、ほとんどのルータでサポートされているプロトコルを示します。一部のルータは、いくつかの追加のプロトコルをサポートしています。たとえば、Cisco 7600 ルータは AARP および DECnet プロトコルをサポートし、Cisco 7200 ルータは directconnect および PPPOE プロトコルをサポートしています。サポートされているプロトコルの完全なリストについては、使用しているルータの **matchprotocol** コマンドのオンライン ヘルプを参照してください。

表 *11* : サポートされるプロトコル

プロトコル名	説明
802-11-iapp	IEEE 802.11 ワイヤレス ローカルエリア ネットワーク ワーキング グループの Internet Access Point Protocol
ace-svr	ACE サーバ/伝達
aol	America-Online Instant Messenger
appleqtc	Apple QuickTime
arp*	IP Address Resolution Protocol（ARP）

プロトコル名	説明
bgp	Border Gateway Protocol; ボーダー ゲートウェイ プロトコル
biff	Biff メール受信通知
bootpc	ブートストラップ プロトコル クライアント
bootps	ブートストラップ プロトコル サーバ
bridge*	bridging
cddbp	CD Database Protocol
cdp*	Cisco Discovery Protocol
cifs	CIFS
cisco-fna	Cisco FNATIVE
cisco-net-mgmt	cisco-net-mgmt
cisco-svcs	Cisco license/perf/GDP/X.25/ident svcs
cisco-sys	Cisco SYSMAINT
cisco-tdp	cisco-tdp
cisco-tna	Cisco TNATIVE
citrix	Citrix Systems メタフレーム
citriximaclient	Citrix IMA クライアント
clns*	ISO Connectionless Network Service
clns_es*	ISO CLNS エンド システム
clns_is*	ISO CLNS 中継システム
clp	Cisco Line Protocol
cmns*	ISO Connection-Mode Network Service
cmp	Cluster Membership Protocol
compressedtcp*	Compressed TCP
creativepartnr	Creative Partner
creativeserver	Creative Server
cuseeme	CU-SeeMe デスクトップ ビデオ会議
daytime	Daytime（RFC 867）

プロトコル名	説明
dbase	dBASE Unix
dbcontrol_agent	Oracle Database Control Agent
ddns-v3	ダイナミック DNS バージョン 3
dhcp	ダイナミック ホスト コンフィギュレーション
dhcp-failover	DHCP フェールオーバー
directconnect	Direct Connect
discard	ポートの廃棄
dns	ドメイン ネーム サーバ ルックアップ
dnsix	DNSIX Security Attribute Token Map
echo	エコー ポート
edonkey	eDonkey
egp	エクステリア ゲートウェイ プロトコル
eigrp	Enhanced Interior Gateway Routing Protocol
entrust-svc-handler	Entrust KM/Admin Service Handler
entrust-svcs	Entrust sps/aaas/aams
exec	リモート プロセスの実行
exchange	Microsoft RPC for Exchange
fasttrack	FastTrack トラフィック（KaZaA、Morpheus、Grokster など）
fcip-port	FCIP
finger	Finger
ftp	ファイル転送プログラム
ftps	FTP over TLS/SSL
gdoi	グループ ドメイン オブ インタープリテーション
giop	Oracle GIOP/SSL
gnutella	Gnutella バージョン 2 トラフィック（BearShare、Shareeza、Morpheus など）
gopher	Gopher
gre	総称ルーティング カプセル化

プロトコル名	説明
gtpv0	GPRS トンネリング プロトコル バージョン 0
gtpv1	GPRS トンネリング プロトコル バージョン 1
h225ras	H225 RAS over Unicast
h323	H.323 プロトコル
h323callsigalt	H323 Call Signal Alternate
hp-alarm-mgr	HP Performance データ アラーム マネージャ
hp-collector	HP Performance データ コレクター
hp-managed-node	HP Performance データ管理対象ノード
hsrp	Hot Standby Router Protocol; ホットスタンバイ ルータ プロトコル
http	ハイパーテキスト転送プロトコル
https	Secure Hypertext Transfer Protocol
ica	ica（Citrix）
icabrowser	icabrowser（Citrix）
icmp	Internet Control Message Protocol; インターネット制御メッセージ プロトコル
ident	認証サービス（Authentication Service）
igmpv3lite	IGMP over UDP for SSM
imap	Internet Message Access Protocol
imap3	Interactive Mail Access Protocol 3
imaps	IMAP over TLS/SSL
ip*	IP（バージョン 4）
ipass	IPASS
ipinip	IP in IP（カプセル化）
ipsec	IP セキュリティ プロトコル（ESP/AH）
ipsec-msft	Microsoft IPsec NAT-T
ipv6*	IP（バージョン 6）
ipx	IPX

プロトコル名	説明
irc	インターネット リレー チャット
irc-serv	IRC-SERV
ircs	IRC over TLS/SSL
ircu	IRCU
isakmp	ISAKMP
iscsi	[iSCSI]
iscsi-target	iSCSI ポート
kazaa2	Kazaa バージョン 2
kerberos	Kerberos
l2tp	レイヤ 2 トンネル プロトコル
ldap	Lightweight Directory Access Protocol
ldap-admin	LDAP 管理サーバ ポート
ldaps	LDAP over TLS/SSL
llc2*	llc2
login	リモート ログイン
lotusmtap	Lotus Mail Tracking Agent Protocol
lotusnote	Lotus Notes
mgcp	Media Gateway Control Protocol
microsoft-ds	Microsoft-DS
msexch-routing	Microsoft Exchange Routing
msnmsgr	MSN Instant Messenger
msrpc	Microsoft Remote Procedure Call
msrpc-smb-netbios	MSRPC over TCP port 445
ms-cluster-net	MS Cluster Net
ms-dotnetster	Microsoft .NETster Port
ms-sna	Microsoft SNA Server/Base
ms-sql	Microsoft SQL

プロトコル名	説明
ms-sql-m	Microsoft SQL モニタ
mysql	MySQL
n2h2server	N2H2 フィルタ サービス ポート
ncp	NCP（Novell）
net8-cman	Oracle Net8 Cman/Admin
netbios	Network Basic Input/Output System
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS セッション サービス
netshow	Microsoft Netshow
netstat	systat のバリアント
nfs	ネットワーク ファイル システム
nntp	Network News Transfer Protocol
novadigm	Novadigm Enterprise Desktop Manager（EDM）
ntp	ネットワーク タイム プロトコル
oem-agent	OEM エージェント（Oracle）
oracle	Oracle
oracle-em-vp	Oracle EM/VP
oraclenames	Oracle Names
orasrv	Oracle SQL*Net v1/v2
ospf	Open Shortest Path First
pad*	Packet Assembler/Disassembler（PAD）のリンク
pcanywhere	Symantec pcANYWHERE
pcanywheredata	pcANYWHEREdata
pcanywherestat	pcANYWHEREstat
pop3	Post Office Protocol
pop3s	POP3 over TLS/SSL

プロトコル名	説明
pppoe	Point-to-Point Protocol over Ethernet
pptp	ポイントツーポイント トンネリング プロトコル
printer	プリント スプーラ/ldp
pwdgen	Password Generator Protocol
qmtp	Quick Mail Transfer Protocol
radius	RADIUS & Accounting
rcmd	Berkeley Software Distribution（BSD）r-commands（rsh、rlogin、rexec）
rdb-dbs-disp	Oracle RDB
realmedia	RealNetwork's Realmedia Protocol
RealSecure	ISS Real Secure Console Service Port
rip	Routing Information Protocol
router	ローカル ルーティング プロセス
rsrb*	リモート ソースルート ブリッジング
rsvd	RSVD
rsvp	リソース予約プロトコル
rsvp-encap	RSVP ENCAPSULATION-1/2
rsvp_tunnel	RSVP トンネル
rtc-pm-port	Oracle RTC-PM ポート
rtelnet	Remote Telnet Service
rtp	Real-Time Protocol：リアルタイム プロトコル
rtsp	Real Time Streaming Protocol
r-winsock	remote-winsock
secure-ftp	FTP over Transport Layer Security/Secure Sockets Layer（TLS/SSL）
secure-http	Secured HTTP
secure-imap	Internet Message Access Protocol over TLS/SSL
secure-irc	Internet Relay Chat over TLS/SSL
secure-ldap	Lightweight Directory Access Protocol over TLS/SSL

プロトコル名	説明
secure-nntp	Network News Transfer Protocol over TLS/SSL
secure-pop3	Post Office Protocol over TLS/SSL
secure-telnet	Telnet over TLS/SSL
send	SEND
shell	リモート コマンド
sip	Session Initiation Protocol
sip-tls	Session Initiation Protocol-Transport Layer Security
skinny	Skinny Client Control Protocol
sms	SMS RCINFO/XFER/CHAT
smtp	Simple Mail Transfer Protocol
snapshot	スナップショット ルーティング サポート
snmp	Simple Network Protocol
snmptrap	SNMP トラップ（SNMP Trap）
socks	Sockets ネットワーク プロキシ プロトコル（SOCKS）
sqlnet	Structured Query Language (SQL)*NET for Oracle
sqlserv	SQL サービス
sqlsrv	SQL サービス
sqlserver	Microsoft SQL Server
ssh	セキュア シェル
sshell	SSLshell
ssp	状態同期プロトコル
streamwork	Xing Technology StreamWorks プレーヤー
stun	シスコ シリアル トンネル
sunrpc	Sun リモート プロシージャ コール（RPC）
syslog	System Logging Utility
syslog-conn	信頼性の高い syslog サービス
tacacs	ログイン ホスト プロトコル（TACACS）

プロトコル名	説明
tacacs-ds	TACACS-Database Service
tarantella	Tarantella
tcp	Transport Control Protocol
telnet	Telnet
telnets	Telnet over TLS/SSL
tftp	トリビアル ファイル転送プロトコル
time	時刻
timed	タイム サーバ
tr-rsrb	Cisco RSRB
tto	Oracle TTC/SSL
udp	ユーザ データグラム プロトコル
uucp	UUCPD/UUCP-RLOGIN
vdolive	VDOLive ストリーミング ビデオ
vofr*	Voice over Frame Relay
vqp	VLAN Query Protocol
webster	ネットワーク ディクショナリ
who	サービス提供元
wins	Microsoft WINS
x11	X Window システム
xdmcp	XDM 制御プロトコル
xwindows*	X-Windows リモート アクセス
ymsgr	Yahoo! インスタント メッセンジャー

* このプロトコルは、Supervisor 32/PISA エンジンが搭載された Catalyst 6500 シリーズ スイッチではサポートされていません。

例

次に、ftpという名前のクラスマップを指定し、FTPプロトコルを一致基準として設定する例を示します。

```
Router(config)# class-map ftp
```

```
Router(config-cmap)
#
 match protocol ftp
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor 用のサービス ポリシーを設定する例を示します。このポリシーは、IP プロトコルのイーサネット インターフェイス 0/0 を通過するパケットが、**fm-2** という名前のフロー モニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match protocol ip
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

Command	Description
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。
matchaccess-group	指定した ACL に基づいてクラス マップの一致基準を設定します。
matchinput-interface	指定された入力インターフェイスを一致基準として使用するクラス マップを設定します。
matchmplsexperimental	指定された実験フィールドの値を一致基準として使用するクラス マップを設定します。
matchprecedence	IP precedence 値を一致基準として識別します。
matchprotocol(NBAR)	NBARが認識するプロトコルタイプにより、トラフィックを照合するように NBAR を設定します。
matchqos-group	指定した EXP フィールド値を一致基準として使用するクラス マップを設定します。

match protocol attribute application-group

指定したアプリケーション グループに基づいてクラス マップの一致基準を設定するには、クラスマップ コンフィギュレーション モードで **matchprotocol attributeapplication-group** コマンドを使用します。アプリケーション グループの一致基準をクラス マップから削除するには、このコマンドの **no** 形式を使用します。

match protocol attribute application-group アプリケーション グループ [*application-name*]
no match protocol attribute application-group アプリケーション グループ

構文の説明

アプリケーション グループ	一致基準とするアプリケーション グループの名前です。ほとんどのルータでサポートされているアプリケーション グループのリストについては、「使用上のガイドライン」セクションを参照してください。
application-name	（任意）アプリケーションの名前です。アプリケーション名を指定すると、アプリケーション グループの代わりにアプリケーションが一致基準として設定されます。

コマンド デフォルト

一致基準は設定されていません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.4S	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 マップにはトラフィック クラスが含まれています。トラフィック クラスには、アプリケーション グループに基づいてパケットを照合する（およびグループにまとめる）ために使用できる、1 つ以上の **match** コマンドが含まれています。複数のトラフィック クラスを作成できます。次の表に、サポートされているアプリケーション グループを示します。

表 *12*：サポートされているアプリケーション グループ

アプリケーショングループ	説明
apple-talk-group	AppleTalk 関連のアプリケーションです。
banyan-group	Banyan 関連のアプリケーションです。
bittorrent-group	Bittorrent 関連のアプリケーションです。
corba-group	Corba 関連のアプリケーションです。

アプリケーショングループ	説明
edonkey-emule-group	edonkey-emule 関連のアプリケーションです。
fasttrack-group	Fasttrack 関連のアプリケーションです。
flash-group	Flash 関連のアプリケーションです。
fring-group	Fring 関連のアプリケーションです。
ftp-group	FTP 関連のアプリケーションです。
gnutella-group	Gnutella 関連のアプリケーションです。
icq-group	I Seek You（ICQ）関連のアプリケーションです。
imap-group	Internet Message Access Protocol（IMAP）関連のアプリケーションです。
irc-group	Internet Relay Chat（IRC）関連のアプリケーションです。
kerberos-group	Kerberos 関連のアプリケーションです。
ldap-group	Lightweight Directory Access Protocol（LDAP）関連のアプリケーションです。
my-jabber-group	My-jabber 関連のアプリケーションです。
netbios-group	NetBIOS 関連のアプリケーションです。
nntp-group	Network News Transfer Protocol（NNTP）関連のアプリケーションです。
npmp-group	Network Peripheral Management Protocol（NPMP）グループ関連の対象です。
other	その他のアプリケーションです。
pop3-group	Post Office Protocol 3（pop3）関連のアプリケーションです。
prm-group	Performance Report Message（PRM）関連のアプリケーションです。
skinny-group	Skinny 関連のアプリケーションです。
skype-group	Skype 関連のアプリケーションです。
smtp-group	Simple Mail Transfer Protocol（SMTP）関連のアプリケーションです。

アプリケーショングループ	説明
snmp-group	Simple Network Management Protocol（SNMP）関連のアプリケーションです。
sqlsvr-group	Structured Query Language（SQL）サーバ関連のアプリケーションです。
telepresence-group	Telepresence 関連のアプリケーションです。
tftp-group	TFTP 関連のアプリケーションです。
wap-group	Wireless Application Protocol（WAP）関連のアプリケーションです。
webex-group	Webex 関連のアプリケーションです。
windows-live-messenger-group	Windows Live Messenger 関連のアプリケーションです。
xns-xerox-group	Xerox Network Services（XNS）の Xerox 関連のアプリケーションです。
yahoo-messenger-group	Yahoo Messenger 関連のアプリケーションです。

例

次に、アプリケーション グループを一致基準として設定する例を示します。

```
Router(config)# class-map apps
Router(config-cmap)# match protocol attribute application-group skype-group
```

関連コマンド

Command	Description
matchprotocol(NBAR)	NBAR が認識するプロトコル タイプにより、トラフィックを照合するように NBAR を設定します。

match protocol attribute category

指定したアプリケーション カテゴリに基づいてクラス マップの一致基準を設定するには、クラスマップ コンフィギュレーション モードで **matchprotocolattributecategory** コマンドを使用します。アプリケーション カテゴリの一致基準をクラス マップから削除するには、このコマンドの **no** 形式を使用します。

match protocol attribute category *application-category* [*application-name*]
no match protocol attribute category *application-category*

構文の説明

application-category	一致基準として使用するアプリケーション カテゴリの名前です。ほとんどのルータでサポートされているアプリケーション カテゴリのリストについては、「使用上のガイドライン」セクションを参照してください。
application-name	（任意）アプリケーションの名前です。アプリケーション名を指定すると、アプリケーション カテゴリの代わりにアプリケーションが一致基準として設定されます。

コマンド デフォルト

一致基準は設定されていません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.4S	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 マップにはトラフィック クラスが含まれています。トラフィック クラスには、アプリケーション カテゴリに基づいてパケットを照合する（およびグループにまとめる）ために使用できる、1 つ以上の **match** コマンドが含まれています。必要に応じて任意の数のトラフィック クラスを作成できます。

次の表に、サポートされているアプリケーション カテゴリを示します。

表 *13*：サポートされているアプリケーション カテゴリ

カテゴリ名	説明
browsing	ブラウジング関連のアプリケーションです。
business-and-productivity-tools	ビジネス ツールと生産性ツール関連のアプリケーションです。
email	電子メール関連のアプリケーションです。
file-sharing	ファイル共有関連のアプリケーションです。

カテゴリ名	説明
gaming	ゲーム関連のアプリケーションです。
industrial-protocols	工業プロトコル関連のアプリケーションです。
instant-messaging	インスタント メッセージ関連のアプリケーションです。
internet-privacy	インターネット プライバシー関連のアプリケーションです。
layer2-non-ip	レイヤ 2 の非 IP 関連のアプリケーションです。
layer3-over-ip	Layer3-over-IP 関連のアプリケーションです。
location-based-services	ロケーションベース サービス関連のアプリケーションです。
net-admin	ネット管理関連のアプリケーションです。
newsgroup	ニュースグループ関連のアプリケーションです。
obsolete	廃止されたアプリケーションです。
other	その他のアプリケーションです。
trojan	トロイの木馬関連のアプリケーションです。
voice-and-video	音声およびビデオ関連のアプリケーションです。

例

次に、電子メール関連のアプリケーションを一致基準として設定する例を示します。

```
Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute category email
```

関連コマンド

Command	Description
match protocol attribute sub-category	指定したアプリケーション サブカテゴリの一致基準を設定します。

match protocol attribute sub-category

指定したアプリケーションサブカテゴリに基づいてクラスマップの一致基準を設定するには、クラスマップ コンフィギュレーション モードで **matchprotocol attributesub-category** コマンドを使用します。アプリケーションサブカテゴリの一致基準をクラスマップから削除するには、このコマンドの **no** 形式を使用します。

match protocol attribute sub-category *sub-category-name* [*aplication-name*]
no match protocol attribute sub-category *sub-category-name*

構文の説明

sub-category-name	一致基準として使用するアプリケーション サブカテゴリの名前です。ほとんどのルータでサポートされているアプリケーション サブカテゴリのリストについては、「使用上のガイドライン」セクションを参照してください。
application-name	（任意）アプリケーションの名前です。アプリケーション名を指定すると、サブカテゴリの代わりにアプリケーションが一致基準として設定されます。

コマンド デフォルト

一致基準は設定されていません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.4S	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 マップにはトラフィック クラスが含まれています。トラフィック クラスには、アプリケーションサブカテゴリに基づいてパケットを照合する（およびグループにまとめる）ために使用できる、1 つ以上の **match** コマンドが含まれています。必要に応じて任意の数のトラフィック クラスを作成できます。

次の表に、サポートされているアプリケーション サブカテゴリを示します。

表 *14 :* サポートされているアプリケーション サブカテゴリ

サブカテゴリ名	説明
authentication-services	認証サービス関連のアプリケーションです。
backup-systems	バックアップ システム関連のアプリケーションです。
client-server	クライアント/サーバ関連のアプリケーションです。
commercial-media-distribution	商用メディア配信関連のアプリケーションです。
control-and-signaling	制御およびシグナリング関連のアプリケーションです。

サブカテゴリ名	説明
database	データベース関連のアプリケーションです。
epayement	電子支払い関連のアプリケーションです。
inter-process-rpc	プロセス間リモートプロシージャ コール関連のアプリケーションです。
license-manager	ライセンス マネージャ関連のアプリケーションです。
naming-services	ネーミング サービス関連のアプリケーションです。
network-management	ネットワーク管理関連のアプリケーションです。
network-protocol	ネットワーク プロトコル関連のアプリケーションです。
other	その他の関連するアプリケーションです。
p2p-file-transfer	ピアツーピア ファイル転送関連のアプリケーションです。
p2p-networking	ピアツーピア ネットワーキング関連のアプリケーションです。
remote-access-terminal	リモート アクセス端末関連のアプリケーションです。
rich-media-http-content	リッチ メディア HTTP コンテンツ関連のアプリケーションです。
routing-protocol	ルーティング プロトコル関連のアプリケーションです。
storage	ストレージ関連のアプリケーションです。
streaming	ストリーミング関連のアプリケーションです。
terminal	端末関連のアプリケーションです。
tunneling-protocols	トンネリング プロトコル関連のアプリケーションです。
voice-video-chat-collaboration	音声/ビデオ チャット コラボレーション関連のアプリケーションです。

例

次に、クライアント/サーバ アプリケーションを一致基準として設定する例を示します。

```
Router(config)# class-map newmap
Router(config-cmap)# match protocol attribute sub-category client-server
```

関連コマンド

Command	Description
match protocol attribute category	指定したアプリケーション カテゴリの一致基準を設定します。

match protocol attribute encrypted

暗号化に基づいてクラス マップの一致基準を設定するには、クラス マップ コンフィギュレーション モードで **matchprotocol attributeencrypted** コマンドを使用します。暗号化の一致基準をクラス マップから削除するには、このコマンドの **no** 形式を使用します。

match protocol attribute encrypted {**encrypted-no**|**encrypted-unassigned**|**encrypted-yes**} [*application-name*]
no match protocol attribute encrypted {**encrypted-no**|**encrypted-unassigned**|**encrypted-yes**}

構文の説明

encrypted-no	暗号化のないアプリケーションを指定します。
encrypted-unassigned	暗号化されたネットワーキング プロトコル アプリケーション タグのないアプリケーションを指定します。
encrypted-yes	暗号化されたアプリケーションを指定します。
application-name	（任意）アプリケーションの名前です。アプリケーション名を指定すると、グループ内のすべてのアプリケーションではなく、指定した暗号化ステータスのそのアプリケーションが一致基準として設定されます。

コマンド デフォルト

一致基準は設定されていません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.4S	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 マップにはトラフィック クラスが含まれています。トラフィック クラスには、暗号化に基づいてパケットを照合する（およびグループにまとめる）ために使用できる、1 つ以上の **match** コマンドが含まれています。複数のトラフィック クラスを作成できます。

例

次に、暗号化を一致基準としてクラス マップを指定する例を示します。

```
Router(config)# class-map my-class
Router(config-cmap)# match protocol attribute encrypted encrypted-no ayiya-ipv6-tunneled

Router(config)# class-map my-class
Router(config-cmap)# match protocol attribute encrypted encrypted-unassigned aurora-cmgr

Router(config)# class-map my-class
Router(config-cmap)# match protocol attribute encrypted encrypted-yes citrix
```

関連コマンド

Command	Description
matchprotocol(NBAR)	NBAR が認識するプロトコル タイプにより、トラフィックを照合するように NBAR を設定します。

match protocol attribute tunnel

トンネリングに基づいてクラスマップの一致基準を設定するには、クラスマップ コンフィギュレーション モードで **matchprotocol attributetunnel** コマンドを使用します。トンネリングの一致基準をクラス マップから削除するには、このコマンドの **no** 形式を使用します。

match protocol attribute tunnel {**tunnel-no|tunnel-unassigned|tunnel-yes**} [*application-name*]
no match protocol attribute tunnel {**tunnel-no|tunnel-unassigned|tunnel-yes**} [*application-name*]

構文の説明

tunnel-no	トンネリングのないアプリケーションを指定します。
tunnel-unassigned	未割り当てのトンネリングされたアプリケーションを指定します。
tunnel-yes	トンネリングされたアプリケーションを指定します。
application-name	（任意）アプリケーションの名前です。アプリケーション名を指定すると、トンネリング グループ内のすべてのアプリケーションではなく、指定したトンネリング ステータスのそのアプリケーションが一致基準として設定されます。

コマンド デフォルト

一致基準は設定されていません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.4S	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 マップにはトラフィック クラスが含まれています。トラフィック クラスには、トンネリングに基づいてパケットを照合する（およびグループにまとめる）ために使用できる、1 つ以上の **match** コマンドが含まれています。複数のトラフィック クラスを作成できます。

例

次に、トンネリングを一致基準としてクラス マップを指定する例を示します。

```
Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute tunnel tunnel-no agentx

Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute tunnel tunnel-unassigned aris

Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute tunnel tunnel-yes rsvp_tunnel
```

関連コマンド

Command	Description
matchprotocol(NBAR)	NBAR が認識するプロトコル タイプにより、トラフィックを照合するように NBAR を設定します。

match protocol (NBAR)

Network-Based Application Recognition（NBAR）が認識するプロトコル タイプによりトラフィックを照合するように NBAR を設定するには、クラス マップ コンフィギュレーション モードで **matchprotocol** コマンドを使用します。NBAR による、既知のプロトコル タイプによるトラフィックの照合を無効にするには、このコマンドの **no** 形式を使用します。

match protocol *protocol-name* [*variable-field-name value*]
no match protocol *protocol-name* [*variable-field-name value*]

構文の説明

protocol-name	NBAR が認識する特定のプロトコル タイプです。これらの既知のプロトコル タイプを使用してトラフィックを照合できます。NBAR が認識するプロトコル タイプのリストについては、下記の「使用上のガイドライン」の表を参照してください。
variable-field-name	（任意。カスタムプロトコルでのみ使用可能）カスタムプロトコルを作成したときに作成された定義済みの変数です。*variable-field-name* 引数の値は、**ipnbarcustom** コマンドを使用してカスタムプロトコルを作成したときに入力した *field-name* 変数と照合されます。
value	（任意。カスタムプロトコルでのみ使用可能）照合するカスタムペイロードの特定の値です。*variable-field-name* 引数の値と併用する場合にのみ、値を入力できます。この値は、10 進数または 16 進数の形式で表すことができます。

コマンド デフォルト

NBAR が認識するプロトコル タイプによりトラフィックが照合されません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合され、*variable-field-namevalue* 引数が追加されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.1(13)T	このコマンドが、FlexWAN モジュールを備えていない Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。

リリース	変更箇所
12.4(2)T	このコマンドが、BitTorrentプロトコルなどの追加プロトコルのサポートを含むように変更されました。
12.4(4)T	このコマンドが、SkypeプロトコルやDirectConnectプロトコルなどの追加プロトコルのサポートを含むように変更されました。
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。
12.2(18)ZY	このコマンドが、Cisco IOS Release 12.2(18)ZY に統合されました。このコマンドが、Supervisor 32/Programmable Intelligent Services Accelerator（PISA）エンジンが搭載された Catalyst 6500 シリーズ スイッチの NBAR 機能を拡張するため、変更されました。
12.2(18)ZYA	Supervisor 32/PISA エンジンが搭載された Catalyst 6500 シリーズ スイッチで NBAR とファイアウォール サービス モジュール（FWSM）機能を統合し、以下の「使用上のガイドライン」の表に記載されている追加プロトコルを認識するように、このコマンドが変更されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。
12.2(18)ZYA1	以下の「使用上のガイドライン」の表に記載されている追加プロトコルを認識するように、このコマンドが変更されました。
Cisco IOS XE リリース 2.3	以下の「使用上のガイドライン」の表に記載されている追加プロトコルを認識するように、このコマンドが変更されました。
12.2(18)ZYA2	このコマンドが、TelePresence プロトコルなどの追加プロトコルを認識するように変更されました。
Cisco IOS XE Release 2.5	以下の「使用上のガイドライン」の表に記載されている追加プロトコルを認識するように、このコマンドが変更されました。
12.2XN	以下の「使用上のガイドライン」の表に記載されている追加プロトコルを認識するように、このコマンドが変更されました。
12.4(24)T	以下の「使用上のガイドライン」の表に記載されている追加プロトコルを認識するように、このコマンドが変更されました。
12.4(24)MDA	以下の「使用上のガイドライン」の表に記載されている追加プロトコルを認識するように、このコマンドが変更されました。
Cisco IOS XE リリース 3.4S	以下の「使用上のガイドライン」の表に記載されている追加プロトコルを認識するように、このコマンドが変更されました。
15.1(3)S	このコマンドが変更されました。Cisco 7200 シリーズ ルータからサポートが削除されました。

使用上のガイドライン

matchprotocol(NBAR) コマンドを使用して、NBAR が認識するプロトコル タイプを照合します。NBAR には、次のタイプのプロトコルを分類する機能があります。

- 非 UDP および非 TCP IP プロトコル
- スタティックに割り当てられたポート番号を使用する TCP および UDP プロトコル
- スタティックに割り当てられたポート番号を使用し、さらにステートフルインスペクションを必須とする TCP および UDP プロトコル
- ダイナミックに割り当てられたポート番号を使用するため、ステートフルインスペクションを必須とする TCP および UDP プロトコル

以下の表に、Cisco IOS ソフトウェアに使用できる NBAR 対応プロトコルをカテゴリ順に示します。この表には、プロトコル タイプ、ウェルノウン ポート番号（該当する場合）、および NBAR でプロトコルを入力するための構文に関する情報も記載されています。この表は、新しいプロトコルが追加されたときや、異なるリリースによりサポートされたときに変更されます。

（注） 以下の表に、12.2(18)ZY および 12.2(18)ZYA リリースに使用できる NBAR 対応プロトコルを示します。12.2(18)ZY および 12.2(18)ZYA リリースは、Supervisor 32/PISA エンジンを搭載する Catalyst 6500 シリーズ スイッチでサポートされます。

表 *15 : NBAR* がサポートするプロトコル

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
エンタープライズアプリケーション	Novadigm	TCP/ UDP	3460 ～ 3465	Novadigm Enterprise Desktop Manager（EDM）	novadigm
	Citrix（ICA、CGP、IMA、SB）	TCP/ UDP	TCP：1494、2512、2513、2598 UDP：1604	Citrix ICA トラフィック	citrix citrix app citrix ica-tag
	Oracle	TCP	1525	Oracle	ora-srv
	PCAnywhere	TCP/UDP	TCP：5631、65301 UDP：22、5632	Symantic PCAnywhere	pcanywhere
	SAP	TCP	3300 ～ 3315 3200 ～ 3215 3600 ～ 3615	アプリケーションサーバからアプリケーション サーバへのトラフィック（sap-pgm.pdlm） クライアントからアプリケーションサーバへのトラフィック（sap-app.pdlm） クライアントからメッセージ サーバへのトラフィック（sap-msg.pdlm）	sap
	Exchange [1]	TCP	135	MS-RPC for Exchange	exchange

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ルーティング プロトコル	BGP	TCP/ UDP	179	Border Gateway Protocol; ボーダー ゲートウェイ プロトコル	bgp
	EGP	IP	8	エクステリア ゲートウェイ プロトコル	egp
	EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp
	OSPF	IP	89	Open Shortest Path First	ospf
	RIP	UDP	520	Routing Information Protocol	rip
データベース	CIFS	TCP	139、445	Common Internet File System	cifs
	MS-SQLServer	TCP	1433	Microsoft SQL Server Desktop Videoconferencing	sqlserver
	SQL-exec	TCP/UDP	9088	SQL Exec	sqlexec
	SQL*NET	TCP/ UDP	1521	SQL*NET for Oracle	sqlnet
金融	FIX	TCP	ヒューリスティック	Financial Information Exchange	fix

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
セキュリティとトンネリング	GRE	IP	47	総称ルーティングカプセル化	gre
IPINIP	IP	4	IP in IP	ipinip	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
IPsec	IP/TCP	50、51 TCP ヒューリスティック	IP Encapsulating Security Payload/Authentication-Header	ipsec	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
L2TP	UDP	1701	L2F/L2TP Tunnel	l2tp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
PPTP	TCP	1723	Point-to-Point Tunneling Protocol for VPN	pptp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
SFTP	TCP	990	セキュア FTP	secure-ftp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
SHTTP	TCP	443	Secure HTTP; セキュア HTTP	secure-http	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3
STELNET	TCP	992	セキュア Telnet	secure-telnet	Cisco IOS XE リリース 2.3

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	SIMAP	TCP/ UDP	585、993	セキュア Internet Message Access Protocol	secure-imap
	SIRC	TCP/ UDP	994	セキュア インターネット リレー チャット	secure-irc
	SLDAP	TCP/ UDP	636	セキュア Lightweight Directory Access Protocol	secure-ldap
	SNNTP	TCP/ UDP	563	セキュア Network News Transfer Protocol	secure-nntp
	SOCKS	TCP	1080	Firewall Security Protocol	socks
	SPOP3	TCP/ UDP	995	Secure POP3	secure-pop3
	SSH	TCP	22	Secured Shell	ssh
	STELNET	TCP	992	セキュア Telnet	secure-telnet

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ネットワーク管理	ICMP	IP	1	Internet Control Message Protocol; インターネット制御メッセージ プロトコル	icmp
	SNMP	TCP/ UDP	161、162	簡易ネットワーク管理プロトコル	snmp
	Syslog	UDP	514	System Logging Utility	syslog
ネットワーク メール サービス	IMAP	TCP/ UDP	143、220	Internet Message Access Protocol	imap
	Notes	TCP/ UDP	1352	Lotus Notes	notes
	POP3	TCP/ UDP	110、ヒューリスティック	Post Office Protocol	pop3
	SMTP	TCP	25、ヒューリスティック	Simple Mail Transfer Protocol	smtp

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ディレクトリ	DHCP/ BOOTP	UDP	67、68	Dynamic Host Configuration Protocol/Bootstrap Protocol	dhcp
	DNS	TCP/ UDP	53	ドメイン ネーム システム	dns
	Finger	TCP	79	Finger User Information Protocol	finger
	Kerberos	TCP/ UDP	88、749	Kerberos Network Authentication Service	kerberos
	LDAP	TCP/ UDP	389	Lightweight Directory Access Protocol	ldap

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
インターネット	FTP	TCP	21、21000、ヒューリスティック	ファイル転送プログラム	FTP
	Gopher	TCP/ UDP	70	Internet Gopher Protocol	gopher
	HTTP	TCP	80[2]、 ヒューリスティック	ハイパーテキスト転送プロトコル	http
	IRC	TCP/ UDP	194	インターネット リレー チャット	irc
	NNTP	TCP/ UDP	119、ヒューリスティック	Network News Transfer Protocol	nntp
	Telnet	TCP	23	Telnet Protocol	telnet
	TFTP	UDP	69	トリビアル ファイル転送プロトコル	tftp
シグナリング	AppleQTC	TCP/UDP	458	Apple Quick Time	appleqtc

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Chargen	TCP/UDP	19	キャラクタ ジェネレータ	chargen	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
ClearCase	TCP/UDP	371	Clear Case Protocol Software Informer	clearcase	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
Corba	TCP/UDP	683、684	Corba Internet Inter-Orb Protocol（IIOP）	corba-iiop	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
Daytime	TCP/UDP	13	Daytime Protocol	daytime	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
Doom	TCP/UDP	666	Doom	doom	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
Echo	TCP/UDP	7	Echo Protocol	echo	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
IBM DB2	TCP/UDP	523	IBM Information Management	ibm-db2	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
IPX	TCP/UDP	213	Internet Packet Exchange	server-ipx	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
ISAKMP	TCP/UDP	500	Internet Security Association and Key Management Protocol	isakmp	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
ISI-GL	TCP/UDP	55	Interoperable Self Installation Graphics Language	isi-gl	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
			KLogin	TCP	543
KShell	TCP		544	KShell	kshell
LockD	TCP/UDP		4045	LockD	lockd
MSSQL	TCP		1433	Microsoft Structured Query Language（SQL）サーバ	mssql
RSVP	IP/UDP		IP：46 UDP：1698、1699	リソース予約プロトコル	rsvp
RPC	AOL-messenger	TCP	5190、443	AOL Instant Messenger Chat Messages	aol-messenger
	NFS	TCP/UDP	2049	ネットワーク ファイル システム	nfs
	Sunrpc	TCP/ UDP	111、ヒューリスティック	Sun Remote Procedure Call	sunrpc

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
非 IP および LAN/レガシー	NetBIOS	TCP/ UDP	TCP-137、138 UDP-137、139	NetBIOS over IP（MS Windows）	netbios
	Nickname	TCP/UDP	43	Nickname	nicname
	NPP	TCP/UDP	92	Network Payment Protocol	npp

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
音声	Google Talk VoIP	TCP/UDP	動的に割り当て	Google Talk VoIP プロトコル	gtalk-voip
	H.323	TCP	ヒューリスティック	H.323 Teleconferencing Protocol	h323
	MSN VoIP	UDP	動的に割り当て	MSN Messenger プロトコル	msn-voip
	RTCP	TCP/ UDP	動的に割り当て	リアルタイム制御プロトコル	rtcp
	RTP	TCP/ UDP	動的に割り当て	Real-Time Transport Protocol Payload Classification	rtp
	SIP	TCP/UPD	5060	Session Initiation Protocol	sip
	STUN	UDP	動的に割り当て	Simple Traversal of UDP through NAT（STUN）	stun-nat
	Skype[3]	TCP/UDP	TCP-80、ヒューリスティック	VoIP クライアント ソフトウェア	skype
	Yahoo VoIP	TCP/UDP	動的に割り当て	Yahoo Messenger VoIP プロトコル	yahoo-voip
デスクトップ メディア	CUSeeMe	TCP/UDP	TCP：7648、7649 UDP：24032	CU-SeeMe デスクトップ ビデオ会議	cuseeme
ストリーミング メディア	RealAudio	TCP/ UDP	動的に割り当て	RealAudio Streaming Protocol	realaudio

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	RTSP	TCP	554、8554	Real Time Streaming Protocol	rtsp
	StreamWorks	UDP	動的に割り当て	Xing Technology Stream Works Audio and Video	streamwork
	VDOLive	TCP/ UDP	インスペクションを使用する場合はスタティック（7000）	VDOLive Streaming Video	vdolive
	YouTube[4]	TCP	スタティック（80）とダイナミック割り当ての両方	オンライン ビデオ共有 Web サイト	youtube
ピアツーピア ファイル共有アプリケーション	BitTorrent[5]	TCP	ヒューリスティック、または 6881 ～ 6889	BitTorrent File Transfer Traffic	bittorrent
DirectConnect	TCP	80、411 ～ 413、ヒューリスティック	Direct Connect File Transfer Traffic	directconnect	Cisco IOS XE Release 2.5
eDonkey/eMule[6]	TCP	80、4662、ヒューリスティック	eDonkey File-Sharing Application また、NBAR では eMule トラフィックは eDonkey トラフィックに分類されます。	edonkey	12.2(18)ZYA1 12.3(11)T Cisco IOS XE リリース 2.5
Encrypted Emule	TCP	ヒューリスティック	P2P ファイル共有暗号化プロトコル	encrypted-emule	Cisco IOS XE リリース 3.4S
FastTrack	—	ヒューリスティック	FastTrack トラフィック	fasttrack	12.1(12c)E 12.2(18)ZYA1 Cisco IOS XE Release 2.5
FastTrack Static	—	ヒューリスティック	FastTrack Static	fasttrack-static	Cisco IOS XE リリース 3.3S
Gnutella	TCP/UDP	ヒューリスティック、または TCP-80、6346 ～ 6349、6355、5634	Gnutella トラフィック	gnutella	Cisco IOS XE Release 2.5
Gnutella Networking	TCP/UDP	ヒューリスティック、または UDP-6346 ～ 6348	Gnutella Networking トラフィック	networking-gnutella	Cisco IOS XE リリース 3.4S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
KaZaA	TCP/ UPD	ヒューリスティック	KaZaA 以前の KaZaA バージョン 1 トラフィックは、FastTrack を使用して分類できます。	kazaa2	12.2(8)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
WinMX	TCP	6699	WinMX ピアツーピア ファイル共有	winmx	12.2(18)ZYA1 12.3(7)T Cisco IOS XE リリース 2.5
その他	3Com AMP3	TCP/UDP	629	3Com AMP3	3com-amp3
	3Com TSMUX	TCP/UDP	106	3Com TSMUX	3com-tsmux
3PC	TCP/UDP	34	Third Party Connect Protocol	3pc	Cisco IOS XE Release 3.1S
914 C/G	TCP/UDP	211	Texas Instruments 914 Terminal	914c/g	Cisco IOS XE Release 3.1S
9PFS	TCP/UDP	564	Plan 9 file service	9pfs	Cisco IOS XE Release 3.1S
ACAP	TCP/UDP	674	ACAP	acap	Cisco IOS XE Release 3.1S
ACAS	TCP/UDP	62	ACA Services	acas	Cisco IOS XE Release 3.1S
AccessBuilder	TCP/UDP	888	Access Builder	accessbuilder	Cisco IOS XE Release 3.1S
AccessNetwork	TCP/UDP	699	アクセス ネットワーク	accessnetwork	Cisco IOS XE Release 3.1S
ACP	TCP/UDP	599	Aeolon Core Protocol	acp	Cisco IOS XE Release 3.1S
ACR-NEMA	TCP/UDP	104	ACR-NEMA Digital Img	acr-nema	Cisco IOS XE Release 3.1S
AED-512	TCP/UDP	149	AED 512 Emulation service	aed-512	Cisco IOS XE Release 3.1S
Agentx	TCP/UDP	705	AgentX	agentx	Cisco IOS XE Release 3.1S
Alpes	TCP/UDP	463	Alpes	alpes	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
AMInet	TCP/UDP	2639	AMInet	aminet	Cisco IOS XE Release 3.1S
AN	TCP/UDP	107	Active Networks	an	Cisco IOS XE Release 3.1S
ANET	TCP/UDP	212	ATEXSSTR	anet	Cisco IOS XE Release 3.1S
ANSANotify	TCP/UDP	116	ANSA REX Notify	ansanotify	Cisco IOS XE Release 3.1S
ANSATrader	TCP/UDP	124	ansatrader	ansatrader	Cisco IOS XE Release 3.1S
AODV	TCP/UDP	654	AODV	aodv	Cisco IOS XE Release 3.1S
	Apertus-LDP	TCP/UDP	539	Apertus Tech Load Distribution	apertus-ldp
	AppleQTC	TCP/UDP	458	apple quick time	appleqtc
AppleQTSRVR	TCP/UDP	545	appleqtcsrvr	appleqtcsrvr	Cisco IOS XE Release 3.1S
Applix	TCP/UDP	999	Applix ac	applix	Cisco IOS XE Release 3.1S
ARCISDMS	TCP/UDP	262	arcisdms	arcisdms	Cisco IOS XE Release 3.1S
ARGUS	TCP/UDP	13	ARGUS	argus	Cisco IOS XE Release 3.1S
Ariel1	TCP/UDP	419	Ariel1	ariel1	Cisco IOS XE Release 3.1S
Ariel2	TCP/UDP	421	Ariel2	ariel2	Cisco IOS XE Release 3.1S
Ariel3	TCP/UDP	422	Ariel3	ariel3	Cisco IOS XE Release 3.1S
ARIS	TCP/UDP	104	ARIS	aris	Cisco IOS XE Release 3.1S
ARNS	TCP/UDP	384	リモートネットワークサーバシステム	arns	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ASA	TCP/UDP	386	ASA Message router object def	asa	Cisco IOS XE Release 3.1S
ASA-Appl-Proto	TCP/UDP	502	asa-appl-proto	asa-appl-proto	Cisco IOS XE Release 3.1S
ASIPRegistry	TCP/UDP	687	asipregistry	asipregistry	Cisco IOS XE Release 3.1S
ASIP-Webadmin	TCP/UDP	311	AppleShare IP WebAdmin	asip-webadmin	Cisco IOS XE Release 3.1S
AS-Servermap	TCP/UDP	449	AS Server Mapper	as-servermap	Cisco IOS XE Release 3.1S
AT-3	TCP/UDP	203	AppleTalk 未使用	at-3	Cisco IOS XE Release 3.1S
AT-5	TCP/UDP	205	AppleTalk 未使用	at-5	Cisco IOS XE Release 3.1S
AT-7	TCP/UDP	207	AppleTalk 未使用	at-7	Cisco IOS XE Release 3.1S
AT-8	TCP/UDP	208	AppleTalk 未使用	at-8	Cisco IOS XE Release 3.1S
	AT-Echo	TCP/UDP	204	AppleTalk Echo	at-echo
AT-NBP	TCP/UDP	202	AppleTalk Name Binding	at-nbp	Cisco IOS XE Release 3.1S
AT-RTMP	TCP/UDP	201	AppleTalk Routing Maintenance	at-rtmp	Cisco IOS XE Release 3.1S
AT-ZIS	TCP/UDP	206	AppleTalk Zone Information	at-zis	Cisco IOS XE Release 3.1S
Audit	TCP/UDP	182	Unisys Audit SITP	audit	Cisco IOS XE Release 3.1S
Auditd	TCP/UDP	48	デジタル監査デーモン	auditd	Cisco IOS XE Release 3.1S
Aurora-CMGR	TCP/UDP	364	Aurora CMGR	aurora-cmgr	Cisco IOS XE Release 3.1S
AURP	TCP/UDP	387	Appletalk Update-Based Routing Protocol	aurp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
AUTH	TCP/UDP	113	認証サービス（Authentication Service）	auth	Cisco IOS XE Release 3.1S
Avian	TCP/UDP	486	avian	avian	Cisco IOS XE Release 3.1S
AX25	TCP/UDP	93	AX.25 フレーム	ax25	Cisco IOS XE Release 3.1S
Banyan-RPC	TCP/UDP	567	Banyan-RPC	banyan-rpc	Cisco IOS XE Release 3.1S
Banyan-VIP	TCP/UDP	573	Banyan-VIP	banyan-vip	Cisco IOS XE Release 3.1S
BBNRCCMON	TCP/UDP	10	BBN RCC モニタリング	bbnrccmon	Cisco IOS XE Release 3.1S
BDP	TCP/UDP	581	バンドル検出プロトコル	bdp	Cisco IOS XE Release 3.1S
BFTP	TCP/UDP	152	バックグラウンドファイル転送プログラム	bftp	Cisco IOS XE Release 3.1S
BGMP	TCP/UDP	264	Border Gateway Multicast Protocol	bgmp	Cisco IOS XE Release 3.1S
BGP	TCP/UDP	179	Border Gateway Protocol; ボーダーゲートウェイプロトコル	bgp	Cisco IOS XE Release 3.1S
BGS-NSI	TCP/UDP	482	BGS-NSI	bgs-nsi	Cisco IOS XE Release 3.1S
	Bhevent	TCP/UDP	357	Bhevent	bhevent
	BHFHS	TCP/UDP	248	BHFHS	bhfhs
BHMDS	TCP/UDP	310	BHMDS	bhmds	Cisco IOS XE Release 3.1S
BL-IDM	TCP/UDP	142	Britton Lee IDM	bl-idm	Cisco IOS XE Release 3.1S
BMPP	TCP/UDP	632	BMPP	bmpp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
BNA	TCP/UDP	49	BNA	bna	Cisco IOS XE Release 3.1S
Bnet	TCP/UDP	415	BNET	bnet	Cisco IOS XE Release 3.1S
Borland-DSJ	TCP/UDP	707	Borland-dsj	borland-dsj	Cisco IOS XE Release 3.1S
BR-SAT-Mon	TCP/UDP	76	Backroom SATNET モニタリング	br-sat-mon	Cisco IOS XE Release 3.1S
Cableport-AX	TCP/UDP	282	Cable Port A/X	cableport-ax	Cisco IOS XE Release 3.1S
Cab-Protocol	TCP/UDP	595	CAB プロトコル	cab-protocol	Cisco IOS XE Release 3.1S
Cadlock	TCP/UDP	770	Cadlock	cadlock	Cisco IOS XE Release 3.1S
CAIlic	TCP/UDP	216	Computer Associates Intl License Server	CAIlic	Cisco IOS XE Release 3.1S
CBT	TCP/UDP	7	CBT	cbt	Cisco IOS XE Release 3.1S
CDC	TCP/UDP	223	Certificate Distribution Center	cdc	Cisco IOS XE Release 3.1S
CFDPTKT	TCP/UDP	120	cfdptkt	cfdptkt	Cisco IOS XE Release 3.1S
CFTP	TCP/UDP	62	CFTP	cftp	Cisco IOS XE Release 3.1S
CHAOS	TCP/UDP	16	Chaos	chaos	Cisco IOS XE Release 3.1S
CharGen	TCP/UDP	19	キャラクタ ジェネレータ	chargen	Cisco IOS XE Release 3.1S
	ChShell	TCP/UDP	562	chcmd	chshell
	Cimplex	TCP/UDP	673	Cimplex	cimplex
Cisco-FNA	TCP/UDP	130	Cisco FNATIVE	cisco-fna	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Cisco-phone[7]	UDP	5060	Cisco IP Phone および PC-Based Unified Communicator	cisco-phone	12.2(18)ZYA 12.2(18)ZYA1
Cisco-SYS	TCP/UDP	132	Cisco SYSMAINT	cisco-sys	Cisco IOS XE Release 3.1S
Cisco-TDP	TCP/UDP	711	Cisco TDP	cisco-tdp	Cisco IOS XE Release 3.1S
Cisco-TNA	TCP/UDP	131	Cisco TNATIVE	cisco-tna	Cisco IOS XE Release 3.1S
Clearcase	TCP/UDP	371	Clearcase	clearcase	Cisco IOS XE Release 3.1S
Cloanto-Net-1	TCP/UDP	356	Cloanto-net-1	cloanto-net-1	Cisco IOS XE Release 3.1S
CMIP-Agent	TCP/UDP	164	CMIP/TCP Agent	cmip-agent	Cisco IOS XE Release 3.1S
CMIP-Man	TCP/UDP	163	CMIP/TCP Manager	cmip-man	Cisco IOS XE Release 3.1S
Coauthor	TCP/UDP	1529	Oracle	coauthor	Cisco IOS XE Release 3.1S
Codaauth2	TCP/UDP	370	Codaauth2	codaauth2	Cisco IOS XE Release 3.1S
Collaborator	TCP/UDP	622	Collaborator	collaborator	Cisco IOS XE Release 3.1S
Commerce	TCP/UDP	542	Commerce	commerce	Cisco IOS XE Release 3.1S
Compaq-Peer	TCP/UDP	110	Compaq Peer Protocol	compaq-peer	Cisco IOS XE Release 3.1S
Compressnet	TCP/UDP	2	管理ユーティリティ	compressnet	Cisco IOS XE Release 3.1S
COMSCM	TCP/UDP	437	COMSCM	comscm	Cisco IOS XE Release 3.1S
CON	TCP/UDP	759	デメリット	con	Cisco IOS XE Release 3.1S
Conference	TCP/UDP	531	チャット（Chat）	conference	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	Connendp	TCP/UDP	693	Almanid 接続エンドポイント	connendp
	ContentServer	TCP/UDP	3365	Contentserver	contentserver
CoreRJD	TCP/UDP	284	Corerjd	corerjd	Cisco IOS XE Release 3.1S
Courier	TCP/UDP	530	RPC	courier	Cisco IOS XE Release 3.1S
Covia	TCP/UDP	64	Communications Integrator	covia	Cisco IOS XE Release 3.1S
CPHB	TCP/UDP	73	Computer Protocol Heart Beat	cphb	Cisco IOS XE Release 3.1S
CPNX	TCP/UDP	72	Computer Protocol Network Executive	cpnx	Cisco IOS XE Release 3.1S
Creativepartnr	TCP/UDP	455	Creativepartnr	creativepartnr	Cisco IOS XE Release 3.1S
Creativeserver	TCP/UDP	453	Creativeserver	creativeserver	Cisco IOS XE Release 3.1S
CRS	TCP/UDP	507	CRS	crs	Cisco IOS XE Release 3.1S
CRTP	TCP/UDP	126	Combat Radio Transport Protocol	crtp	Cisco IOS XE Release 3.1S
CRUDP	TCP/UDP	127	Combat Radio User Datagram	crudp	Cisco IOS XE Release 3.1S
CryptoAdmin	TCP/UDP	624	Crypto Admin	cryptoadmin	Cisco IOS XE Release 3.1S
CSI-SGWP	TCP/UDP	348	Cabletron Management Protocol	csi-sgwp	Cisco IOS XE Release 3.1S
CSNET-NS	TCP/UDP	105	Mailbox Name Nameserver	csnet-ns	Cisco IOS XE Release 3.1S
CTF	TCP/UDP	84	共通トレース機能	ctf	Cisco IOS XE Release 3.1S
CUSTIX	TCP/UDP	528	Customer Ixchange	custix	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
CVC_Hostd	TCP/UDP	442	CVC_Hostd	cvc_hostd	Cisco IOS XE Release 3.1S
Cybercash	TCP/UDP	551	Cybercash	cybercash	Cisco IOS XE Release 3.1S
Cycleserv	TCP/UDP	763	Cycleserv	cycleserv	Cisco IOS XE Release 3.1S
	Cycleserv2	TCP/UDP	772	Cycleserv2	cycleserv2
Dantz	TCP/UDP	497	Dantz	dantz	Cisco IOS XE Release 3.1S
DASP	TCP/UDP	439	Dasp	dasp	Cisco IOS XE Release 3.1S
DataSurfSRV	TCP/UDP	461	DataRamp Svr	datasurfsrv	Cisco IOS XE Release 3.1S
DataSurfSRVSec	TCP/UDP	462	DataRamp Svr svs	datasurfsrvsec	Cisco IOS XE Release 3.1S
Datex-ASN	TCP/UDP	355	datex-asn	datex-asn	Cisco IOS XE Release 3.1S
Daytime	TCP/UDP	13	Daytime（RFC 867）	daytime	Cisco IOS XE Release 3.1S
Dbase	TCP/UDP	217	dBASE Unix	dbase	Cisco IOS XE Release 3.1S
DCCP	TCP/UDP	33	データグラム輻輳制御プロトコル	dccp	Cisco IOS XE Release 3.1S
DCN-Meas	TCP/UDP	19	DCN 測定サブシステム	dcn-meas	Cisco IOS XE Release 3.1S
DCP	TCP/UDP	93	デバイス制御プロトコル	dcp	Cisco IOS XE Release 3.1S
DCTP	TCP/UDP	675	DCTP	dctp	Cisco IOS XE Release 3.1S
DDM-DFM	TCP/UDP	447	DDM 分散ファイル管理	ddm-dfm	Cisco IOS XE Release 3.1S
DDM-RDB	TCP/UDP	446	DDM リモート リレーショナルデータベースアクセス	ddm-rdb	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
DDM-SSL	TCP/UDP	448	セキュア ソケットを使用した DDM リモート DB アクセス	ddm-ssl	Cisco IOS XE Release 3.1S
DDP	TCP/UDP	37	データグラム送達プロトコル	ddp	Cisco IOS XE Release 3.1S
DDX	TCP/UDP	116	D-II データ交換	ddx	Cisco IOS XE Release 3.1S
DEC_DLM	TCP/UDP	625	dec_dlm	dec_dlm	Cisco IOS XE Release 3.1S
Decap	TCP/UDP	403	Decap	decap	Cisco IOS XE Release 3.1S
	Decauth	TCP/UDP	316	Decauth	decauth
Decbsrv	TCP/UDP	579	Decbsrv	decbsrv	Cisco IOS XE Release 3.1S
Decladebug	TCP/UDP	410	DECLadebug リモート デバッグ プロトコル	decladebug	Cisco IOS XE Release 3.1S
Decvms-sysmgt	TCP/UDP	441	Decvms-sysmgt	decvms-sysmgt	Cisco IOS XE Release 3.1S
DEI-ICDA	TCP/UDP	618	dei-icda	dei-icda	Cisco IOS XE Release 3.1S
DEOS	TCP/UDP	76	分散外部オブジェクト ストア	deos	Cisco IOS XE Release 3.1S
Device	TCP/UDP	801	Device	device	Cisco IOS XE Release 3.1S
DGP	TCP/UDP	86	異種ゲートウェイ プロトコル	dgp	Cisco IOS XE Release 3.1S
DHCP-Failover	TCP/UDP	647	DHCP フェールオーバー	dhcp-failover	Cisco IOS XE Release 3.1S
DHCP-Failover2	TCP/UDP	847	dhcp-failover2	dhcp-failover2	Cisco IOS XE Release 3.1S
DHCPv6-client	TCP/UDP	546	DHCPv6 クライアント	dhcpv6-client	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
DHCPv6-server	TCP/UDP	547	DHCPv6 サーバ	dhcpv6-server	Cisco IOS XE Release 3.1S
Dicom	TCP/UDP	ヒューリスティック	Digital Imaging and Communications in Medicine	dicom	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S
Digital-VRC	TCP/UDP	466	digital-vrc	digital-vrc	Cisco IOS XE Release 3.1S
Directplay	TCP/UDP	2234	DirectPlay	directplay	Cisco IOS XE Release 3.1S
Directplay8	TCP/UDP	6073	DirectPlay8	directplay8	Cisco IOS XE Release 3.1S
Directv-Catlg	TCP/UDP	3337	Direct TV Data Catalog	directv-catlg	Cisco IOS XE Release 3.1S
Directv-Soft	TCP/UDP	3335	Direct TV Software Updates	directv-soft	Cisco IOS XE Release 3.1S
	Directv-Tick	TCP/UDP	3336	Direct TV Tickers	directv-tick
	Directv-Web	TCP/UDP	3334	Direct TV Webcasting	directv-web
Discard	TCP/UDP	9	廃棄	discard	Cisco IOS XE Release 3.1S
Disclose	TCP/UDP	667	選挙献金開示	disclose	Cisco IOS XE Release 3.1S
Dixie	TCP/UDP	96	DIXIE プロトコル仕様	dixie	Cisco IOS XE Release 3.1S
DLS	TCP/UDP	197	Directory Location Service	dls	Cisco IOS XE Release 3.1S
DLS-Mon	TCP/UDP	198	Directory Location Service Monitor	dls-mon	Cisco IOS XE Release 3.1S
DN6-NLM-AUD	TCP/UDP	195	DNSIX Network Level Module Audit	dn6-nlm-aud	Cisco IOS XE Release 3.1S
DNA-CML	TCP/UDP	436	DNA-CML	dna-cml	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
DNS	TCP/UDP	53	ドメイン ネーム サーバ ルックアップ	dns	Cisco IOS XE Release 3.1S
DNSIX	TCP/UDP	90	DNSIX Security Attribute Token Map	dnsix	Cisco IOS XE Release 3.1S
DOOM	TCP/UDP	666	Doom Id Software	doom	Cisco IOS XE Release 3.1S
DPSI	TCP/UDP	315	DPSI	dpsi	Cisco IOS XE Release 3.1S
DSFGW	TCP/UDP	438	DSFGW	dsfgw	Cisco IOS XE Release 3.1S
DSP	TCP/UDP	33	表示支援プロトコル	dsp	Cisco IOS XE Release 3.1S
DSP3270	TCP/UDP	246	表示システム プロトコル	dsp3270	Cisco IOS XE Release 3.1S
DSR	TCP/UDP	48	動的ソースルーティング プロトコル	dsr	Cisco IOS XE Release 3.1S
DTAG-DTE-SB	TCP/UDP	352	DTAG	dtag-ste-sb	Cisco IOS XE Release 3.1S
DTK	TCP/UDP	365	DTK	dtk	Cisco IOS XE Release 3.1S
	DWR	TCP/UDP	644	DWR	dwr
Echo	TCP/UDP	7	エコー（Echo）	echo	Cisco IOS XE Release 3.1S
EGP	TCP/UDP	8	エクステリア ゲートウェイ プロトコル	egp	Cisco IOS XE Release 3.1S
EIGRP	TCP/UDP	88	Enhanced Interior Gateway Routing Protocol	eigrp	Cisco IOS XE Release 3.1S
ELCSD	TCP/UDP	704	errlog コピー/サーバ デーモン	elcsd	Cisco IOS XE Release 3.1S
EMBL-NDT	TCP/UDP	394	EMBL Nucleic Data Transfer	embl-ndt	Cisco IOS XE Release 3.1S
EMCON	TCP/UDP	18	EMCON	emcon	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
EMFIS-CNTLl	TCP/UDP	141	EMFIS Control Service	emfis-cntl	Cisco IOS XE Release 3.1S
EMFIS-Data	TCP/UDP	140	EMFIS Data Service	emfis-data	Cisco IOS XE Release 3.1S
Encap	TCP/UDP	98	カプセル化ヘッダー	encap	Cisco IOS XE Release 3.1S
Encrypted Bittorrent	TCP	ヒューリスティック	Encrypted Bittorrent	encrypted-bittorrent	Cisco IOS XE リリース 3.4S
Entomb	TCP/UDP	775	Entomb	entomb	Cisco IOS XE Release 3.1S
Entrust-AAAS	TCP/UDP	680	Entrust-aaas	entrust-aaas	Cisco IOS XE Release 3.1S
Entrust-AAMS	TCP/UDP	681	Entrust-aams	entrust-aams	Cisco IOS XE Release 3.1S
Entrust-ASH	TCP/UDP	710	Entrust Administration Service Handler	entrust-ash	Cisco IOS XE Release 3.1S
Entrust-KMSH	TCP/UDP	709	Entrust Key Management Service Handler	entrust-kmsh	Cisco IOS XE Release 3.1S
Entrust-SPS	TCP/UDP	640	entrust-sps	entrust-sps	Cisco IOS XE Release 3.1S
ERPC	TCP/UDP	121	Encore Expedited Remote Pro.Call	erpc	Cisco IOS XE Release 3.1S
ESCP-IP	TCP/UDP	621	escp-ip	escp-ip	Cisco IOS XE Release 3.1S
	ESRO-GEN	TCP/UDP	259	Efficient Short Remote Operations	esro-gen
ESRP-EMSDP	TCP/UDP	642	ESRO-EMSDP V1.3	esro-emsdp	Cisco IOS XE Release 3.1S
EtherIP	TCP/UDP	97	Ethernet-within-IP カプセル化	etherip	Cisco IOS XE Release 3.1S
Eudora-Set	TCP/UDP	592	Eudora Set	eudora-set	Cisco IOS XE Release 3.1S
EXEC	TCP/UDP	512	リモート プロセスの実行	exec	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Fatserv	TCP/UDP	347	Fatmen Server	fatserv	Cisco IOS XE Release 3.1S
FC	TCP/UDP	133	ファイバ チャネル（Fibre Channel）	fc	Cisco IOS XE Release 3.1S
FCP	TCP/UDP	510	FirstClass プロトコル	fcp	Cisco IOS XE Release 3.1S
Finger	TCP/UDP	79	Finger	finger	Cisco IOS XE Release 3.1S
FIRE	TCP/UDP	125	FIRE	fire	Cisco IOS XE Release 3.1S
FlexLM	TCP/UDP	744	Flexible License Manager	flexlm	Cisco IOS XE Release 3.1S
FLN-SPX	TCP/UDP	221	Berkeley rlogind with SPX auth	fln-spx	Cisco IOS XE Release 3.1S
FTP-Agent	TCP/UDP	574	FTP ソフトウェア エージェント システム	ftp-agent	Cisco IOS XE Release 3.1S
FTP-Data	TCP/UDP	20	ファイル転送	ftp-data	Cisco IOS XE Release 3.1S
FTPS-Data	TCP/UDP	989	ftp プロトコル、データ、TLS/SSL 上	ftps-data	Cisco IOS XE Release 3.1S
Fujitsu-Dev	TCP/UDP	747	Fujitsu Device Control	fujitsu-dev	Cisco IOS XE Release 3.1S
GACP	TCP/UDP	190	ゲートウェイ アクセス コントロール プロトコル	gacp	Cisco IOS XE Release 3.1S
GDOMAP	TCP/UDP	538	gdomap	gdomap	Cisco IOS XE Release 3.1S
Genie	TCP/UDP	402	Genie プロトコル	genie	Cisco IOS XE Release 3.1S
	Genrad-MUX	TCP/UDP	176	Genrad-mux	genrad-mux
	GGF-NCP	TCP/UDP	678	GNU Generation Foundation NCP	ggf-ncp
GGP	TCP/UDP	3	ゲートウェイ間	ggp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Ginad	TCP/UDP	634	ginad	ginad	Cisco IOS XE Release 3.1S
GMTP	TCP/UDP	100	GMTP	gmtp	Cisco IOS XE Release 3.1S
Go-Login	TCP/UDP	491	Go-login	go-login	Cisco IOS XE Release 3.1S
Gopher	TCP/UDP	70	Gopher	gopher	Cisco IOS XE Release 3.1S
Graphics	TCP/UDP	41	グラフィックス（Graphics）	graphics	Cisco IOS XE Release 3.1S
GRE	TCP/UDP	47	総称ルーティングカプセル化	gre	Cisco IOS XE Release 3.1S
Groove	TCP/UDP	2492	Groove	groove	Cisco IOS XE Release 3.1S
GSS-HTTP	TCP/UDP	488	gss-http	gss-http	Cisco IOS XE Release 3.1S
GSS-XLICEN	TCP/UDP	128	GNU Generation Foundation NCP	gss-xlicen	Cisco IOS XE Release 3.1S
GTP-User	TCP/UDP	2152	GTP-ユーザ プレーン	gtp-user	Cisco IOS XE Release 3.1S
HA-Cluster	TCP/UDP	694	ha-cluster	ha-cluster	Cisco IOS XE Release 3.1S
HAP	TCP/UDP	661	hap	hap	Cisco IOS XE Release 3.1S
Hassle	TCP/UDP	375	Hassle	hassle	Cisco IOS XE Release 3.1S
HCP-Wismar	TCP/UDP	686	ハードウェア制御プロトコル Wismar	hcp-wismar	Cisco IOS XE Release 3.1S
HDAP	TCP/UDP	263	hdap	hdap	Cisco IOS XE Release 3.1S
Hello-port	TCP/UDP	652	HELLO_PORT	hello-port	Cisco IOS XE Release 3.1S
HEMS	TCP/UDP	151	hems	hems	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	HIP	TCP/UDP	139	ホスト識別プロトコル	hip
	HL7	TCP	動的に割り当て	Health Level Seven	hl7
HMMP-IND	TCP/UDP	612	HMMP 表示	hmmp-ind	Cisco IOS XE Release 3.1S
HMMP-OP	TCP/UDP	613	HMMP 処理	hmmp-op	Cisco IOS XE Release 3.1S
HMP	TCP/UDP	20	ホスト モニタリング	hmp	Cisco IOS XE Release 3.1S
HOPOPT	TCP/UDP	0	IPv6 ホップバイホップ オプション	hopopt	Cisco IOS XE Release 3.1S
Hostname	TCP/UDP	101	NIC ホスト ネーム サーバ	hostname	Cisco IOS XE Release 3.1S
HP-Alarm-Mgr	TCP/UDP	383	HP パフォーマンス データ アラーム マネージャ	hp-alarm-mgr	Cisco IOS XE Release 3.1S
HP-Collector	TCP/UDP	381	HP パフォーマンス データ コレクター	hp-collector	Cisco IOS XE Release 3.1S
HP-Managed-Node	TCP/UDP	382	HP パフォーマンス データ 管理対象ノード	hp-managed-node	Cisco IOS XE Release 3.1S
HTTP-ALT	TCP/UDP	8080	HTTP 代替	http-alt	Cisco IOS XE Release 3.1S
HTTP-Mgmt	TCP/UDP	280	http-mgmt	http-mgmt	Cisco IOS XE Release 3.1S
HTTP-RPC-EPMAP	TCP/UDP	593	HTTP RPC Ep Map	http-rpc-epmap	Cisco IOS XE Release 3.1S
Hybrid-POP	TCP/UDP	473	Hybrid-pop	hybrid-pop	Cisco IOS XE Release 3.1S
Hyper-G	TCP/UDP	418	Hyper-g	hyper-g	Cisco IOS XE Release 3.1S
Hyperwave-ISP	TCP/UDP	692	Hyperwave-isp	hyperwave-isp	Cisco IOS XE Release 3.1S
IAFDBase	TCP/UDP	480	iafdbase	iafdbase	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
IAFServer	TCP/UDP	479	iafserver	iafserver	Cisco IOS XE Release 3.1S
IASD	TCP/UDP	432	iasd	iasd	Cisco IOS XE Release 3.1S
IATP	TCP/UDP	117	インタラクティブエージェント転送プロトコル	iatp	Cisco IOS XE Release 3.1S
IBM-App	TCP/UDP	385	IBM アプリケーション	ibm-app	Cisco IOS XE Release 3.1S
	IBM-DB2	TCP/UDP	523	IBM-DB2	ibm-db2
IBProtocol	TCP/UDP	6714	インターネット バックプレーン プロトコル	ibprotocol	Cisco IOS XE Release 3.1S
ICLCNet-Locate	TCP/UDP	886	ICL coNETion locate server	iclcnet-locate	Cisco IOS XE Release 3.1S
ICLNet_SVInfo	TCP/UDP	887	ICL coNETion server info	iclcnet_svinfo	Cisco IOS XE Release 3.1S
ICMP	TCP/UDP	1	インターネット制御メッセージ	icmp	Cisco IOS XE Release 3.1S
IDFP	TCP/UDP	549	idfp	idfp	Cisco IOS XE Release 3.1S
IDPR	TCP/UDP	35	ドメイン間ポリシー ルーティング プロトコル	idpr	Cisco IOS XE Release 3.1S
IDPRr-CMTP	TCP/UDP	38	IDPR 制御メッセージ トランスポート プロトコル	idpr-cmtp	Cisco IOS XE Release 3.1S
IDRP	TCP/UDP	45	ドメイン間ルーティング プロトコル	idrp	Cisco IOS XE Release 3.1S
IEEE-MMS	TCP/UDP	651	ieee-mms	ieee-mms	Cisco IOS XE Release 3.1S
IEEE-MMS-SSL	TCP/UDP	695	ieee-mms-ssl	ieee-mms-ssl	Cisco IOS XE Release 3.1S
IFMP	TCP/UDP	101	Ipsilon フロー管理プロトコル	ifmp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
IGRP	TCP/UDP	9	シスコ内部ゲートウェイ	igrp	Cisco IOS XE Release 3.1S
IIOP	TCP/UDP	535	iiop	iiop	Cisco IOS XE Release 3.1S
IL	TCP/UDP	40	IL トランスポートプロトコル	il	Cisco IOS XE Release 3.1S
IMSP	TCP/UDP	406	インタラクティブ メール支援プロトコル	imsp	Cisco IOS XE Release 3.1S
InBusiness	TCP/UDP	244	Inbusiness	inbusiness	Cisco IOS XE Release 3.1S
Infoseek	TCP/UDP	414	InfoSeek	infoseek	Cisco IOS XE Release 3.1S
Ingres-Net	TCP/UDP	134	INGRES-NET Service	ingres-net	Cisco IOS XE Release 3.1S
	I-NLSP	TCP/UDP	52	Integrated Net Layer Security TUBA	i-nlsp
Intecourier	TCP/UDP	495	Intecourier	intecourier	Cisco IOS XE Release 3.1S
Integra-SME	TCP/UDP	484	Integra ソフトウェア管理環境	integra-sme	Cisco IOS XE Release 3.1S
Intrinsia	TCP/UDP	503	intrinsa	intrinsa	Cisco IOS XE Release 3.1S
IPCD	TCP/UDP	576	ipcd	ipcd	Cisco IOS XE Release 3.1S
IPComp	TCP/UDP	108	IP ペイロード圧縮プロトコル	ipcomp	Cisco IOS XE Release 3.1S
IPCServer	TCP/UDP	600	Sun IPC サーバ	ipcserver	Cisco IOS XE Release 3.1S
IPCV	TCP/UDP	71	インターネットパケットコア ユーティリティ	ipcv	Cisco IOS XE Release 3.1S
IPDD	TCP/UDP	578	ipdd	ipdd	Cisco IOS XE Release 3.1S
IPINIP	TCP/UDP	4	IP in IP	ipinip	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
IPIP	TCP/UDP	94	IP-within-IP カプセル化プロトコル	ipip	Cisco IOS XE Release 3.1S
IPLT	TCP/UDP	129	IPLT	iplt	Cisco IOS XE Release 3.1S
IPP	TCP/UDP	631	インターネット印刷プロトコル	ipp	Cisco IOS XE Release 3.1S
IPPC	TCP/UDP	67	Internet Pluribus Packet Core	ippc	Cisco IOS XE Release 3.1S
Ipv6-Frag	TCP/UDP	44	Fragment Header for IPv6	ipv6-frag	Cisco IOS XE Release 3.1S
Ipv6-ICMP	TCP/UDP	58	IPv6 の ICMP	ipv6-icmp	Cisco IOS XE Release 3.1S
Ipv6INIP	TCP/UDP	41	Ipv6 encapsulated	ipv6inip	Cisco IOS XE Release 3.1S
ipv6-NonXT	TCP/UDP	59	No Next Header for IPv6	ipv6-nonxt	Cisco IOS XE Release 3.1S
	Ipv6-OPTS	TCP/UDP	60	Destination Options for IPv6	ipv6-opts
Ipv6-Route	TCP/UDP	43	Routing Header for IPv6	ipv6-route	Cisco IOS XE Release 3.1S
IRC	TCP/UDP	194	インターネット リレーチャット	irc	Cisco IOS XE Release 3.1S
IRC-SERV	TCP/UDP	529	IRC-SERV	irc-serv	Cisco IOS XE Release 3.1S
IRTP	TCP/UDP	36	インターネット高信頼性トランザクション	irtp	Cisco IOS XE Release 3.1S
IS99C	TCP/UDP	379	TIA/EIA/IS-99 モデム クライアント	is99c	Cisco IOS XE Release 3.1S
IS99S	TCP/UDP	380	TIA/EIA/IS-99 モデム サーバ	is99s	Cisco IOS XE Release 3.1S
ISAKMP	UDP	500、4500	Internet Security Association & Key Management Protocol	isakmp	Cisco IOS XE Release 3.1S
ISI-GI	TCP/UDP	55	ISI Graphics Language	isi-gl	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ISIS	TCP/UDP	124	ISIS over IPv4	isis	Cisco IOS XE Release 3.1S
ISO-ILL	TCP/UDP	499	ISO ILL プロトコル	iso-ill	Cisco IOS XE Release 3.1S
ISO-IP	TCP/UDP	147	iso-ip	iso-ip	Cisco IOS XE Release 3.1S
ISO-TP0	TCP/UDP	146	iso-tp0	iso-tp0	Cisco IOS XE Release 3.1S
ISO-TP4	TCP/UDP	29	ISO トランスポート プロトコル クラス 4	iso-tp4	Cisco IOS XE Release 3.1S
ISO-TSAP	TCP/UDP	102	ISO-TSAP クラス 0	iso-tsap	Cisco IOS XE Release 3.1S
ISO-TSAP-C2	TCP/UDP	399	ISO トランスポート クラス 2 非制御	iso-tsap-c2	Cisco IOS XE Release 3.1S
ITM-MCELL-S	TCP/UDP	828	itm-mcell-s	itm-mcell-s	Cisco IOS XE Release 3.1S
IXP-IN-IP	TCP/UDP	111	IPX in IP	ixp-in-ip	Cisco IOS XE Release 3.1S
Jargon	TCP/UDP	148	Jargon	jargon	Cisco IOS XE Release 3.1S
	Kali	TCP/UDP	2213	Kali	kali
	K-Block	TCP/UDP	287	K-block	k-block
Keyserver	TCP/UDP	584	キー サーバ	keyserver	Cisco IOS XE Release 3.1S
KIS	TCP/UDP	186	KIS プロトコル	kis	Cisco IOS XE Release 3.1S
Klogin	TCP/UDP	543	klogin	klogin	Cisco IOS XE Release 3.1S
Knet-CMP	TCP/UDP	157	KNET/VM コマンド/メッセージ プロトコル	knet-cmp	Cisco IOS XE Release 3.1S
Konspire2b	TCP/UDP	6085	Konspire2b p2p ネットワーク	Konspire2b	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Kpasswd	TCP/UDP	464	Kpasswd	kpasswd	Cisco IOS XE Release 3.1S
Kryptolan	TCP/UDP	398	Kryptolan	kryptolan	Cisco IOS XE Release 3.1S
Kshell	TCP/UDP	544	Kshell	kshell	Cisco IOS XE Release 3.1S
L2TP	TCP/UDP	1701	l2tp	l2tp	Cisco IOS XE Release 3.1S
LA-Maint	TCP/UDP	51	IMP 論理アドレス メンテナンス	la-maint	Cisco IOS XE Release 3.1S
LANServer	TCP/UDP	637	lanserver	lanserver	Cisco IOS XE Release 3.1S
LARP	TCP/UDP	91	Locus アドレス解決プロトコル	larp	Cisco IOS XE Release 3.1S
LDAP	TCP/UDP	389	Lightweight Directory Access Protocol	ldap	Cisco IOS XE Release 3.1S
LDP	TCP/UDP	646	LDP	ldp	Cisco IOS XE Release 3.1S
Leaf-1	TCP/UDP	25	Leaf-1	leaf-1	Cisco IOS XE Release 3.1S
Leaf-2	TCP/UDP	26	Leaf-2	leaf-2	Cisco IOS XE Release 3.1S
Legent-1	TCP/UDP	373	Legent Corporation	legent-1	Cisco IOS XE Release 3.1S
	Legent-2	TCP/UDP	374	Legent Corporation	legent-2
LJK-Login	TCP/UDP	472	ljk-login	ljk-login	Cisco IOS XE Release 3.1S
Lockd	TCP/UDP	4045	NFS Lock Daemon Manager	lockd	Cisco IOS XE Release 3.1S
Locus-Con	TCP/UDP	127	Locus PC-Interface Conn Server	locus-con	Cisco IOS XE Release 3.1S
Locus-Map	TCP/UDP	125	Locus PC-Interface Net Map Ser	locus-map	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
MAC-SRVR-Admin	TCP/UDP	660	MacOS Server Admin	mac-srvr-admin	Cisco IOS XE Release 3.1S
Magenta-Logic	TCP/UDP	313	Magenta-logic	magenta-logic	Cisco IOS XE Release 3.1S
Mailbox-LM	TCP/UDP	505	Mailbox-lm	mailbox-lm	Cisco IOS XE Release 3.1S
Mailq	TCP/UDP	174	MAILQ	mailq	Cisco IOS XE Release 3.1S
Maitrd	TCP/UDP	997	Maitrd	maitrd	Cisco IOS XE Release 3.1S
MANET	TCP/UDP	138	MANET プロトコル	manet	Cisco IOS XE Release 3.1S
MasqDialer	TCP/UDP	224	Masqdialer	masqdialer	Cisco IOS XE Release 3.1S
Matip-Type-A	TCP/UDP	350	MATIP Type A	matip-type-a	Cisco IOS XE Release 3.1S
Matip-Type-B	TCP/UDP	351	MATIP Type B	matip-type-b	Cisco IOS XE Release 3.1S
MCIDAS	TCP/UDP	112	McIDAS データ伝送プロトコル	mcidas	Cisco IOS XE Release 3.1S
MCNS-Sec	TCP/UDP	638	mcns-sec	mcns-sec	Cisco IOS XE Release 3.1S
MDC-Portmapper	TCP/UDP	685	mdc-portmapper	mdc-portmapper	Cisco IOS XE Release 3.1S
MeComm	TCP/UDP	668	MeComm	mecomm	Cisco IOS XE Release 3.1S
	MeRegister	TCP/UDP	669	MeRegister	meregister
Merit-INP	TCP/UDP	32	MERIT ノード間プロトコル	merit-inp	Cisco IOS XE Release 3.1S
Meta5	TCP/UDP	393	Meta5	meta5	Cisco IOS XE Release 3.1S
Metagram	TCP/UDP	99	Metagram	metagram	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Meter	TCP/UDP	570	Meter	meter	Cisco IOS XE Release 3.1S
Mfcobol	TCP/UDP	86	Micro Focus Cobol	mfcobol	Cisco IOS XE Release 3.1S
MFE-NSP	TCP/UDP	31	MFE ネットワーク サービス プロトコル	mfe-nsp	Cisco IOS XE Release 3.1S
MFTP	TCP/UDP	349	mftp	mftp	Cisco IOS XE Release 3.1S
Micom-PFS	TCP/UDP	490	Micom-pfs	micom-pfs	Cisco IOS XE Release 3.1S
MICP	TCP/UDP	95	モバイル インターネットワーキング制御プロトコル	micp	Cisco IOS XE Release 3.1S
Micromuse-LM	TCP/UDP	1534	micromuse-lm	micromuse-lm	Cisco IOS XE Release 3.1S
MIT-DOV	TCP/UDP	91	MIT Dover Spooler	mit-dov	Cisco IOS XE Release 3.1S
MIT-ML-Dev	TCP/UDP	83	MIT ML Device	mit-ml-dev	Cisco IOS XE Release 3.1S
Mobile	TCP/UDP	55	IP モビリティ	mobile	Cisco IOS XE Release 3.1S
モバイル IP エージェント	TCP/UDP	434	mobileip-agent	mobileip-agent	Cisco IOS XE Release 3.1S
MobilIP-MN	TCP/UDP	435	mobilip-mn	mobilip-mn	Cisco IOS XE Release 3.1S
Mondex	TCP/UDP	471	Mondex	mondex	Cisco IOS XE Release 3.1S
Monitor	TCP/UDP	561	モニタ（Monitor）	monitor	Cisco IOS XE Release 3.1S
Mortgageware	TCP/UDP	367	Mortgageware	mortgageware	Cisco IOS XE Release 3.1S
	MPLS-IN-IP	TCP/UDP	137	MPLS-in-IP	mpls-in-ip
MPM	TCP/UDP	45	メッセージ処理モジュール	mpm	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
MPM-Flags	TCP/UDP	44	MPM FLAGS プロトコル	mpm-flags	Cisco IOS XE Release 3.1S
MPM-SND	TCP/UDP	46	MPM [default send]	mpm-snd	Cisco IOS XE Release 3.1S
MPP	TCP/UDP	218	Netix メッセージ投稿プロトコル	mpp	Cisco IOS XE Release 3.1S
MPTN	TCP/UDP	397	Multi Protocol Transport Network	mptn	Cisco IOS XE Release 3.1S
MRM	TCP/UDP	679	mrm	mrm	Cisco IOS XE Release 3.1S
MSDP	TCP/UDP	639	msdp	msdp	Cisco IOS XE Release 3.1S
MSExch-Routing	TCP/UDP	691	MS Exchange ルーティング	msexch-routing	Cisco IOS XE Release 3.1S
MSFT-GC	TCP/UDP	3268	Microsoft グローバル カタログ	msft-gc	Cisco IOS XE Release 3.1S
MSFT-GC-SSL	TCP/UDP	3269	LDAP/SSL を使用した Microsoft グローバル カタログ	msft-gc-ssl	Cisco IOS XE Release 3.1S
MSG-AUTH	TCP/UDP	31	msg-auth	msg-auth	Cisco IOS XE Release 3.1S
MSG-ICP	TCP/UDP	29	msg-icp	msg-icp	Cisco IOS XE Release 3.1S
MSNP	TCP/UDP	1863	msnp	msnp	Cisco IOS XE Release 3.1S
MS-OLAP	TCP/UDP	2393	Microsoft OLAP	ms-olap	Cisco IOS XE Release 3.1S
MSP	TCP/UDP	18	Message Send Protocol	msp	Cisco IOS XE Release 3.1S
MS-Rome	TCP/UDP	569	Microsoft rome	ms-rome	Cisco IOS XE Release 3.1S
MS-Shuttle	TCP/UDP	568	Microsoft shuttle	ms-shuttle	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
MS-SQLl-M	TCP/UDP	1434	Microsoft-SQL-Monitor	ms-sql-m	Cisco IOS XE Release 3.1S
	MS-wbt	TCP	3389/ヒューリスティック	Microsoft Windows ベース Terminal Services	ms-wbt
	MTP	TCP/UDP	92	マルチキャスト トランスポート プロトコル	mtp
Multiling-HTTP	TCP/UDP	777	Multiling HTTP	multiling-http	Cisco IOS XE Release 3.1S
Multiplex	TCP/UDP	171	Network Innovations Multiplex	multiplex	Cisco IOS XE Release 3.1S
Mumps	TCP/UDP	188	Plus Fives MUMPS	mumps	Cisco IOS XE Release 3.1S
MUX	TCP/UDP	18	多重化	mux	Cisco IOS XE Release 3.1S
Mylex-MAPD	TCP/UDP	467	mylex-mapd	mylex-mapd	Cisco IOS XE Release 3.1S
MySQL	TCP/UDP	3306	MySQL	mysql	Cisco IOS XE Release 3.1S
Name	TCP/UDP	54	ホスト ネーム サーバ	name	Cisco IOS XE Release 3.1S
NAMP	TCP/UDP	167	namp	namp	Cisco IOS XE Release 3.1S
NARP	TCP/UDP	54	NBMA アドレス解決プロトコル	narp	Cisco IOS XE Release 3.1S
NAS	TCP/UDP	991	ネットニュース管理システム	nas	Cisco IOS XE Release 3.1S
NCED	TCP/UDP	404	nced	nced	Cisco IOS XE Release 3.1S
NCLD	TCP/UDP	405	ncld	ncld	Cisco IOS XE Release 3.1S
NCP	TCP/UDP	524	NCP	ncp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
NDSAuth	TCP/UDP	353	NDSAUTH	ndsauth	Cisco IOS XE Release 3.1S
Nest-Protocol	TCP/UDP	489	Nest-protocol	nest-protocol	Cisco IOS XE Release 3.1S
Net8-CMAN	TCP/UDP	1830	Oracle Net8 CMan Admin	net8-cman	Cisco IOS XE Release 3.1S
Net-Assistant	TCP/UDP	3283	net-assistant	net-assistant	Cisco IOS XE Release 3.1S
Netblt	TCP/UDP	30	一括データ転送プロトコル	netblt	Cisco IOS XE Release 3.1S
	NetGW	TCP/UDP	741	netgw	netgw
	NetNews	TCP/UDP	532	readnews	netnews
NetRCS	TCP/UDP	742	ネットワーク ベース RCS	netrcs	Cisco IOS XE Release 3.1S
NetRJS-1	TCP/UDP	71	リモート ジョブ サービス	netrjs-1	Cisco IOS XE Release 3.1S
NetRJS-2	TCP/UDP	72	リモート ジョブ サービス	netrjs-2	Cisco IOS XE Release 3.1S
NetRJS-3	TCP/UDP	73	リモート ジョブ サービス	netrjs-3	Cisco IOS XE Release 3.1S
NetRJS-4	TCP/UDP	74	リモート ジョブ サービス	netrjs-4	Cisco IOS XE Release 3.1S
NETSC-Dev	TCP/UDP	155	NETSC	netsc-dev	Cisco IOS XE Release 3.1S
NETSC-Prod	TCP/UDP	154	NETSC	netsc-prod	Cisco IOS XE Release 3.1S
NetViewDM1	TCP/UDP	729	IBM NetView M	netviewdm1	Cisco IOS XE Release 3.1S
NetviewDM2	TCP/UDP	730	IBM NetView DM	netviewdm2	Cisco IOS XE Release 3.1S
NetviewDM3	TCP/UDP	731	IBM NetView DM	netviewdm3	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Netwall	TCP/UDP	533	緊急放送向け	netwall	Cisco IOS XE Release 3.1S
Netware-IP	TCP/UDP	396	Novell Netware over IP	netware-ip	Cisco IOS XE Release 3.1S
New-RWHO	TCP/UDP	550	new who	new-rwho	Cisco IOS XE Release 3.1S
NextStep	TCP/UDP	178	NextStep Window Server	nextstep	Cisco IOS XE Release 3.1S
NFS	TCP/UDP	2049	ネットワーク ファイル システム	nfs	Cisco IOS XE Release 3.1S
NicName	TCP/UDP	43	Who Is	nicname	Cisco IOS XE Release 3.1S
NI-FTP	TCP/UDP	47	NI FTP	ni-ftp	Cisco IOS XE Release 3.1S
NI-Mail	TCP/UDP	61	NI MAIL	ni-mail	Cisco IOS XE Release 3.1S
	Nlogin	TCP/UDP	758	nlogin	nlogin
	NMAP	TCP/UDP	689	nmap	nmap
NMSP（NMSP）	TCP/UDP	537	ネットワーク メディア ストリーミング プロトコル	nmsp	Cisco IOS XE Release 3.1S
NNSP	TCP/UDP	433	nnsp	nnsp	Cisco IOS XE Release 3.1S
Notes	TCP/UDP	1352	Lotus Notes(R)	notes	Cisco IOS XE Release 3.1S
NovaStorBakcup	TCP/UDP	308	Novastor Backup	novastorbakcup	Cisco IOS XE Release 3.1S
NPMP-GUI	TCP/UDP	611	npmp-gui	npmp-gui	Cisco IOS XE Release 3.1S
NPMP-Local	TCP/UDP	610	npmp-local	npmp-local	Cisco IOS XE Release 3.1S
NPMP-Trap	TCP/UDP	609	npmp-trap	npmp-trap	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
NPP	TCP/UDP	92	ネットワーク印刷プロトコル	npp	Cisco IOS XE Release 3.1S
NQS	TCP/UDP	607	nqs	nqs	Cisco IOS XE Release 3.1S
NS	TCP/UDP	760	ns	ns	Cisco IOS XE Release 3.1S
NSFNET-IGP	TCP/UDP	85	NSFNET-IGP	nsfnet-igp	Cisco IOS XE Release 3.1S
NSIIOPS	TCP/UDP	261	IIOP Name Service over TLS/SSL	nsiiops	Cisco IOS XE Release 3.1S
NSRMP	TCP/UDP	359	ネットワーク セキュリティ リスク マネジメント プロトコル	nsrmp	Cisco IOS XE Release 3.1S
NSS-Routing	TCP/UDP	159	NSS-Routing	nss-routing	Cisco IOS XE Release 3.1S
NSW-FE	TCP/UDP	27	NSW User System FE	nsw-fe	Cisco IOS XE Release 3.1S
Ntalk	TCP/UDP	518	Ntalk	ntalk	Cisco IOS XE Release 3.1S
NTP	TCP/ UDP	123	ネットワーク タイム プロトコル	ntp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S
	NVP-II	TCP/UDP	11	ネットワーク音声プロトコル	nvp-ii
NXEdit	TCP/UDP	126	nxedit	nxedit	Cisco IOS XE Release 3.1S
OBCBinder	TCP/UDP	183	ocbinder	ocbinder	Cisco IOS XE Release 3.1S
OBEX	TCP/UDP	650	obex	obex	Cisco IOS XE Release 3.1S
ObjCall	TCP/UDP	94	Tivoli Object Dispatcher	objcall	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
OCS_AMU	TCP/UDP	429	ocs_amu	ocs_amu	Cisco IOS XE Release 3.1S
OCS_CMU	TCP/UDP	428	ocs_cmu	ocs_cmu	Cisco IOS XE Release 3.1S
OCServer	TCP/UDP	184	ocserver	ocserver	Cisco IOS XE Release 3.1S
ODMR	TCP/UDP	366	odmr	odmr	Cisco IOS XE Release 3.1S
OHIMSRV	TCP/UDP	506	ohimsrv	ohimsrv	Cisco IOS XE Release 3.1S
OLSR	TCP/UDP	698	olsr	olsr	Cisco IOS XE Release 3.1S
OMGInitialRefs	TCP/UDP	900	omginitialrefs	omginitialrefs	Cisco IOS XE Release 3.1S
OMServ	TCP/UDP	764	omserv	omserv	Cisco IOS XE Release 3.1S
ONMUX	TCP/UDP	417	onmux	onmux	Cisco IOS XE Release 3.1S
Opalis-RDV	TCP/UDP	536	Opalis-rdv	opalis-rdv	Cisco IOS XE Release 3.1S
Opalis-Robot	TCP/UDP	314	oOpalis-robot	opalis-robot	Cisco IOS XE Release 3.1S
OPC-Job-Start	TCP/UDP	423	IBM Operations Planning and Control Start	opc-job-start	Cisco IOS XE Release 3.1S
OPC-Job-Track	TCP/UDP	424	IBM Operations Planning and Control Track	opc-job-track	Cisco IOS XE Release 3.1S
	Openport	TCP/UDP	260	Openport	openport
OpenVMS-Sysipc	TCP/UDP	557	Openvms-sysipc	openvms-sysipc	Cisco IOS XE Release 3.1S
OracleNames	TCP/UDP	1575	Oraclenames	oraclenames	Cisco IOS XE Release 3.1S
OracleNet8CMAN	TCP/UDP	1630	Oracle Net8 Cman	oraclenet8cman	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ORA-Srv	TCP/UDP	1525	Oracle TCP/IP Listener	ora-srv	12.2(18)ZYA 12.2(18)ZYA Cisco IOS XE Release 3.1S
Orbix-Config	TCP/UDP	3076	Orbix 2000 Config	orbix-config	Cisco IOS XE Release 3.1S
Orbix-Locator	TCP/UDP	3075	Orbix 2000 Locator	orbix-locator	Cisco IOS XE Release 3.1S
Orbix-Loc-SSL	TCP/UDP	3077	Orbix 2000 Locator SSL	orbix-loc-ssl	Cisco IOS XE Release 3.1S
OSPF	TCP/UDP	89	Open Shortest Path First	ospf	Cisco IOS XE Release 3.1S
OSU-NMS	TCP/UDP	192	OSUネットワーク モニタリング システム	osu-nms	Cisco IOS XE Release 3.1S
Parsec-Game	TCP/UDP	6582	Parsec Gameserver	parsec-game	Cisco IOS XE Release 3.1S
Passgo	TCP/UDP	511	Passgo	passgo	Cisco IOS XE Release 3.1S
Passgo-Tivoli	TCP/UDP	627	Passgo-tivoli	passgo-tivoli	Cisco IOS XE Release 3.1S
Password-Chg	TCP/UDP	586	パスワードの変更	password-chg	Cisco IOS XE Release 3.1S
Pawserv	TCP/UDP	345	Perf Analysis Workbench	pawserv	Cisco IOS XE Release 3.1S
PCMail-SRV	TCP/UDP	158	PCMail サーバ	pcmail-srv	Cisco IOS XE Release 3.1S
PDAP	TCP/UDP	344	Prosperoデータ アクセス プロトコル	pdap	Cisco IOS XE Release 3.1S
Personal-link	TCP/UDP	281	Personal-link	personal-link	Cisco IOS XE Release 3.1S
PFTP	TCP/UDP	662	パラレル ファイル転送プロトコル	pftp	Cisco IOS XE Release 3.1S
	PGM	TCP/UDP	113	PGM 高信頼性トランスポート プロトコル	pgm

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Philips-VC	TCP/UDP	583	Philips ビデオ会議	philips-vc	Cisco IOS XE Release 3.1S
Phonebook	TCP/UDP	767	電話	phonebook	Cisco IOS XE Release 3.1S
Photuris	TCP/UDP	468	Photuris	photuris	Cisco IOS XE Release 3.1S
PIM	TCP/UDP	103	Protocol Independent Multicast	pim	Cisco IOS XE Release 3.1S
PIM-RP-DISC	TCP/UDP	496	PIM-RP-DISC	pim-rp-disc	Cisco IOS XE Release 3.1S
PIP	TCP/UDP	1321	pip	pip	Cisco IOS XE Release 3.1S
PIPE	TCP/UDP	131	Private IP Encapsulation within IP	pipe	Cisco IOS XE Release 3.1S
PIRP	TCP/UDP	553	pirp	pirp	Cisco IOS XE Release 3.1S
PKIX-3-CA-RA	TCP/UDP	829	PKIX-3 CA/RA	pkix-3-ca-ra	Cisco IOS XE Release 3.1S
PKIX-Timestamp	TCP/UDP	318	pkix-timestamp	pkix-timestamp	Cisco IOS XE Release 3.1S
PNNI	TCP/UDP	102	PNNI over IP	pnni	Cisco IOS XE Release 3.1S
Pop2	TCP/UDP	109	Post Office Protocol（POP）Version 2	pop2	Cisco IOS XE Release 3.1S
Pop3	TCP/UDP	110、ヒューリスティック	Post Office Protocol 3	pop3	Cisco IOS XE Release 3.1S
POV-Ray	TCP/UDP	494	pov-ray	pov-ray	Cisco IOS XE Release 3.1S
Powerburst	TCP/UDP	485	Air Soft Power Burst	powerburst	Cisco IOS XE Release 3.1S
PPStream	TCP/UDP	ヒューリスティック	P2P TV アプリケーション	ppstream	Cisco IOS XE リリース 3.3S
PPTP	TCP/UDP	1723	ポイントツーポイントトンネリング プロトコル	pptp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	プリンタ	TCP/UDP	515	spooler	printer
Print-SRV	TCP/UDP	170	Network PostScript	print-srv	Cisco IOS XE Release 3.1S
PRM	TCP/UDP	21	Packet Radio Measurement	prm	Cisco IOS XE Release 3.1S
PRM-NM	TCP/UDP	409	Prospero Resource Manager Node Man	prm-nm	Cisco IOS XE Release 3.1S
PRM-SM	TCP/UDP	408	Prospero Resource Manager Sys.Man	prm-sm	Cisco IOS XE Release 3.1S
Profile	TCP/UDP	136	PROFILE Naming System	profile	Cisco IOS XE Release 3.1S
Prospero	TCP/UDP	191	Prosper Directory Service	prospero	Cisco IOS XE Release 3.1S
PTCNameService	TCP/UDP	597	PTC Name Service	ptcnameservice	Cisco IOS XE Release 3.1S
PTP	TCP/UDP	123	Performance Transparency Protocol	ptp	Cisco IOS XE Release 3.1S
PTP-Event	TCP/UDP	319	PTP イベント	ptp-event	Cisco IOS XE Release 3.1S
PTP-General	TCP/UDP	320	PTP General	ptp-general	Cisco IOS XE Release 3.1S
Pump	TCP/UDP	751	Pump	pump	Cisco IOS XE Release 3.1S
PUP	TCP/UDP	12	PUP	pup	Cisco IOS XE Release 3.1S
Purenoise	TCP/UDP	663	purenoise	purenoise	Cisco IOS XE Release 3.1S
PVP	TCP/UDP	75	パケットビデオプロトコル	pvp	Cisco IOS XE Release 3.1S
PWDGen	TCP/UDP	129	Password Generator Protocol	pwdgen	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
QBIKGDP	TCP/UDP	368	qbikgdp	qbikgdp	Cisco IOS XE Release 3.1S
QFT	TCP/UDP	189	Queued File Transport	qft	Cisco IOS XE Release 3.1S
QMQP	TCP/UDP	628	qmqp	qmqp	Cisco IOS XE Release 3.1S
	QMTP	TCP/UDP	209	クイック メール転送プロトコル	qmtp
	QNX	TCP/UDP	106	QNX	qnx
QoTD	TCP/UDP	17	Quote of the Day	qotd	Cisco IOS XE Release 3.1S
QRH	TCP/UDP	752	qrh	qrh	Cisco IOS XE Release 3.1S
QUOTD	TCP/UDP	762	quotad	quotad	Cisco IOS XE Release 3.1S
r-commands	TCP	動的に割り当て	rsh、rlogin、rexec	rcmd	12.0(5)XE2 12.1(1)E 12.1(5) 12.2(18)ZYA1
RAP	TCP/UDP	38	ルートアクセスプロトコル	rap	Cisco IOS XE Release 3.1S
RCMD	TCP	512–514	BSD r-コマンド	rcmd	Cisco IOS XE リリース 3.3S
RCP	TCP/UDP	469	無線制御プロトコル	rcp	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisc IOS XE Release 3.1S
RDA	TCP/UDP	630	rda	rda	Cisco IOS XE Release 3.1S
RDB-DBS-DISP	TCP/UDP	1571	Oracle リモート データベース	rdb-dbs-disp	Cisco IOS XE Release 3.1S
RDP	TCP/UDP	27	高信頼性データ プロトコル	rdp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Realm-RUSD	TCP/UDP	688	ApplianceWare 管理プロトコル	realm-rusd	Cisco IOS XE Release 3.1S
RE-Mail-CK	TCP/UDP	50	リモート メール確認プロトコル	re-mail-ck	Cisco IOS XE Release 3.1S
RemoteFS	TCP/UDP	556	rfs サーバ	remotefs	Cisco IOS XE Release 3.1S
Remote-KIS	TCP/UDP	185	Remote-kis	remote-kis	Cisco IOS XE Release 3.1S
REPCMD	TCP/UDP	641	repcmd	repcmd	Cisco IOS XE Release 3.1S
REPSCMD	TCP/UDP	653	repscmd	repscmd	Cisco IOS XE Release 3.1S
RESCAP	TCP/UDP	283	rescap	rescap	Cisco IOS XE Release 3.1S
RIP	TCP/UDP	520	Routing Information Protocol	rip	Cisco IOS XE Release 3.1S
	RIPING	TCP/UDP	521	ripng	ripng
	RIS	TCP/UDP	180	Intergraph	ris
RIS-CM	TCP/UDP	748	Russell Info Sci Calendar Manager	ris-cm	Cisco IOS XE Release 3.1S
RJE	TCP/UDP	5	リモート ジョブ エントリ	rje	Cisco IOS XE Release 3.1S
RLP	TCP/UDP	39	リソース ロケーション プロトコル	rlp	Cisco IOS XE Release 3.1S
RLZDBASE	TCP/UDP	635	rlzdbase	rlzdbase	Cisco IOS XE Release 3.1S
RMC	TCP/UDP	657	rmc	rmc	Cisco IOS XE Release 3.1S
RMIActivation	TCP/UDP	1098	rmiactivation	rmiactivation	Cisco IOS XE Release 3.1S
RMIRegistry	TCP/UDP	1099	rmiregistry	rmiregistry	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
RMonitor	TCP/UDP	560	Rmonitord	rmonitor	Cisco IOS XE Release 3.1S
RMT	TCP/UDP	411	リモート MT プロトコル	rmt	Cisco IOS XE Release 3.1S
RPC2Portmap	TCP/UDP	369	rpc2portmap	rpc2portmap	Cisco IOS XE Release 3.1S
RRH	TCP/UDP	753	rrh	rrh	Cisco IOS XE Release 3.1S
RRP	TCP/UDP	648	Registry Registrar Protocol	rrp	Cisco IOS XE Release 3.1S
RSH-SPX	TCP/UDP	222	Berkeley rshd with SPX auth	rsh-spx	Cisco IOS XE Release 3.1S
RSVD	TCP/UDP	168	rsvd	rsvd	Cisco IOS XE Release 3.1S
RSVP_Tunnel	TCP/UDP	363	rsvp_tunnel	rsvp_tunnel	Cisco IOS XE Release 3.1S
RSVP-E2E-Ignore	TCP/UDP	134	RSVP-E2E-IGNORE	rsvp-e2e-ignore	Cisco IOS XE Release 3.1S
Rsync	TCP/UDP	873	Rsync	rsync	Cisco IOS XE Release 3.1S
RTelnet	TCP/UDP	107	Remote Telnet Service	rtelnet	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisc IOS XE Release 3.1S
	RTIP	TCP/UDP	771	Real Time Streaming Protocol	rtip
RTMP	TCP	ヒューリスティック	Real Time Messaging Protocol	rtmp	Cisco IOS XE リリース 3.4S
RTSPS	TCP/UDP	322	RTSPS	rtsps	Cisco IOS XE Release 3.1S
Rushd	TCP/UDP	696	Rushd	rushd	Cisco IOS XE Release 3.1S
RVD	TCP/UDP	66	MIT リモート仮想ディスクプロトコル	rvd	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
RXE	TCP/UDP	761	rxe	rxe	Cisco IOS XE Release 3.1S
SAFT	TCP/UDP	487	saft 簡易非同期ファイル転送	saft	Cisco IOS XE Release 3.1S
Sanity	TCP/UDP	643	Sanity	sanity	Cisco IOS XE Release 3.1S
SAT-EXPAK	TCP/UDP	64	SATNET and Backroom EXPAK	sat-expak	Cisco IOS XE Release 3.1S
SAT-Mon	TCP/UDP	69	SATNET モニタリング	sat-mon	Cisco IOS XE Release 3.1S
SCC-Security	TCP/UDP	582	scc-security	scc-security	Cisco IOS XE Release 3.1S
SCC-SP	TCP/UDP	96	Semaphore Communications Sec.Pro.	scc-sp	Cisco IOS XE Release 3.1S
SCO-DTMgr	TCP/UDP	617	SCOデスクトップ管理サーバ	sco-dtmgr	Cisco IOS XE Release 3.1S
SCOHELP	TCP/UDP	457	scohelp	scohelp	Cisco IOS XE Release 3.1S
SCOI2ODialog	TCP/UDP	360	scoi2odialog	scoi2odialog	Cisco IOS XE Release 3.1S
SCO-Inetmgr	TCP/UDP	615	Internet Configuration Manager	sco-inetmgr	Cisco IOS XE Release 3.1S
SCO-SysMgr	TCP/UDP	616	SCO システム管理サーバ	sco-sysmgr	Cisco IOS XE Release 3.1S
SCO-WebsrvrMg3	TCP/UDP	598	SCO Web Server Manager 3	sco-websrvrmg3	Cisco IOS XE Release 3.1S
SCO-WebsrvrMgr	TCP/UDP	620	SCO WebServer Manager	sco-websrvrmgr	Cisco IOS XE Release 3.1S
	SCPS	TCP/UDP	105	SCPS	scps
SCTP	TCP/UDP	132	Stream Control Transmission Protocol（SCTP）	sctp	Cisco IOS XE Release 3.1S
SCX-Proxy	TCP/UDP	470	scx-proxy	scx-proxy	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
SDNSKMP	TCP/UDP	558	SDNSKMP	sdnskmp	Cisco IOS XE Release 3.1S
SDRP	TCP/UDP	54	Source Demand Routing Protocol	sdrp	Cisco IOS XE Release 3.1S
Secure-ftp	TCP/UDP	990	ftp プロトコル、制御、TLS/SSL 上	secure-ftp	Cisco IOS XE Release 3.1S
Secure-IRC	TCP/UDP	994	irc protocol over TLS	secure-irc	Cisco IOS XE Release 3.1S
Secure-LDAP	TCP/UDP	636	ldap protocol over TLS	secure-ldap	Cisco IOS XE Release 3.1S
Secure-NNTP	TCP/UDP	563	nntp protocol over TLS	secure-nntp	Cisco IOS XE Release 3.1S
Secure-Pop3	TCP/UDP	995	pop3 protocol over TLS	secure-pop3	Cisco IOS XE Release 3.1S
Secure-Telnet	TCP/UDP	992	telnet protocol over TLS	secure-telnet	Cisco IOS XE Release 3.1S
Secure-VMTP	TCP/UDP	82	SECURE-VMTP	secure-vmtp	Cisco IOS XE Release 3.1S
Semantix	TCP/UDP	361	Semantix	semantix	Cisco IOS XE Release 3.1S
Send	TCP/UDP	169	SEND	send	Cisco IOS XE Release 3.1S
Server-IPX	TCP/UDP	213	Internetwork Packet Exchange Protocol	server-ipx	Cisco IOS XE Release 3.1S
Servstat	TCP/UDP	633	サービス ステータス更新	servstat	Cisco IOS XE Release 3.1S
SET	TCP/UDP	257	機密保護電子商取引	set	Cisco IOS XE Release 3.1S
SFS-Config	TCP/UDP	452	Cray SFS config server	sfs-config	Cisco IOS XE Release 3.1S
	SFS-SMP-Net	TCP/UDP	451	Cray Network Semaphore server	sfs-smp-net
SFTP	TCP/UDP	115	簡易ファイル転送プロトコル	sftp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
SGCP	TCP/UDP	440	sgcp	sgcp	Cisco IOS XE Release 3.1S
SGMP	TCP/UDP	153	sgmp	sgmp	Cisco IOS XE Release 3.1S
SGMP-Traps	TCP/UDP	160	sgmp-traps	sgmp-traps	Cisco IOS XE Release 3.1S
Shockwave	TCP/UDP	1626	Shockwave	shockwave	Cisco IOS XE Release 3.1S
Shrinkwrap	TCP/UDP	358	Shrinkwrap	shrinkwrap	Cisco IOS XE Release 3.1S
SIAM	TCP/UDP	498	siam	siam	Cisco IOS XE Release 3.1S
SIFT-UFT	TCP/UDP	608	送信者指定型/未承諾ファイル転送	sift-uft	Cisco IOS XE Release 3.1S
SILC	TCP/UDP	706	silc	silc	Cisco IOS XE Release 3.1S
SitaraDir	TCP/UDP	2631	Sitaradir	sitaradir	Cisco IOS XE Release 3.1S
SitaraMgmt	TCP/UDP	2630	Sitaramgmt	sitaramgmt	Cisco IOS XE Release 3.1S
Sitaraserver	TCP/UDP	2629	sitaraserver	sitaraserver	Cisco IOS XE Release 3.1S
SKIP	TCP/UDP	57	SKIP	skip	Cisco IOS XE Release 3.1S
SKRONK	TCP/UDP	460	skronk	skronk	Cisco IOS XE Release 3.1S
SM	TCP/UDP	122	SM	sm	Cisco IOS XE Release 3.1S
Smakynet	TCP/UDP	122	Smakynet	smakynet	Cisco IOS XE Release 3.1S
SmartSDP	TCP/UDP	426	Smartsdp	smartsdp	Cisco IOS XE Release 3.1S
SMP	TCP/UDP	121	簡易メッセージプロトコル	smp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	SMPNameRes	TCP/UDP	901	smpnameres	smpnameres
	SMSD	TCP/UDP	596	smsd	smsd
SMSP	TCP/UDP	413	ストレージ管理サービス プロトコル	smsp	Cisco IOS XE Release 3.1S
SMUX	TCP/UDP	199	SMUX	smux	Cisco IOS XE Release 3.1S
SNAGas	TCP/UDP	108	SNA ゲートウェイ アクセス サーバ	snagas	Cisco IOS XE Release 3.1S
Snare	TCP/UDP	509	Snare	snare	Cisco IOS XE Release 3.1S
S-Net	TCP/UDP	166	Sirius Systems	s-net	Cisco IOS XE Release 3.1S
SNP	TCP/UDP	109	Sitara ネットワーク プロトコル	snp	Cisco IOS XE Release 3.1S
SNPP	TCP/UDP	444	簡易ネットワーク ページング プロトコル	snpp	Cisco IOS XE Release 3.1S
SNTP-Heartbeat	TCP/UDP	580	SNTP HEARTBEAT	sntp-heartbeat	Cisco IOS XE Release 3.1S
SoftPC	TCP/UDP	215	Insignia Solutions	softpc	Cisco IOS XE Release 3.1S
Sonar	TCP/UDP	572	Sonar	sonar	Cisco IOS XE Release 3.1S
SPMP	TCP/UDP	656	spmp	spmp	Cisco IOS XE Release 3.1S
Sprite-RPC	TCP/UDP	90	Sprite RPC プロトコル	sprite-rpc	Cisco IOS XE Release 3.1S
SPS	TCP/UDP	130	セキュア パケット シールド	sps	Cisco IOS XE Release 3.1S
SPSC	TCP/UDP	478	spsc	spsc	Cisco IOS XE Release 3.1S
SQL*Net	TCP/UDP	66	Oracle SQL*NET	sql*net	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
SQLExec	TCP/UDP	9088	SQL Informix	sqlexec	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.1S
SQL-Net	TCP/UDP	150	SQL-NET	sql-net	Cisco IOS XE Release 3.1S
	SQLServ	TCP/UDP	118	SQL サービス	sqlserv
SQLServer	TCP/UDP	1433	Microsoft-SQL-Server	sqlserver	Cisco IOS XE Release 3.1S
SRC	TCP/UDP	200	IBM System Resource Controller	src	Cisco IOS XE Release 3.1S
SRMP	TCP/UDP	193	Spider リモート モニタリング プロトコル	srmp	Cisco IOS XE Release 3.1S
SRP	TCP/UDP	119	SpectraLink 無線プロトコル	srp	Cisco IOS XE Release 3.1S
SRSSend	TCP/UDP	362	srssend	srssend	Cisco IOS XE Release 3.1S
SS7NS	TCP/UDP	477	ss7ns	ss7ns	Cisco IOS XE Release 3.1S
SSCOPMCE	TCP/UDP	128	SSCOPMCE	sscopmce	Cisco IOS XE Release 3.1S
SSH	TCP/UDP	22	セキュア シェル プロトコル	ssh	Cisco IOS XE Release 3.1S
Sshell	TCP/UDP	614	SSLshell	sshell	Cisco IOS XE Release 3.1S
SST	TCP/UDP	266	SCSI on ST	sst	Cisco IOS XE Release 3.1S
ST	TCP/UDP	5	Stream	st	Cisco IOS XE Release 3.1S
StatSRV	TCP/UDP	133	Statistics Service	statsrv	Cisco IOS XE Release 3.1S
STMF	TCP/UDP	501	stmf	stmf	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
STP	TCP/UDP	118	スケジュール転送プロトコル	stp	Cisco IOS XE Release 3.1S
StreetTalk	TCP/UDP	566	Streettalk	streettalk	Cisco IOS XE Release 3.1S
Stun-NAT	TCP/UDP	3478	STUN	stun-nat	Cisco IOS XE Release 3.1S
STX	TCP/UDP	527	Stock IXChange	stx	Cisco IOS XE Release 3.1S
Submission	TCP/UDP	587	Submission	submission	Cisco IOS XE Release 3.1S
	Subntbcst_TFTP	TCP/UDP	247	subntbcst_tftp	subntbcst_tftp
SU-MIT-TG	TCP/UDP	89	SU/MIT Telnet ゲートウェイ	su-mit-tg	Cisco IOS XE Release 3.1S
Sun-DR	TCP/UDP	665	sun-dr	sun-dr	Cisco IOS XE Release 3.1S
Sun-ND	TCP/UDP	77	SUN ND PROTOCOL-Temporary	sun-nd	Cisco IOS XE Release 3.1S
SupDup	TCP/UDP	95	SUPDUP	supdup	Cisco IOS XE Release 3.1S
Surf	TCP/UDP	1010	Surf	surf	Cisco IOS XE Release 3.1S
Sur-Meas	TCP/UDP	243	Survey Measurement	sur-meas	Cisco IOS XE Release 3.1S
Svrloc	TCP/UDP	427	Server Location	svrloc	Cisco IOS XE Release 3.1S
Swift-RVF	TCP/UDP	97	Swift リモート仮想ファイルプロトコル	swift-rvf	Cisco IOS XE Release 3.1S
Swipe	TCP/UDP	53	IP with Encryption	swipe	Cisco IOS XE Release 3.1S
Synoptics-Trap	TCP/UDP	412	Trap Convention Port	synoptics-trap	Cisco IOS XE Release 3.1S
Synotics-Broker	TCP/UDP	392	SynOptics Port Broker Port	synotics-broker	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Synotics-Relay	TCP/UDP	391	SynOptics SNMP Relay Port	synotics-relay	Cisco IOS XE Release 3.1S
Systat	TCP/UDP	11	Active Users	systat	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S
TACACS	TCP/UDP	49、65	Terminal Access Controller Access Control System	tacacs	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S
TAC News	TCP/UDP	98	TAC News	tacnews	Cisco IOS XE Release 3.1S
Talk	TCP/UDP	517	通話（Talk）	talk	Cisco IOS XE Release 3.1S
		TCF	TCP/UDP	87	TCF
TD-Replica	TCP/UDP	268	Tobit David Replica	td-replica	Cisco IOS XE Release 3.1S
TD-Service	TCP/UDP	267	Tobit David Service Layer	td-service	Cisco IOS XE Release 3.1S
Teedtap	TCP/UDP	559	Teedtap	teedtap	Cisco IOS XE Release 3.1S
Tell	TCP/UDP	754	Send	tell	Cisco IOS XE Release 3.1S
Telnet	TCP/UDP	23	Telnet	telnet	Cisco IOS XE Release 3.1S
Tempo	TCP/UDP	526	newdate	tempo	Cisco IOS XE Release 3.1S
Tenfold	TCP/UDP	658	Tenfold	tenfold	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Texar	TCP/UDP	333	Texar セキュリティ ポート	texar	Cisco IOS XE Release 3.1S
TICF-1	TCP/UDP	492	Transport Independent Convergence for FNA	ticf-1	Cisco IOS XE Release 3.1S
TICF-2	TCP/UDP	493	Transport Independent Convergence for FNA	ticf-2	Cisco IOS XE Release 3.1S
Timbuktu	TCP/UDP	407	Timbuktu	timbuktu	Cisco IOS XE Release 3.1S
Time	TCP/UDP	37	時刻（Time）	time	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisc IOS XE Release 3.1S
Timed	TCP/UDP	525	Timeserver	timed	Cisco IOS XE Release 3.1S
TINC	TCP/UDP	655	tinc	tinc	Cisco IOS XE Release 3.1S
TLISRV	TCP/UDP	1527	Oracle	tlisrv	Cisco IOS XE Release 3.1S
TLSP	TCP/UDP	72	トランスポート層セキュリティ プロトコル	tlsp	Cisco IOS XE Release 3.1S
TNETOS	TCP/UDP	377	日本電気株式会社	tnETOS	Cisco IOS XE Release 3.1S
TNS-CML	TCP/UDP	590	tns-cml	tns-cml	Cisco IOS XE Release 3.1S
TN-TL-FD1	TCP/UDP	476	tn-tl-fd1	tn-tl-fd1	Cisco IOS XE Release 3.1S
TP++	TCP/UDP	39	TP++ トランスポート プロトコル	tp++	Cisco IOS XE Release 3.1S
TPIP	TCP/UDP	594	tpip	tpip	Cisco IOS XE Release 3.1S
Trunk-1	TCP/UDP	23	Trunk-1	trunk-1	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Trunk-2	TCP/UDP	24	Trunk-2	trunk-2	Cisco IOS XE Release 3.1S
TServer	TCP/UDP	450	コンピュータ支援電気通信アプリケーション	tserver	Cisco IOS XE Release 3.1S
TTP	TCP/UDP	84	TTP	ttp	Cisco IOS XE Release 3.1S
UAAC	TCP/UDP	145	UAAC プロトコル	uaac	Cisco IOS XE Release 3.1S
UARPs	TCP/UDP	219	Unisys ARPs	uarps	Cisco IOS XE Release 3.1S
UDPLite	TCP/UDP	136	UDPLite	udplite	Cisco IOS XE Release 3.1S
UIS	TCP/UDP	390	uis	uis	Cisco IOS XE Release 3.1S
uLISTProc	TCP/UDP	372	List Processor	ulistproc	Cisco IOS XE Release 3.1S
ULP	TCP/UDP	522	ulp	ulp	Cisco IOS XE Release 3.1S
ULPNet	TCP/UDP	483	ulpnet	ulpnet	Cisco IOS XE Release 3.1S
Unidata-LDM	TCP/UDP	388	Unidata LDM	unidata-ldm	Cisco IOS XE Release 3.1S
Unify	TCP/UDP	181	Unify	unify	Cisco IOS XE Release 3.1S
UPS	TCP/UDP	401	無停電電源	ups	Cisco IOS XE Release 3.1S
	URM	TCP/UDP	606	Cray Unified Resource Manager	urm
	UTI	TCP/UDP	120	UTI	uti
Utime	TCP/UDP	519	Unixtime	utime	Cisco IOS XE Release 3.1S
UTMPCD	TCP/UDP	431	utmpcd	utmpcd	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
UTMPSD	TCP/UDP	430	utmpsd	utmpsd	Cisco IOS XE Release 3.1S
UUCP	TCP/UDP	540	uucpd	uucp	Cisco IOS XE Release 3.1S
UUCP-Path	TCP/UDP	117	UUCP Path Service	uucp-path	Cisco IOS XE Release 3.1S
UUCP-rLogin	TCP/UDP	541	uucp-rlogin	uucp-rlogin	Cisco IOS XE Release 3.1S
UUIDGEN	TCP/UDP	697	UUIDGEN	uuidgen	Cisco IOS XE Release 3.1S
VACDSM-App	TCP/UDP	671	VACDSM-APP	vacdsm-app	Cisco IOS XE Release 3.1S
VACDSM-SWS	TCP/UDP	670	VACDSM-SWS	vacdsm-sws	Cisco IOS XE Release 3.1S
VATP	TCP/UDP	690	Velazquez アプリケーション転送プロトコル	vatp	Cisco IOS XE Release 3.1S
VEMMI	TCP/UDP	575	vemmi	vemmi	Cisco IOS XE Release 3.1S
VID	TCP/UDP	769	vid	vid	Cisco IOS XE Release 3.1S
Videotex	TCP/UDP	516	videotex	videotex	Cisco IOS XE Release 3.1S
VISA	TCP/UDP	70	VISA プロトコル	visa	Cisco IOS XE Release 3.1S
VNC	TCP/UDP	5800、5900、5901	Virtual Network Computing	vnc	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
VMNet	TCP/UDP	175	vmnet	vmnet	Cisco IOS XE Release 3.1S
VMPWSCS	TCP/UDP	214	vmpwscs	vmpwscs	Cisco IOS XE Release 3.1S
VMTP	TCP/UDP	81	VMTP	vmtp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	VNAS	TCP/UDP	577	vnas	vnas
VPP	TCP/UDP	677	仮想実在プロトコル	vpp	Cisco IOS XE Release 3.1S
VPPS-QUA	TCP/UDP	672	vpps-qua	vpps-qua	Cisco IOS XE Release 3.1S
VPPS-VIA	TCP/UDP	676	vpps-via	vpps-via	Cisco IOS XE Release 3.1S
VRRP	TCP/UDP	112	Virtual Router Redundancy Protocol; 仮想ルータ冗長プロトコル	vrrp	Cisco IOS XE Release 3.1S
VSINet	TCP/UDP	996	vsinet	vsinet	Cisco IOS XE Release 3.1S
VSLMP	TCP/UDP	312	vslmp	vslmp	Cisco IOS XE Release 3.1S
WAP-Push	TCP/UDP	2948	WAP PUSH	wap-push	Cisco IOS XE Release 3.1S
WAP-Push-HTTP	TCP/UDP	4035	WAP Push OTA-HTTP port	wap-push-http	Cisco IOS XE Release 3.1S
WAP-Push-HTTPS	TCP/UDP	4036	WAP Push OTA-HTTP secure	wap-push-https	Cisco IOS XE Release 3.1S
WAP-Pushsecure	TCP/UDP	2949	WAP PUSH SECURE	wap-pushsecure	Cisco IOS XE Release 3.1S
WAP-VACL-S	TCP/UDP	9207	WAP vCal Secure	wap-vcal-s	Cisco IOS XE Release 3.1S
WAP-VCAL	TCP/UDP	9205	WAP vCal	wap-vcal	Cisco IOS XE Release 3.1S
WAP-VCARD	TCP/UDP	9204	WAP vCard	wap-vcard	Cisco IOS XE Release 3.1S
WAP-VCARD-S	TCP/UDP	9206	WAP vCard Secure	wap-vcard-s	Cisco IOS XE Release 3.1S
WAP-WSP	TCP/UDP	9200	WAP コネクションレス型セッション サービス	wap-wsp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
WAP-WSP-S	TCP/UDP	9202	WAP セキュア コネクションレス型セッションサービス	wap-wsp-s	Cisco IOS XE Release 3.1S
WAP-WSP-WTP	TCP/UDP	9201	WAP セッション サービス	wap-wsp-wtp	Cisco IOS XE Release 3.1S
WAP-WSP-WTP-S	TCP/UDP	9203	WAP セキュア セッション サービス	wap-wsp-wtp-s	Cisco IOS XE Release 3.1S
	WB-Expak	TCP/UDP	79	WIDEBAND EXPAK	wb-expak
WB-Mon	TCP/UDP	78	WIDEBAND モニタリング	wb-mon	Cisco IOS XE Release 3.1S
Webster	TCP/UDP	765	Webster	webster	Cisco IOS XE Release 3.1S
Webex Meeting	TCP	ヒューリスティック	Webex Meeting	webex-meeting	Cisco IOS XE リリース 3.4S
WhoAmI	TCP/UDP	565	whoami	whoami	Cisco IOS XE Release 3.1S
Whois++	TCP/UDP	63	whois++ サービス	whois++	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S
Windows Update	TCP	80、443、ヒューリスティック	Windows Update	windows-update	Cisco IOS XE リリース 3.4S
WorldFusion	TCP/UDP	2595	World Fusion	worldfusion	Cisco IOS XE Release 3.1S
WPGS	TCP/UDP	780	wpgs	wpgs	Cisco IOS XE Release 3.1S
WSN	TCP/UDP	74	Wang Span Network	wsn	Cisco IOS XE Release 3.1S
XAct-Backup	TCP/UDP	911	Xact-backup	xact-backup	Cisco IOS XE Release 3.1S
X-Bone-CTL	TCP/UDP	265	Xbone CTL	x-bone-ctl	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
XDMCP	TCP/UDP	177	X Display Manager Control Protocol	xdmcp	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S
XDTP	TCP/UDP	3088	拡張可能データ転送プロトコル	xdtp	Cisco IOS XE Release 3.1S
XFER	TCP/UDP	82	XFER ユーティリティ	xfer	Cisco IOS XE Release 3.1S
XNET	TCP/UDP	15	Cross Net Debugger	xnet	Cisco IOS XE Release 3.1S
XNS-Auth	TCP/UDP	72	XNS 認証	xns-auth	Cisco IOS XE Release 3.1S
XNS-CH	TCP/UDP	54	XNS Clearinghouse	xns-ch	Cisco IOS XE Release 3.1S
	XNS-Courier	TCP/UDP	165	Xerox	xns-courier
XNS-IDP	TCP/UDP	22	XEROX NS IDP	xns-idp	Cisco IOS XE Release 3.1S
XNS-Mail	TCP/UDP	58	XNS メール	xns-mail	Cisco IOS XE Release 3.1S
XNS-Time	TCP/UDP	52	XNS 時間プロトコル	xns-time	Cisco IOS XE Release 3.1S
XTP	TCP/UDP	36	XTP	xtp	Cisco IOS XE Release 3.1S
XVTTP	TCP/UDP	508	xvttp	xvttp	Cisco IOS XE Release 3.1S
XYPlex-Mux	TCP/UDP	173	Xyplex	xyplex-mux	Cisco IOS XE Release 3.1S
X Windows	TCP	6000 ～ 6003	X Window システム	xwindows	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
z39.50	TCP/UDP	210	ANSI Z39.50	z39.50	Cisco IOS XE Release 3.1S
Zannet	TCP/UDP	317	Zannet	zannet	Cisco IOS XE Release 3.1S
ZServ	TCP/UDP	346	Zebra サーバ	zserv	Cisco IOS XE Release 3.1S
AN	IP	107	Active Networks	an	Cisco IOS XE Release 3.1S
AOL-Protocol[8]		TCP	5190	America OnLine プロトコル	aol-protocol
ARGUS		IP	13	ARGUS	argus
ARIS		IP	104	ARIS	aris
AX25		IP	93	AX.25 フレーム	ax25
BBNR RCC Mon		IP	10	BBN RCC モニタリング	bbnrccmon
BLIZWOW		TCP、UDP	3724	World of Warcraft ゲーム プロトコル	blizwow
BNA		IP	49	BNA	bna
	BR-SAT-Mon	IP	76	Backroom SATNET モニタリング	br-sat-mon
	CBT	IP	7	CBT	cbt
CFTP	IP	62	CFTP	cftp	Cisco IOS XE Release 3.1S
Choas	IP	16	Chaos	chaos	Cisco IOS XE Release 3.1S
Compaq-Peer	IP	110	Compaq Peer Protocol	compaq-peer	Cisco IOS XE Release 3.1S
CPHB	IP	73	Computer Protocol Heart Beat	cphb	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
CPNX	IP	72	Computer Protocol Network Executive	cpnx	Cisco IOS XE Release 3.1S
CRTP	IP	126	Combat Radio Transport Protocol	crtp	Cisco IOS XE Release 3.1S
CRUDP	IP	127	Combat Radio User Datagram	crudp	Cisco IOS XE Release 3.1S
DCCP	IP	33	データグラム輻輳制御プロトコル	dccp	Cisco IOS XE Release 3.1S
DCN-Meas	IP	19	DCN 測定サブシステム	dcn-meas	Cisco IOS XE Release 3.1S
DDP	IP	37	データグラム送達プロトコル	ddp	Cisco IOS XE Release 3.1S
DDX	IP	116	D-II データ交換	ddx	Cisco IOS XE Release 3.1S
DGP	IP	86	異種ゲートウェイプロトコル	dgp	Cisco IOS XE Release 3.1S
DSR	IP	48	動的ソースルーティングプロトコル	dsr	Cisco IOS XE Release 3.1S
EGP	IP	8	エクステリアゲートウェイプロトコル	egp	Cisco IOS XE Release 3.1S
EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp	Cisco IOS XE Release 3.1S
EMCON	IP	18	EMCON	emcon	Cisco IOS XE Release 3.1S
Encap	IP	98	カプセル化ヘッダー	encap	15.1(3)T
EtherIP	IP	97	Ethernet-within-IP カプセル化	etherip	Cisco IOS XE Release 3.1S
	FC	IP	133	ファイバチャネル（Fibre Channel）	fc
FIRE	IP	125	FIRE	fire	Cisco IOS XE Release 3.1S
GGP	IP	3	ゲートウェイ間	ggp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
GMTP	IP	100	GMTP	gmtp	Cisco IOS XE Release 3.1S
GRE	IP	47	総称ルーティング カプセル化	gre	Cisco IOS XE Release 3.1S
HIP	IP	139	ホスト識別プロトコル	hip	Cisco IOS XE Release 3.1S
HMP	IP	20	ホスト モニタリング	hmp	Cisco IOS XE Release 3.1S
HopOpt	IP	0	IPv6 ホップバイホップ オプション	hopopt	Cisco IOS XE Release 3.1S
ICQ	TCP	80、ヒューリスティック	I seek you インスタント メッセージ プロトコル	icq	Cisco IOS XE リリース 3.3S
IATP	IP	117	インタラクティブ エージェント転送プロトコル	iatp	Cisco IOS XE Release 3.1S
ICMP	IP	1	インターネット制御メッセージ	icmp	Cisco IOS XE Release 3.1S
IDPR	IP	35	ドメイン間ポリシー ルーティング プロトコル	idpr	Cisco IOS XE Release 3.1S
IDPR-CMTP	IP	38	IDPR 制御メッセージ トランスポート プロトコル	idpr-cmtp	Cisco IOS XE Release 3.1S
IDRP	IP	45	ドメイン間ルーティング プロトコル	idrp	Cisco IOS XE Release 3.1S
IFMP	IP	101	Ipsilon フロー管理プロトコル	ifmp	Cisco IOS XE Release 3.1S
IGRP	IP	9	シスコ内部ゲートウェイ	igrp	Cisco IOS XE Release 3.1S
IL	IP	40	IL トランスポート プロトコル	il	Cisco IOS XE Release 3.1S
I-NLSP	IP	52	Integrated Net Layer Security TUBA	i-nlsp	Cisco IOS XE Release 3.1S
IMPCOMP	IP	108	IP ペイロード圧縮プロトコル	ipcomp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	IPCU	IP	71	インターネット パケット コア ユーティリティ	ipcv
IPinIP	IP	4	IP in IP	ipinip	Cisco IOS XE Release 3.1S
IPIP	IP	94	IP-within-IP カプセル化プロトコル	ipip	Cisco IOS XE Release 3.1S
IPLT	IP	129	IPLT	iplt	Cisco IOS XE Release 3.1S
IPPC	IP	67	Internet Pluribus Packet Core	ippc	Cisco IOS XE Release 3.1S
IPv6-Frag	IP	44	Fragment Header for IPv6	ipv6-frag	Cisco IOS XE Release 3.1S
IPv6-ICMP	IP	58	IPv6 の ICMP	ipv6-icmp	Cisco IOS XE Release 3.1S
IPv6INIP	IP	41	Ipv6 encapsulated	ipv6inip	Cisco IOS XE Release 3.1S
IPv6-NONXT	IP	59	No Next Header for IPv6	ipv6-nonxt	Cisco IOS XE Release 3.1S
IPv6-Opts	IP	60	Destination Options for IPv6	ipv6-opts	Cisco IOS XE Release 3.1S
IPv6-Route	IP	43	Routing Header for IPv6	ipv6-route	Cisco IOS XE Release 3.1S
IRTP	IP	36	インターネット高信頼性トランザクション	irtp	Cisco IOS XE Release 3.1S
ISIS	IP	124	ISIS over IPv4	isis	Cisco IOS XE Release 3.1S
ISO-TP4	IP	29	ISO トランスポート プロトコル クラス 4	iso-tp4	Cisco IOS XE Release 3.1S
IXP-in-IP	IP	111	IPX in IP	ixp-in-ip	Cisco IOS XE Release 3.1S
LARP	IP	91	Locus アドレス解決プロトコル	larp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Leaf-1	IP	25	Leaf-1	leaf-1	Cisco IOS XE Release 3.1S
6to4 IPv6 Tunneled	L3 Protocol	--	6to4 IPv6 Tunneled	6to4 IPv6 Tunneled	Cisco IOS XE Release 3.2S
	AYIYA IPv6 Tunneled	UDP	5072	AYIYA トラフィックに基づく IPv6 Tunneled	AYIYA IPv6 Tunneled
	BabelGum	TCP、UDP	80 + ヒューリスティック	BabelGum	BabelGum
Baidu ムービー	TCP、UDP	80 + ヒューリスティック	Baidu ムービー	Baidu ムービー	Cisco IOS XE Release 3.2S
DHCP	UDP	67、68	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	Cisco IOS XE Release 3.2S
DHT	UDP	ヒューリスティック	Distributed sloppy ハッシュテーブル プロトコル	DHT	Cisco IOS XE Release 3.2S
Filetopia	TCP	ヒューリスティック	Filetopia P2P ファイル共有	filetopia	Cisco IOS XE Release 3.2S
Fring-VoIP	UDP	ヒューリスティック	Fring VoIP	fring-voip	Cisco IOS XE リリース 3.3S
GoogleEarth	TCP	80 + ヒューリスティック	GoogleEarth	GoogleEarth	Cisco IOS XE Release 3.2S
Guruguru	TCP	ヒューリスティック	Guruguru	guruguru	Cisco IOS XE Release 3.2S
IMAP	TCP	143,220	Internet Mail Access Protocol	imap	Cisco IOS XE Release 3.2S
IRC	TCP	80 + ヒューリスティック	IRC	IRC	Cisco IOS XE Release 3.2S
ISATAP IPv6 Tunneled	L3 Protocol		Intra-Site Automatic Tunnel Addressing Protocol（ISATAP）IPv6 トンネル	ISATAP IPv6 Tunneled	Cisco IOS XE Release 3.2S
iTunes	TCP	80 + ヒューリスティック	iTunes	iTunes	Cisco IOS XE Release 3.2S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Kuro	TCP	ヒューリスティック	Kuro	kuro	Cisco IOS XE リリース 3.3S
Manolito	TCP、UDP	TCP - ヒューリスティックポート、UDP - 41170	Manolito P2P 音楽共有プロトコル	manolito	Cisco IOS XE Release 3.2S
MapleStory	TCP	ヒューリスティック	メイプルストーリーゲームプロトコル	MapleStory	Cisco IOS XE Release 3.2S
SIP	TCP、UDP	TCP/UDP - 5060 + ヒューリスティック	Session Initiation Protocol	sip	Cisco IOS XE Release 3.2S
	MGCP	TCP、UDP	UDP 2427/2727 - TCP 2427/2428/2727 + ヒューリスティック	Media Gateway Control Protocol	MGCP
Microsoft-DS	TCP、UDP	445	Microsoft-ds	microsoftds	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S
MSN Messenger	TCP	1080、1863、80、ヒューリスティック	MSN Messenger	msn-messenger	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S
MyJabber File Transfer	TCP	ヒューリスティック	MyJabber File Transfer	MyJabber File Transfer	Cisco IOS XE Release 3.2S
Napster	TCP	80 + ヒューリスティック	Napster	napster	Cisco IOS XE Release 3.2S
Netshow	TCP	1755 + ヒューリスティック	Netshow	netshow	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1
NNTP	TCP	TCP - 119 + ヒューリスティック、UDP -119	Network News Transfer Protocol	NNTP	Cisco IOS XE Release 3.2S
NTP	UDP	123	ネットワークタイムプロトコル	NTP	Cisco IOS XE Release 3.2S
Pando	TCP、UDP	TCP - 80 + ヒューリスティック、UDP - ヒューリスティック	Pando	Pando	Cisco IOS XE Release 3.2S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
POCO	TCP、UDP	ヒューリスティック	POCO ファイル共有アプリケーション	POCO	Cisco IOS XE Release 3.2S
POP3	TCP	110、ヒューリスティック	POP3	POP3	Cisco IOS XE Release 3.2S
PPTP	TCP	1723	ポイントツーポイントトンネリング プロトコル	pptp	Cisco IOS XE Release 3.2S
RADIUS	UDP	1812、1813	Remote Authentication Dial In User Service プロトコル	radius	Cisco IOS XE リリース 3.3S
	SCCP/Skinny	TCP	2000 ～ 2002	Skinny Call Control Protocol	skinny
	Soribada	TCP	TCP - 80 + ヒューリスティック、UDP - ヒューリスティック	Soribada、韓国の P2P 音楽共有プロトコル	soribada
	Soulseek	TCP	ヒューリスティック	SoulSeek インターネット ダウンロード マネージャ プロトコル	soulseek
	TeamSpeak	UDP	ヒューリスティック	TeamSpeak インターネットベース音声会議プロトコル	TeamSpeak
TelePresence	TCP/UDP	動的に割り当て	Cisco TelePresence System	telepresence-media	12.2(18)ZYA2
Telepresence-control	TCP、UDP	TCP-5060、UDP-ヒューリスティック	Telepresence-control	telepresence-control	Cisco IOS XE Release 3.2S
Teredo IPv6 Tunneled	TCP、UDP	TCP-ヒューリスティック、UDP - 3544 + ヒューリスティック	Teredo IPv6 Tunneled	teredo-ipv6-tunneled	Cisco IOS XE Release 3.2S
TFTP	UDP	69	トリビアル ファイル転送プロトコル	tftp	Cisco IOS XE Release 3.2S
TomatoPang	TCP	ヒューリスティック	TomatoPang P2P 共有プロトコル	TomatoPang	Cisco IOS XE Release 3.2S
Tunnel-HTTP	TCP	80 + ヒューリスティック	HTTP トンネリング	tunnel-http	Cisco IOS XE Release 3.2S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Ventrilo	TCP、UDP	ヒューリスティック	Ventrilo VoIP プロトコル	Ventrilo	Cisco IOS XE Release 3.2S
Waste	TCP/UDP	ヒューリスティック	Waste	waste	Cisco IOS XE リリース 3.3S
WebThunder	TCP、UDP	TCP-80、UDP-ヒューリスティック	WebThunder ピアツーピアファイル共有	WebThunder	Cisco IOS XE Release 3.2S
Yahoo-Messenger	TCP	TCP-5050/5101/1080/119/80/ヒューリスティック	Yahoo Messenger	yahoo-messenger	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S
Yahoo-Messenger-VoIP	TCP/UDP	ヒューリスティック	Yahoo Messenger VoIP	yahoo-voip-messenger	Cisco IOS XE リリース 3.3S
Yahoo VoIP over SIP	TCP/UDP	5060/ヒューリスティック	Yahoo VoIP over SIP	yahoo-voip-over-sip	Cisco IOS XE リリース 3.4S

[1] Release 12.2(18)ZYA および Cisco IOS XE Release 2.5 Cisco では、Exchange 03 および 07 のみをサポートしています。MS クライアント アクセスは認識されますが、Web クライアント アクセスは認識されません。

[2] Release 12.3(4)T では、HTTP トラフィック用の NBAR Extended Inspection 機能が導入されました。この機能を使用すると、NBAR は不明な TCP ポートをスキャンし、そのルータを通過する HTTP トラフィックを識別できます。Cisco IOS XE Release 2.1 では、URL またはホスト名による HTTP トラフィックの分類はサポートされていません。Cisco IOS XE Release 2.5 は、URL またはホスト名による HTTP トラフィックの分類をサポートしています。

[3] Cisco IOS Release 12.4(4)T で Skype が導入されました。この導入により、Skype が Cisco IOS ソフトウェアに含まれるようになり、Cisco IOS リリース 12.4(4)T の新機能である NBAR インフラストラクチャを使用するようになりました。シスコ ソフトウェアは Skype 1.0、2.5、および 3.0 をサポートしています。Cisco IOS XE Release 2.1 では、Skype は TCP タイプでのみサポートされています。一部のハードウェア プラットフォームは Skype をサポートしていません。たとえば、Supervisor/PISA エンジンが搭載されている Catalyst 6500 シリーズ スイッチでは Skype はサポートされません。Cisco IOS XE Release 2.5 は、TCP および UDP タイプで Skype をサポートしています。

[4] Release 12.2(18)ZYA では、HTTP 経由の YouTube へのアクセスのみが認識されます。

[5] BitTorrent は、暗号化されていないトラフィックのみを分類します。

[6] eDonkey は、暗号化されていないトラフィックのみを分類します。

[7] Release 12.2(18)ZYA では、SIP および Skinny 電話接続（cisco-phone トラフィック接続）のみが認識されます。H.323 電話接続は認識されません。

[8] AOL-Protocol は、ICQ クライアントと AOL クライアントの間で共有されるトラフィックを分類します。

ip nbar custom コマンドによって作成されたカスタム プロトコル

variable-field-name 引数は、**ipnbarcustom** コマンドを使用してカスタム プロトコルを作成したときに入力された **variable***field-namefield-length* オプションと組み合わせて使用されます。変数オプションにより、NBAR がカスタム プロトコルの特定の値に基づいてトラフィックを照合することができます。たとえば、カスタム プロトコルを作成するために

ipnbarcustomftdd125variablescid2tcprange50015005 が入力され、**matchprotocolftddscid804** を使用するクラス マップが作成された場合、作成されたクラス マップは、TCP ポート 5001 ～ 5005 を出入りする、バイト 125 に値「804」を持つすべてのトラフィックを照合します。

クラス マップで、カスタム プロトコルごとに最大で 24 個の変数値を示すことができます。たとえば、以下の設定では 4 個の変数が使用されており、さらに 20 個の「scid」値が使用できます。

```
Router(config)# ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005
Router(config)# class-map active-craft
Router(config-cmap)# match protocol ftdd scid 0x15
Router(config-cmap)# match protocol ftdd scid 0x21
Router(config)# class-map passive-craft
Router(config-cmap)# match protocol ftdd scid 0x11
Router(config-cmap)# match protocol ftdd scid 0x22
```

match protocol コマンドの制限（Catalyst 6500 シリーズ スイッチのみ）

ポリシー マップにはトラフィック クラスが含まれています。トラフィック クラスには、プロトコル タイプまたはアプリケーションに基づいてパケットを照合する（およびグループにまとめる）ために使用できる、1 つ以上の **match** コマンドが含まれています。必要に応じて任意の数のトラフィック クラスを作成できます。

Cisco IOS Release 12.2(18)ZY には、Supervisor 32/PISA エンジンが搭載された Catalyst 6500 シリーズ スイッチ用のソフトウェアが含まれています。このリリースおよびプラットフォームでは、ポリシー マップと **matchprotocol** コマンドの使用に関する次の制限に注意してください。

- 1 つのトラフィック クラスは、最大 8 個のプロトコルまたはアプリケーションに一致するように設定できます。
- 複数のトラフィック クラスは、累積で最大 95 個のプロトコルまたはアプリケーションに一致するように設定できます。

例

次に、FTP トラフィックを照合するように NBAR を設定する例を示します。

```
Router(config-cmap)# match protocol ftp
```

次の例では、カスタム プロトコル ftdd が変数を使用して作成されています。変数に基づいて、このカスタム プロトコルを照合するクラス マップも作成されます。この例では、クラス マップ matchscidinftdd は、TCP ポート 5001 ～ 5005 を出入りする、バイト 125 に値「804」を持つすべてのトラフィックを照合します。変数 scid の長さは 2 バイトです。

```
Router(config)# ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
Router(config)# class-map matchscidinftdd
Router(config-cmap)# match protocol ftdd scid 804
```

次の例は、クラス マップで 16 進数を使用して、次のようにコマンドを記述することもできることを示しています。

```
Router(config)#
ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
```

```
Router(config)# class-map matchscidinftdd
Router(config-cmap)# match protocol ftdd scid 0x324
```

次の例では、カスタム プロトコルの作成中に **variable** キーワードが使用され、変数フィールド内のさまざまな値をさまざまなトラフィック クラスに分類するようにクラスマップが設定されています。具体的には、次の例では、変数 scid 値 0x15、0x21、および 0x27 は、クラス マップ active-craft に分類され、scid 値 0x11、0x22、および 0x25 はクラス マップ passive-craft に分類されます。

```
Router(config)# ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005
Router(config)# class-map active-craft
Router(config-cmap)# match protocol ftdd scid 0x15
Router(config-cmap)# match protocol ftdd scid 0x21
Router(config-cmap)# match protocol ftdd scid 0x27
Router(config)# class-map passive-craft
Router(config-cmap)# match protocol ftdd scid 0x11
Router(config-cmap)# match protocol ftdd scid 0x22
Router(config-cmap)# match protocol ftdd scid 0x25
```

関連コマンド

Command	Description
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
ipnbarcustom	NBAR Protocol Discovery 機能を拡張し、追加の静的ポート アプリケーションを分類および監視できます。または、NBAR はサポートしていない静的ポート トラフィックを分類できるようになります。

match protocol potentially (NBAR)

Network-Based Application Recognition（NBAR）が認識するプロトコル タイプによりトラフィックを照合するように NBAR を設定するには、クラス マップ コンフィギュレーション モードで **match protocol** コマンドを使用します。NBAR による、既知のプロトコル タイプによるトラフィックの照合を無効にするには、このコマンドの **no** 形式を使用します。

match protocol *protocol-name* **potentially**
no match protocol *protocol-name* **potentially**

構文の説明

protocol-name	NBAR が認識する特定のプロトコル タイプです。これらの既知のプロトコル タイプを使用してトラフィックを照合できます。NBAR が認識するプロトコル タイプのリストについては、下記の「使用上のガイドライン」の表を参照してください。
potentially	（任意）プロトコルとすべての潜在的なトラフィックを照合します。

コマンド デフォルト

NBAR が認識するプロトコル タイプによりトラフィックが照合されません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 2.1S	このコマンドが Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。
Cisco IOS XE リリース 2.3S	以下の「使用上のガイドライン」の表に記載されている追加プロトコルを認識するように、このコマンドが変更されました。
Cisco IOS XE Release 2.5S	以下の「使用上のガイドライン」の表に記載されている追加プロトコルを認識するように、このコマンドが変更されました。
Cisco IOS XE リリース 3.4S	以下の「使用上のガイドライン」の表に記載されている追加プロトコルを認識するように、このコマンドが変更されました。
Cisco IOS XE リリース 3.16S	このコマンドは、特定のアプリケーションのみを許可するポリシーを定義するように変更され、そのポリシーに準拠しないすべてのアプリケーションをブロックします。
15.1(3)S	このコマンドが変更されました。Cisco 7200 シリーズ ルータからサポートが削除されました。
Cisco IOS XE 3.17.3	このコマンドは廃止されました。
Cisco Everest 16.4.1	このコマンドは廃止されました。

使用上のガイドライン

「潜在的一致」を使用したクラス マップは、次のトラフィックをチェックします。

- アクティブなエンジンが照合されるプロトコルの署名を持つ、最終的でない未知のトラフィック
- 照合されるプロトコルに転じる、最終的でない分類されるトラフィック
- 完全一致の、最終的なトラフィック/最終的でないトラフィック
- 照合されるプロトコルから取得される、最終的なトラフィック/最終的でないトラフィック

クラス マップのタイプ（match-any/match-all）により、クラス マップで許可される潜在的一致（PM）の数が決まります。

- match-any：任意の数の PM
- match-all：1 つのみの PM のインスタンス

（注） クラス マップに複数の PM を定義すると、次のようになります。

- 冗長：両方のプロトコルが同じ階層にある場合は、片方のプロトコルが一致したときに、もう片方のプロトコルも一致します。
- 欠陥：2 つのプロトコルが同じ階層にない場合は、クラスマップが一致することはありません。

match protocol potentially (NBAR) コマンドを使用して、NBAR が認識するプロトコル タイプを照合します。NBAR には、次のタイプのプロトコルを分類する機能があります。

- 非 UDP および非 TCP IP プロトコル
- スタティックに割り当てられたポート番号を使用する TCP および UDP プロトコル
- スタティックに割り当てられたポート番号を使用し、さらにステートフルインスペクションを必須とする TCP および UDP プロトコル
- ダイナミックに割り当てられたポート番号を使用するため、ステートフルインスペクションを必須とする TCP および UDP プロトコル

以下の表に、Cisco IOS ソフトウェアに使用できる NBAR 対応プロトコルをカテゴリ順に示します。この表には、プロトコル タイプ、ウェルノウン ポート番号（該当する場合）、および NBAR でプロトコルを入力するための構文に関する情報も記載されています。この表は、新しいプロトコルが追加されたときや、異なるリリースによりサポートされたときに変更されます。

（注） 以下の表に、12.2(18)ZY および 12.2(18)ZYA リリースに使用できる NBAR 対応プロトコルを示します。12.2(18)ZY および 12.2(18)ZYA リリースは、Supervisor 32/PISA エンジンを搭載する Catalyst 6500 シリーズ スイッチでサポートされます。

表 *16 : NBAR* がサポートするプロトコル

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
エンタープライズアプリケーション	Novadigm	TCP/ UDP	3460 ～ 3465	Novadigm Enterprise Desktop Manager（EDM）	novadigm
	Citrix（ICA、CGP、IMA、SB）	TCP/ UDP	TCP：1494、2512、2513、2598 UDP：1604	Citrix ICA トラフィック	citrix citrix app citrix ica-tag
	Oracle	TCP	1525	Oracle	ora-srv
	PCAnywhere	TCP/UDP	TCP：5631、65301 UDP：22、5632	Symantic PCAnywhere	pcanywhere
	SAP	TCP	3300 ～ 3315 3200 ～ 3215 3600 ～ 3615	アプリケーション サーバからアプリケーション サーバへのトラフィック（sap-pgm.pdlm） クライアントからアプリケーション サーバへのトラフィック（sap-app.pdlm） クライアントからメッセージ サーバへのトラフィック（sap-msg.pdlm）	sap
	Exchange [9]	TCP	135	MS-RPC for Exchange	exchange

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ルーティング プロトコル	BGP	TCP/ UDP	179	Border Gateway Protocol; ボーダー ゲートウェイ プロトコル	bgp
	EGP	IP	8	エクステリア ゲートウェイ プロトコル	egp
	EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp
	OSPF	IP	89	Open Shortest Path First	ospf
	RIP	UDP	520	Routing Information Protocol	rip
データベース	CIFS	TCP	139、445	Common Internet File System	cifs
	MS-SQLServer	TCP	1433	Microsoft SQL Server Desktop Videoconferencing	sqlserver
	SQL-exec	TCP/UDP	9088	SQL Exec	sqlexec
	SQL*NET	TCP/ UDP	1521	SQL*NET for Oracle	sqlnet
金融	FIX	TCP	ヒューリスティック	Financial Information Exchange	fix

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
セキュリティとトンネリング	GRE	IP	47	総称ルーティングカプセル化	gre
IPINIP	IP	4	IP in IP	ipinip	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
IPsec	IP/TCP	50、51 TCP ヒューリスティック	IP Encapsulating Security Payload/Authentication-Header	ipsec	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
L2TP	UDP	1701	L2F/L2TP Tunnel	l2tp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
PPTP	TCP	1723	Point-to-Point Tunneling Protocol for VPN	pptp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
SFTP	TCP	990	セキュア FTP	secure-ftp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
SHTTP	TCP	443	Secure HTTP; セキュア HTTP	secure-http	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3
STELNET	TCP	992	セキュア Telnet	secure-telnet	Cisco IOS XE リリース 2.3

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	SIMAP	TCP/ UDP	585、993	セキュア Internet Message Access Protocol	secure-imap
	SIRC	TCP/ UDP	994	セキュア インターネット リレー チャット	secure-irc
	SLDAP	TCP/ UDP	636	セキュア Lightweight Directory Access Protocol	secure-ldap
	SNNTP	TCP/ UDP	563	セキュア Network News Transfer Protocol	secure-nntp
	SOCKS	TCP	1080	Firewall Security Protocol	socks
	SPOP3	TCP/ UDP	995	Secure POP3	secure-pop3
	SSH	TCP	22	Secured Shell	ssh
	STELNET	TCP	992	セキュア Telnet	secure-telnet

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ネットワーク管理	ICMP	IP	1	Internet Control Message Protocol; インターネット制御メッセージ プロトコル	[icmp]
	SNMP	TCP/ UDP	161、162	簡易ネットワーク管理プロトコル	snmp
	Syslog	UDP	514	System Logging Utility	syslog
ネットワーク メール サービス	IMAP	TCP/ UDP	143、220	Internet Message Access Protocol	imap
	Notes	TCP/ UDP	1352	Lotus Notes	notes
	POP3	TCP/ UDP	110、ヒューリスティック	Post Office Protocol	pop3
	SMTP	TCP	25、ヒューリスティック	Simple Mail Transfer Protocol	smtp

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ディレクトリ	DHCP/ BOOTP	UDP	67、68	Dynamic Host Configuration Protocol/Bootstrap Protocol	dhcp
	DNS	TCP/ UDP	53	ドメイン ネーム システム	dns
	Finger	TCP	79	Finger User Information Protocol	finger
	Kerberos	TCP/ UDP	88、749	Kerberos Network Authentication Service	kerberos
	LDAP	TCP/ UDP	389	Lightweight Directory Access Protocol	ldap

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
インターネット	FTP	TCP	21、21000、ヒューリスティック	ファイル転送プログラム	FTP
	Gopher	TCP/ UDP	70	Internet Gopher Protocol	gopher
	HTTP	TCP	80[10]、 ヒューリスティック	ハイパーテキスト転送プロトコル	http
	IRC	TCP/ UDP	194	インターネット リレー チャット	irc
	NNTP	TCP/ UDP	119、ヒューリスティック	Network News Transfer Protocol	nntp
	Telnet	TCP	23	Telnet Protocol	telnet
	TFTP	UDP	69	トリビアル ファイル転送プロトコル	tftp
シグナリング	AppleQTC	TCP/UDP	458	Apple Quick Time	appleqtc

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Chargen	TCP/UDP	19	キャラクタ ジェネレータ	chargen	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
ClearCase	TCP/UDP	371	Clear Case Protocol Software Informer	clearcase	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
Corba	TCP/UDP	683、684	Corba Internet Inter-Orb Protocol（IIOP）	corba-iiop	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
Daytime	TCP/UDP	13	Daytime Protocol	daytime	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
Doom	TCP/UDP	666	Doom	doom	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
Echo	TCP/UDP	7	Echo Protocol	echo	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
IBM DB2	TCP/UDP	523	IBM Information Management	ibm-db2	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
IPX	TCP/UDP	213	Internet Packet Exchange	server-ipx	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
ISAKMP	TCP/UDP	500	Internet Security Association and Key Management Protocol	isakmp	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3
ISI-GL	TCP/UDP	55	Interoperable Self Installation Graphics Language	isi-gl	12.2(18)ZYA 12.2(18)ZYA1Cis IOS XE Release 2.3

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
			KLogin	TCP	543
KShell	TCP		544	KShell	kshell
LockD	TCP/UDP		4045	LockD	lockd
MSSQL	TCP		1433	Microsoft Structured Query Language（SQL）サーバ	mssql
RSVP	IP/UDP		IP：46 UDP：1698、1699	リソース予約プロトコル	rsvp
RPC	AOL-messenger	TCP	5190、443	AOL Instant Messenger Chat Messages	aol-messenger
	NFS	TCP/UDP	2049	ネットワーク ファイル システム	nfs
	Sunrpc	TCP/ UDP	111、ヒューリスティック	Sun Remote Procedure Call	sunrpc

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
非 IP および LAN/レガシー	NetBIOS	TCP/ UDP	TCP-137、138 UDP-137、139	NetBIOS over IP（MS Windows）	netbios
	Nickname	TCP/UDP	43	Nickname	nicname
	NPP	TCP/UDP	92	Network Payment Protocol	npp

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
音声	Google Talk VoIP	TCP/UDP	動的に割り当て	Google Talk VoIP プロトコル	gtalk-voip
	H.323	TCP	ヒューリスティック	H.323 Teleconferencing Protocol	h323
	MSN VoIP	UDP	動的に割り当て	MSN Messenger プロトコル	msn-voip
	RTCP	TCP/ UDP	動的に割り当て	リアルタイム制御プロトコル	rtcp
	RTP	TCP/ UDP	動的に割り当て	Real-Time Transport Protocol Payload Classification	rtp
	SIP	TCP/UPD	5060	Session Initiation Protocol	sip
	STUN	UDP	動的に割り当て	Simple Traversal of UDP through NAT（STUN）	stun-nat
	Skype[11]	TCP/UDP	TCP-80、ヒューリスティック	VoIP クライアント ソフトウェア	skype
	Yahoo VoIP	TCP/UDP	動的に割り当て	Yahoo Messenger VoIP プロトコル	yahoo-voip
デスクトップ メディア	CUSeeMe	TCP/UDP	TCP：7648、7649 UDP：24032	CU-SeeMe デスクトップ ビデオ会議	cuseeme
ストリーミング メディア	RealAudio	TCP/ UDP	動的に割り当て	RealAudio Streaming Protocol	realaudio

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	RTSP	TCP	554、8554	Real Time Streaming Protocol	rtsp
	StreamWorks	UDP	動的に割り当て	Xing Technology Stream Works Audio and Video	streamwork
	VDOLive	TCP/ UDP	インスペクションを使用する場合はスタティック（7000）	VDOLive Streaming Video	vdolive
	YouTube[12]	TCP	スタティック（80）とダイナミック割り当ての両方	オンライン ビデオ共有 Web サイト	youtube
ピアツーピア ファイル共有アプリケーション	BitTorrent[13]	TCP	ヒューリスティック、または 6881 ～ 6889	BitTorrent File Transfer Traffic	bittorrent
DirectConnect	TCP	80、411 ～ 413、ヒューリスティック	Direct Connect File Transfer Traffic	directconnect	Cisco IOS XE Release 2.5
eDonkey/eMule[14]	TCP	80、4662、ヒューリスティック	eDonkey File-Sharing Application また、NBAR では eMule トラフィックは eDonkey トラフィックに分類されます。	edonkey	12.2(18)ZYA1 12.3(11)T Cisco IOS XE リリース 2.5
Encrypted Emule	TCP	ヒューリスティック	P2P ファイル共有暗号化プロトコル	encrypted-emule	Cisco IOS XE リリース 3.4S
FastTrack	—	ヒューリスティック	FastTrack トラフィック	fasttrack	12.1(12c)E 12.2(18)ZYA1 Cisco IOS XE Release 2.5
FastTrack Static	—	ヒューリスティック	FastTrack Static	fasttrack-static	Cisco IOS XE リリース 3.3S
Gnutella	TCP/UDP	ヒューリスティック、または TCP-80、6346 ～ 6349、6355、5634	Gnutella トラフィック	gnutella	Cisco IOS XE Release 2.5
Gnutella Networking	TCP/UDP	ヒューリスティック、または UDP-6346 ～ 6348	Gnutella Networking トラフィック	networking-gnutella	Cisco IOS XE リリース 3.4S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
KaZaA	TCP/ UPD	ヒューリスティック	KaZaA 以前の KaZaA バージョン 1 トラフィックは、FastTrack を使用して分類できます。	kazaa2	12.2(8)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
WinMX	TCP	6699	WinMX ピアツーピア ファイル共有	winmx	12.2(18)ZYA1 12.3(7)T Cisco IOS XE リリース 2.5
その他	3Com AMP3	TCP/UDP	629	3Com AMP3	3com-amp3
	3Com TSMUX	TCP/UDP	106	3Com TSMUX	3com-tsmux
3PC	TCP/UDP	34	Third Party Connect Protocol	3pc	Cisco IOS XE Release 3.1S
914 C/G	TCP/UDP	211	Texas Instruments 914 Terminal	914c/g	Cisco IOS XE Release 3.1S
9PFS	TCP/UDP	564	Plan 9 file service	9pfs	Cisco IOS XE Release 3.1S
ACAP	TCP/UDP	674	ACAP	acap	Cisco IOS XE Release 3.1S
ACAS	TCP/UDP	62	ACA Services	acas	Cisco IOS XE Release 3.1S
AccessBuilder	TCP/UDP	888	Access Builder	accessbuilder	Cisco IOS XE Release 3.1S
AccessNetwork	TCP/UDP	699	アクセス ネットワーク	accessnetwork	Cisco IOS XE Release 3.1S
ACP	TCP/UDP	599	Aeolon Core Protocol	acp	Cisco IOS XE Release 3.1S
ACR-NEMA	TCP/UDP	104	ACR-NEMA Digital Img	acr-nema	Cisco IOS XE Release 3.1S
AED-512	TCP/UDP	149	AED 512 Emulation service	aed-512	Cisco IOS XE Release 3.1S
Agentx	TCP/UDP	705	AgentX	agentx	Cisco IOS XE Release 3.1S
Alpes	TCP/UDP	463	Alpes	alpes	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
AMInet	TCP/UDP	2639	AMInet	aminet	Cisco IOS XE Release 3.1S
AN	TCP/UDP	107	Active Networks	an	Cisco IOS XE Release 3.1S
ANET	TCP/UDP	212	ATEXSSTR	anet	Cisco IOS XE Release 3.1S
ANSANotify	TCP/UDP	116	ANSA REX Notify	ansanotify	Cisco IOS XE Release 3.1S
ANSATrader	TCP/UDP	124	ansatrader	ansatrader	Cisco IOS XE Release 3.1S
AODV	TCP/UDP	654	AODV	aodv	Cisco IOS XE Release 3.1S
	Apertus-LDP	TCP/UDP	539	Apertus Tech Load Distribution	apertus-ldp
	AppleQTC	TCP/UDP	458	apple quick time	appleqtc
AppleQTSRVR	TCP/UDP	545	appleqtcsrvr	appleqtcsrvr	Cisco IOS XE Release 3.1S
Applix	TCP/UDP	999	Applix ac	applix	Cisco IOS XE Release 3.1S
ARCISDMS	TCP/UDP	262	arcisdms	arcisdms	Cisco IOS XE Release 3.1S
ARGUS	TCP/UDP	13	ARGUS	argus	Cisco IOS XE Release 3.1S
Ariel1	TCP/UDP	419	Ariel1	ariel1	Cisco IOS XE Release 3.1S
Ariel2	TCP/UDP	421	Ariel2	ariel2	Cisco IOS XE Release 3.1S
Ariel3	TCP/UDP	422	Ariel3	ariel3	Cisco IOS XE Release 3.1S
ARIS	TCP/UDP	104	ARIS	aris	Cisco IOS XE Release 3.1S
ARNS	TCP/UDP	384	リモートネットワークサーバシステム	arns	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ASA	TCP/UDP	386	ASA Message router object def	asa	Cisco IOS XE Release 3.1S
ASA-Appl-Proto	TCP/UDP	502	asa-appl-proto	asa-appl-proto	Cisco IOS XE Release 3.1S
ASIPRegistry	TCP/UDP	687	asipregistry	asipregistry	Cisco IOS XE Release 3.1S
ASIP-Webadmin	TCP/UDP	311	AppleShare IP WebAdmin	asip-webadmin	Cisco IOS XE Release 3.1S
AS-Servermap	TCP/UDP	449	AS Server Mapper	as-servermap	Cisco IOS XE Release 3.1S
AT-3	TCP/UDP	203	AppleTalk 未使用	at-3	Cisco IOS XE Release 3.1S
AT-5	TCP/UDP	205	AppleTalk 未使用	at-5	Cisco IOS XE Release 3.1S
AT-7	TCP/UDP	207	AppleTalk 未使用	at-7	Cisco IOS XE Release 3.1S
AT-8	TCP/UDP	208	AppleTalk 未使用	at-8	Cisco IOS XE Release 3.1S
	AT-Echo	TCP/UDP	204	AppleTalk Echo	at-echo
AT-NBP	TCP/UDP	202	AppleTalk Name Binding	at-nbp	Cisco IOS XE Release 3.1S
AT-RTMP	TCP/UDP	201	AppleTalk Routing Maintenance	at-rtmp	Cisco IOS XE Release 3.1S
AT-ZIS	TCP/UDP	206	AppleTalk Zone Information	at-zis	Cisco IOS XE Release 3.1S
Audit	TCP/UDP	182	Unisys Audit SITP	audit	Cisco IOS XE Release 3.1S
Auditd	TCP/UDP	48	デジタル監査デーモン	auditd	Cisco IOS XE Release 3.1S
Aurora-CMGR	TCP/UDP	364	Aurora CMGR	aurora-cmgr	Cisco IOS XE Release 3.1S
AURP	TCP/UDP	387	Appletalk Update-Based Routing Protocol	aurp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
AUTH	TCP/UDP	113	認証サービス（Authentication Service）	auth	Cisco IOS XE Release 3.1S
Avian	TCP/UDP	486	avian	avian	Cisco IOS XE Release 3.1S
AX25	TCP/UDP	93	AX.25 フレーム	ax25	Cisco IOS XE Release 3.1S
Banyan-RPC	TCP/UDP	567	Banyan-RPC	banyan-rpc	Cisco IOS XE Release 3.1S
Banyan-VIP	TCP/UDP	573	Banyan-VIP	banyan-vip	Cisco IOS XE Release 3.1S
BBNRCCMON	TCP/UDP	10	BBN RCC モニタリング	bbnrccmon	Cisco IOS XE Release 3.1S
BDP	TCP/UDP	581	バンドル検出プロトコル	bdp	Cisco IOS XE Release 3.1S
BFTP	TCP/UDP	152	バックグラウンドファイル転送プログラム	bftp	Cisco IOS XE Release 3.1S
BGMP	TCP/UDP	264	Border Gateway Multicast Protocol	bgmp	Cisco IOS XE Release 3.1S
BGP	TCP/UDP	179	Border Gateway Protocol; ボーダーゲートウェイプロトコル	bgp	Cisco IOS XE Release 3.1S
BGS-NSI	TCP/UDP	482	BGS-NSI	bgs-nsi	Cisco IOS XE Release 3.1S
	Bhevent	TCP/UDP	357	Bhevent	bhevent
	BHFHS	TCP/UDP	248	BHFHS	bhfhs
BHMDS	TCP/UDP	310	BHMDS	bhmds	Cisco IOS XE Release 3.1S
BL-IDM	TCP/UDP	142	Britton Lee IDM	bl-idm	Cisco IOS XE Release 3.1S
BMPP	TCP/UDP	632	BMPP	bmpp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
BNA	TCP/UDP	49	BNA	bna	Cisco IOS XE Release 3.1S
Bnet	TCP/UDP	415	BNET	bnet	Cisco IOS XE Release 3.1S
Borland-DSJ	TCP/UDP	707	Borland-dsj	borland-dsj	Cisco IOS XE Release 3.1S
BR-SAT-Mon	TCP/UDP	76	Backroom SATNET モニタリング	br-sat-mon	Cisco IOS XE Release 3.1S
Cableport-AX	TCP/UDP	282	Cable Port A/X	cableport-ax	Cisco IOS XE Release 3.1S
Cab-Protocol	TCP/UDP	595	CAB プロトコル	cab-protocol	Cisco IOS XE Release 3.1S
Cadlock	TCP/UDP	770	Cadlock	cadlock	Cisco IOS XE Release 3.1S
CAIlic	TCP/UDP	216	Computer Associates Intl License Server	CAIlic	Cisco IOS XE Release 3.1S
CBT	TCP/UDP	7	CBT	cbt	Cisco IOS XE Release 3.1S
CDC	TCP/UDP	223	Certificate Distribution Center	cdc	Cisco IOS XE Release 3.1S
CFDPTKT	TCP/UDP	120	cfdptkt	cfdptkt	Cisco IOS XE Release 3.1S
CFTP	TCP/UDP	62	CFTP	cftp	Cisco IOS XE Release 3.1S
CHAOS	TCP/UDP	16	Chaos	chaos	Cisco IOS XE Release 3.1S
CharGen	TCP/UDP	19	キャラクタ ジェネレータ	chargen	Cisco IOS XE Release 3.1S
	ChShell	TCP/UDP	562	chcmd	chshell
	Cimplex	TCP/UDP	673	Cimplex	cimplex
Cisco-FNA	TCP/UDP	130	Cisco FNATIVE	cisco-fna	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Cisco-phone[15]	UDP	5060	Cisco IP Phone および PC-Based Unified Communicator	cisco-phone	12.2(18)ZYA 12.2(18)ZYA1
Cisco-SYS	TCP/UDP	132	Cisco SYSMAINT	cisco-sys	Cisco IOS XE Release 3.1S
Cisco-TDP	TCP/UDP	711	Cisco TDP	cisco-tdp	Cisco IOS XE Release 3.1S
Cisco-TNA	TCP/UDP	131	Cisco TNATIVE	cisco-tna	Cisco IOS XE Release 3.1S
Clearcase	TCP/UDP	371	Clearcase	clearcase	Cisco IOS XE Release 3.1S
Cloanto-Net-1	TCP/UDP	356	Cloanto-net-1	cloanto-net-1	Cisco IOS XE Release 3.1S
CMIP-Agent	TCP/UDP	164	CMIP/TCP Agent	cmip-agent	Cisco IOS XE Release 3.1S
CMIP-Man	TCP/UDP	163	CMIP/TCP Manager	cmip-man	Cisco IOS XE Release 3.1S
Coauthor	TCP/UDP	1529	Oracle	coauthor	Cisco IOS XE Release 3.1S
Codaauth2	TCP/UDP	370	Codaauth2	codaauth2	Cisco IOS XE Release 3.1S
Collaborator	TCP/UDP	622	Collaborator	collaborator	Cisco IOS XE Release 3.1S
Commerce	TCP/UDP	542	Commerce	commerce	Cisco IOS XE Release 3.1S
Compaq-Peer	TCP/UDP	110	Compaq Peer Protocol	compaq-peer	Cisco IOS XE Release 3.1S
Compressnet	TCP/UDP	2	管理ユーティリティ	compressnet	Cisco IOS XE Release 3.1S
COMSCM	TCP/UDP	437	COMSCM	comscm	Cisco IOS XE Release 3.1S
CON	TCP/UDP	759	デメリット	con	Cisco IOS XE Release 3.1S
Conference	TCP/UDP	531	チャット（Chat）	conference	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	Connendp	TCP/UDP	693	Almanid 接続エンドポイント	connendp
	ContentServer	TCP/UDP	3365	Contentserver	contentserver
CoreRJD	TCP/UDP	284	Corerjd	corerjd	Cisco IOS XE Release 3.1S
Courier	TCP/UDP	530	RPC	courier	Cisco IOS XE Release 3.1S
Covia	TCP/UDP	64	Communications Integrator	covia	Cisco IOS XE Release 3.1S
CPHB	TCP/UDP	73	Computer Protocol Heart Beat	cphb	Cisco IOS XE Release 3.1S
CPNX	TCP/UDP	72	Computer Protocol Network Executive	cpnx	Cisco IOS XE Release 3.1S
Creativepartnr	TCP/UDP	455	Creativepartnr	creativepartnr	Cisco IOS XE Release 3.1S
Creativeserver	TCP/UDP	453	Creativeserver	creativeserver	Cisco IOS XE Release 3.1S
CRS	TCP/UDP	507	CRS	crs	Cisco IOS XE Release 3.1S
CRTP	TCP/UDP	126	Combat Radio Transport Protocol	crtp	Cisco IOS XE Release 3.1S
CRUDP	TCP/UDP	127	Combat Radio User Datagram	crudp	Cisco IOS XE Release 3.1S
CryptoAdmin	TCP/UDP	624	Crypto Admin	cryptoadmin	Cisco IOS XE Release 3.1S
CSI-SGWP	TCP/UDP	348	Cabletron Management Protocol	csi-sgwp	Cisco IOS XE Release 3.1S
CSNET-NS	TCP/UDP	105	Mailbox Name Nameserver	csnet-ns	Cisco IOS XE Release 3.1S
CTF	TCP/UDP	84	共通トレース機能	ctf	Cisco IOS XE Release 3.1S
CUSTIX	TCP/UDP	528	Customer Ixchange	custix	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
CVC_Hostd	TCP/UDP	442	CVC_Hostd	cvc_hostd	Cisco IOS XE Release 3.1S
Cybercash	TCP/UDP	551	Cybercash	cybercash	Cisco IOS XE Release 3.1S
Cycleserv	TCP/UDP	763	Cycleserv	cycleserv	Cisco IOS XE Release 3.1S
	Cycleserv2	TCP/UDP	772	Cycleserv2	cycleserv2
Dantz	TCP/UDP	497	Dantz	dantz	Cisco IOS XE Release 3.1S
DASP	TCP/UDP	439	Dasp	dasp	Cisco IOS XE Release 3.1S
DataSurfSRV	TCP/UDP	461	DataRamp Svr	datasurfsrv	Cisco IOS XE Release 3.1S
DataSurfSRVSec	TCP/UDP	462	DataRamp Svr svs	datasurfsrvsec	Cisco IOS XE Release 3.1S
Datex-ASN	TCP/UDP	355	datex-asn	datex-asn	Cisco IOS XE Release 3.1S
Daytime	TCP/UDP	13	Daytime（RFC 867）	daytime	Cisco IOS XE Release 3.1S
Dbase	TCP/UDP	217	dBASE Unix	dbase	Cisco IOS XE Release 3.1S
DCCP	TCP/UDP	33	データグラム輻輳制御プロトコル	dccp	Cisco IOS XE Release 3.1S
DCN-Meas	TCP/UDP	19	DCN 測定サブシステム	dcn-meas	Cisco IOS XE Release 3.1S
DCP	TCP/UDP	93	デバイス制御プロトコル	dcp	Cisco IOS XE Release 3.1S
DCTP	TCP/UDP	675	DCTP	dctp	Cisco IOS XE Release 3.1S
DDM-DFM	TCP/UDP	447	DDM 分散ファイル管理	ddm-dfm	Cisco IOS XE Release 3.1S
DDM-RDB	TCP/UDP	446	DDM リモート リレーショナルデータベースアクセス	ddm-rdb	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
DDM-SSL	TCP/UDP	448	セキュア ソケットを使用した DDM リモート DB アクセス	ddm-ssl	Cisco IOS XE Release 3.1S
DDP	TCP/UDP	37	データグラム送達プロトコル	ddp	Cisco IOS XE Release 3.1S
DDX	TCP/UDP	116	D-II データ交換	ddx	Cisco IOS XE Release 3.1S
DEC_DLM	TCP/UDP	625	dec_dlm	dec_dlm	Cisco IOS XE Release 3.1S
Decap	TCP/UDP	403	Decap	decap	Cisco IOS XE Release 3.1S
	Decauth	TCP/UDP	316	Decauth	decauth
Decbsrv	TCP/UDP	579	Decbsrv	decbsrv	Cisco IOS XE Release 3.1S
Decladebug	TCP/UDP	410	DECLadebug リモート デバッグ プロトコル	decladebug	Cisco IOS XE Release 3.1S
Decvms-sysmgt	TCP/UDP	441	Decvms-sysmgt	decvms-sysmgt	Cisco IOS XE Release 3.1S
DEI-ICDA	TCP/UDP	618	dei-icda	dei-icda	Cisco IOS XE Release 3.1S
DEOS	TCP/UDP	76	分散外部オブジェクト ストア	deos	Cisco IOS XE Release 3.1S
Device	TCP/UDP	801	Device	デバイス	Cisco IOS XE Release 3.1S
DGP	TCP/UDP	86	異種ゲートウェイ プロトコル	dgp	Cisco IOS XE Release 3.1S
DHCP-Failover	TCP/UDP	647	DHCP フェールオーバー	dhcp-failover	Cisco IOS XE Release 3.1S
DHCP-Failover2	TCP/UDP	847	dhcp-failover2	dhcp-failover2	Cisco IOS XE Release 3.1S
DHCPv6-client	TCP/UDP	546	DHCPv6 クライアント	dhcpv6-client	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
DHCPv6-server	TCP/UDP	547	DHCPv6 サーバ	dhcpv6-server	Cisco IOS XE Release 3.1S
Dicom	TCP/UDP	ヒューリスティック	Digital Imaging and Communications in Medicine	dicom	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S
Digital-VRC	TCP/UDP	466	digital-vrc	digital-vrc	Cisco IOS XE Release 3.1S
Directplay	TCP/UDP	2234	DirectPlay	directplay	Cisco IOS XE Release 3.1S
Directplay8	TCP/UDP	6073	DirectPlay8	directplay8	Cisco IOS XE Release 3.1S
Directv-Catlg	TCP/UDP	3337	Direct TV Data Catalog	directv-catlg	Cisco IOS XE Release 3.1S
Directv-Soft	TCP/UDP	3335	Direct TV Software Updates	directv-soft	Cisco IOS XE Release 3.1S
	Directv-Tick	TCP/UDP	3336	Direct TV Tickers	directv-tick
	Directv-Web	TCP/UDP	3334	Direct TV Webcasting	directv-web
Discard	TCP/UDP	9	廃棄	discard	Cisco IOS XE Release 3.1S
Disclose	TCP/UDP	667	選挙献金開示	disclose	Cisco IOS XE Release 3.1S
Dixie	TCP/UDP	96	DIXIE プロトコル仕様	dixie	Cisco IOS XE Release 3.1S
DLS	TCP/UDP	197	Directory Location Service	dls	Cisco IOS XE Release 3.1S
DLS-Mon	TCP/UDP	198	Directory Location Service Monitor	dls-mon	Cisco IOS XE Release 3.1S
DN6-NLM-AUD	TCP/UDP	195	DNSIX Network Level Module Audit	dn6-nlm-aud	Cisco IOS XE Release 3.1S
DNA-CML	TCP/UDP	436	DNA-CML	dna-cml	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
DNS	TCP/UDP	53	ドメイン ネーム サーバ ルックアップ	dns	Cisco IOS XE Release 3.1S
DNSIX	TCP/UDP	90	DNSIX Security Attribute Token Map	dnsix	Cisco IOS XE Release 3.1S
DOOM	TCP/UDP	666	Doom Id Software	doom	Cisco IOS XE Release 3.1S
DPSI	TCP/UDP	315	DPSI	dpsi	Cisco IOS XE Release 3.1S
DSFGW	TCP/UDP	438	DSFGW	dsfgw	Cisco IOS XE Release 3.1S
DSP	TCP/UDP	33	表示支援プロトコル	dsp	Cisco IOS XE Release 3.1S
DSP3270	TCP/UDP	246	表示システム プロトコル	dsp3270	Cisco IOS XE Release 3.1S
DSR	TCP/UDP	48	動的ソースルーティング プロトコル	dsr	Cisco IOS XE Release 3.1S
DTAG-DTE-SB	TCP/UDP	352	DTAG	dtag-ste-sb	Cisco IOS XE Release 3.1S
DTK	TCP/UDP	365	DTK	dtk	Cisco IOS XE Release 3.1S
	DWR	TCP/UDP	644	DWR	dwr
Echo	TCP/UDP	7	エコー（Echo）	echo	Cisco IOS XE Release 3.1S
EGP	TCP/UDP	8	エクステリア ゲートウェイ プロトコル	egp	Cisco IOS XE Release 3.1S
EIGRP	TCP/UDP	88	Enhanced Interior Gateway Routing Protocol	eigrp	Cisco IOS XE Release 3.1S
ELCSD	TCP/UDP	704	errlog コピー/サーバ デーモン	elcsd	Cisco IOS XE Release 3.1S
EMBL-NDT	TCP/UDP	394	EMBL Nucleic Data Transfer	embl-ndt	Cisco IOS XE Release 3.1S
EMCON	TCP/UDP	18	EMCON	emcon	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
EMFIS-CNTLl	TCP/UDP	141	EMFIS Control Service	emfis-cntl	Cisco IOS XE Release 3.1S
EMFIS-Data	TCP/UDP	140	EMFIS Data Service	emfis-data	Cisco IOS XE Release 3.1S
Encap	TCP/UDP	98	カプセル化ヘッダー	encap	Cisco IOS XE Release 3.1S
Encrypted Bittorrent	TCP	ヒューリスティック	Encrypted Bittorrent	encrypted-bittorrent	Cisco IOS XE リリース 3.4S
Entomb	TCP/UDP	775	Entomb	entomb	Cisco IOS XE Release 3.1S
Entrust-AAAS	TCP/UDP	680	Entrust-aaas	entrust-aaas	Cisco IOS XE Release 3.1S
Entrust-AAMS	TCP/UDP	681	Entrust-aams	entrust-aams	Cisco IOS XE Release 3.1S
Entrust-ASH	TCP/UDP	710	Entrust Administration Service Handler	entrust-ash	Cisco IOS XE Release 3.1S
Entrust-KMSH	TCP/UDP	709	Entrust Key Management Service Handler	entrust-kmsh	Cisco IOS XE Release 3.1S
Entrust-SPS	TCP/UDP	640	entrust-sps	entrust-sps	Cisco IOS XE Release 3.1S
ERPC	TCP/UDP	121	Encore Expedited Remote Pro.Call	erpc	Cisco IOS XE Release 3.1S
ESCP-IP	TCP/UDP	621	escp-ip	escp-ip	Cisco IOS XE Release 3.1S
	ESRO-GEN	TCP/UDP	259	Efficient Short Remote Operations	esro-gen
ESRP-EMSDP	TCP/UDP	642	ESRO-EMSDP V1.3	esro-emsdp	Cisco IOS XE Release 3.1S
EtherIP	TCP/UDP	97	Ethernet-within-IP カプセル化	etherip	Cisco IOS XE Release 3.1S
Eudora-Set	TCP/UDP	592	Eudora Set	eudora-set	Cisco IOS XE Release 3.1S
EXEC	TCP/UDP	512	リモート プロセスの実行	exec	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Fatserv	TCP/UDP	347	Fatmen Server	fatserv	Cisco IOS XE Release 3.1S
FC	TCP/UDP	133	ファイバ チャネル（Fibre Channel）	fc	Cisco IOS XE Release 3.1S
FCP	TCP/UDP	510	FirstClass プロトコル	fcp	Cisco IOS XE Release 3.1S
Finger	TCP/UDP	79	Finger	finger	Cisco IOS XE Release 3.1S
FIRE	TCP/UDP	125	FIRE	fire	Cisco IOS XE Release 3.1S
FlexLM	TCP/UDP	744	Flexible License Manager	flexlm	Cisco IOS XE Release 3.1S
FLN-SPX	TCP/UDP	221	Berkeley rlogind with SPX auth	fln-spx	Cisco IOS XE Release 3.1S
FTP-Agent	TCP/UDP	574	FTP ソフトウェア エージェント システム	ftp-agent	Cisco IOS XE Release 3.1S
FTP-Data	TCP/UDP	20	ファイル転送	ftp-data	Cisco IOS XE Release 3.1S
FTPS-Data	TCP/UDP	989	ftp プロトコル、データ、TLS/SSL 上	ftps-data	Cisco IOS XE Release 3.1S
Fujitsu-Dev	TCP/UDP	747	Fujitsu Device Control	fujitsu-dev	Cisco IOS XE Release 3.1S
GACP	TCP/UDP	190	ゲートウェイ アクセス コントロール プロトコル	gacp	Cisco IOS XE Release 3.1S
GDOMAP	TCP/UDP	538	gdomap	gdomap	Cisco IOS XE Release 3.1S
Genie	TCP/UDP	402	Genie プロトコル	genie	Cisco IOS XE Release 3.1S
	Genrad-MUX	TCP/UDP	176	Genrad-mux	genrad-mux
	GGF-NCP	TCP/UDP	678	GNU Generation Foundation NCP	ggf-ncp
GGP	TCP/UDP	3	ゲートウェイ間	ggp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Ginad	TCP/UDP	634	ginad	ginad	Cisco IOS XE Release 3.1S
GMTP	TCP/UDP	100	GMTP	gmtp	Cisco IOS XE Release 3.1S
Go-Login	TCP/UDP	491	Go-login	go-login	Cisco IOS XE Release 3.1S
Gopher	TCP/UDP	70	Gopher	gopher	Cisco IOS XE Release 3.1S
Graphics	TCP/UDP	41	グラフィックス（Graphics）	graphics	Cisco IOS XE Release 3.1S
GRE	TCP/UDP	47	総称ルーティングカプセル化	gre	Cisco IOS XE Release 3.1S
Groove	TCP/UDP	2492	Groove	groove	Cisco IOS XE Release 3.1S
GSS-HTTP	TCP/UDP	488	gss-http	gss-http	Cisco IOS XE Release 3.1S
GSS-XLICEN	TCP/UDP	128	GNU Generation Foundation NCP	gss-xlicen	Cisco IOS XE Release 3.1S
GTP-User	TCP/UDP	2152	GTP-ユーザ プレーン	gtp-user	Cisco IOS XE Release 3.1S
HA-Cluster	TCP/UDP	694	ha-cluster	ha-cluster	Cisco IOS XE Release 3.1S
HAP	TCP/UDP	661	hap	hap	Cisco IOS XE Release 3.1S
Hassle	TCP/UDP	375	Hassle	hassle	Cisco IOS XE Release 3.1S
HCP-Wismar	TCP/UDP	686	ハードウェア制御プロトコル Wismar	hcp-wismar	Cisco IOS XE Release 3.1S
HDAP	TCP/UDP	263	hdap	hdap	Cisco IOS XE Release 3.1S
Hello-port	TCP/UDP	652	HELLO_PORT	hello-port	Cisco IOS XE Release 3.1S
HEMS	TCP/UDP	151	hems	hems	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	HIP	TCP/UDP	139	ホスト識別プロトコル	hip
	HL7	TCP	動的に割り当て	Health Level Seven	hl7
HMMP-IND	TCP/UDP	612	HMMP 表示	hmmp-ind	Cisco IOS XE Release 3.1S
HMMP-OP	TCP/UDP	613	HMMP 処理	hmmp-op	Cisco IOS XE Release 3.1S
HMP	TCP/UDP	20	ホスト モニタリング	hmp	Cisco IOS XE Release 3.1S
HOPOPT	TCP/UDP	0	IPv6 ホップバイホップ オプション	hopopt	Cisco IOS XE Release 3.1S
Hostname	TCP/UDP	101	NIC ホスト ネーム サーバ	hostname	Cisco IOS XE Release 3.1S
HP-Alarm-Mgr	TCP/UDP	383	HP パフォーマンス データ アラーム マネージャ	hp-alarm-mgr	Cisco IOS XE Release 3.1S
HP-Collector	TCP/UDP	381	HP パフォーマンス データ コレクター	hp-collector	Cisco IOS XE Release 3.1S
HP-Managed-Node	TCP/UDP	382	HP パフォーマンス データ 管理対象ノード	hp-managed-node	Cisco IOS XE Release 3.1S
HTTP-ALT	TCP/UDP	8080	HTTP 代替	http-alt	Cisco IOS XE Release 3.1S
HTTP-Mgmt	TCP/UDP	280	http-mgmt	http-mgmt	Cisco IOS XE Release 3.1S
HTTP-RPC-EPMAP	TCP/UDP	593	HTTP RPC Ep Map	http-rpc-epmap	Cisco IOS XE Release 3.1S
Hybrid-POP	TCP/UDP	473	Hybrid-pop	hybrid-pop	Cisco IOS XE Release 3.1S
Hyper-G	TCP/UDP	418	Hyper-g	hyper-g	Cisco IOS XE Release 3.1S
Hyperwave-ISP	TCP/UDP	692	Hyperwave-isp	hyperwave-isp	Cisco IOS XE Release 3.1S
IAFDBase	TCP/UDP	480	iafdbase	iafdbase	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
IAFServer	TCP/UDP	479	iafserver	iafserver	Cisco IOS XE Release 3.1S
IASD	TCP/UDP	432	iasd	iasd	Cisco IOS XE Release 3.1S
IATP	TCP/UDP	117	インタラクティブエージェント転送プロトコル	iatp	Cisco IOS XE Release 3.1S
IBM-App	TCP/UDP	385	IBM アプリケーション	ibm-app	Cisco IOS XE Release 3.1S
	IBM-DB2	TCP/UDP	523	IBM-DB2	ibm-db2
IBProtocol	TCP/UDP	6714	インターネット バックプレーン プロトコル	ibprotocol	Cisco IOS XE Release 3.1S
ICLCNet-Locate	TCP/UDP	886	ICL coNETion locate server	iclcnet-locate	Cisco IOS XE Release 3.1S
ICLNet_SVInfo	TCP/UDP	887	ICL coNETion server info	iclcnet_svinfo	Cisco IOS XE Release 3.1S
ICMP	TCP/UDP	1	インターネット制御メッセージ	icmp	Cisco IOS XE Release 3.1S
IDFP	TCP/UDP	549	idfp	idfp	Cisco IOS XE Release 3.1S
IDPR	TCP/UDP	35	ドメイン間ポリシー ルーティング プロトコル	idpr	Cisco IOS XE Release 3.1S
IDPRr-CMTP	TCP/UDP	38	IDPR 制御メッセージ トランスポート プロトコル	idpr-cmtp	Cisco IOS XE Release 3.1S
IDRP	TCP/UDP	45	ドメイン間ルーティング プロトコル	idrp	Cisco IOS XE Release 3.1S
IEEE-MMS	TCP/UDP	651	ieee-mms	ieee-mms	Cisco IOS XE Release 3.1S
IEEE-MMS-SSL	TCP/UDP	695	ieee-mms-ssl	ieee-mms-ssl	Cisco IOS XE Release 3.1S
IFMP	TCP/UDP	101	Ipsilon フロー管理プロトコル	ifmp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
IGRP	TCP/UDP	9	シスコ内部ゲートウェイ	igrp	Cisco IOS XE Release 3.1S
IIOP	TCP/UDP	535	iiop	iiop	Cisco IOS XE Release 3.1S
IL	TCP/UDP	40	IL トランスポートプロトコル	il	Cisco IOS XE Release 3.1S
IMSP	TCP/UDP	406	インタラクティブ メール支援プロトコル	imsp	Cisco IOS XE Release 3.1S
InBusiness	TCP/UDP	244	Inbusiness	inbusiness	Cisco IOS XE Release 3.1S
Infoseek	TCP/UDP	414	InfoSeek	infoseek	Cisco IOS XE Release 3.1S
Ingres-Net	TCP/UDP	134	INGRES-NET Service	ingres-net	Cisco IOS XE Release 3.1S
	I-NLSP	TCP/UDP	52	Integrated Net Layer Security TUBA	i-nlsp
Intecourier	TCP/UDP	495	Intecourier	intecourier	Cisco IOS XE Release 3.1S
Integra-SME	TCP/UDP	484	Integra ソフトウェア管理環境	integra-sme	Cisco IOS XE Release 3.1S
Intrinsia	TCP/UDP	503	intrinsa	intrinsa	Cisco IOS XE Release 3.1S
IPCD	TCP/UDP	576	ipcd	ipcd	Cisco IOS XE Release 3.1S
IPComp	TCP/UDP	108	IP ペイロード圧縮プロトコル	ipcomp	Cisco IOS XE Release 3.1S
IPCServer	TCP/UDP	600	Sun IPC サーバ	ipcserver	Cisco IOS XE Release 3.1S
IPCV	TCP/UDP	71	インターネットパケットコア ユーティリティ	ipcv	Cisco IOS XE Release 3.1S
IPDD	TCP/UDP	578	ipdd	ipdd	Cisco IOS XE Release 3.1S
IPINIP	TCP/UDP	4	IP in IP	ipinip	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
IPIP	TCP/UDP	94	IP-within-IP カプセル化プロトコル	ipip	Cisco IOS XE Release 3.1S
IPLT	TCP/UDP	129	IPLT	iplt	Cisco IOS XE Release 3.1S
IPP	TCP/UDP	631	インターネット印刷プロトコル	ipp	Cisco IOS XE Release 3.1S
IPPC	TCP/UDP	67	Internet Pluribus Packet Core	ippc	Cisco IOS XE Release 3.1S
Ipv6-Frag	TCP/UDP	44	Fragment Header for IPv6	ipv6-frag	Cisco IOS XE Release 3.1S
Ipv6-ICMP	TCP/UDP	58	IPv6 の ICMP	ipv6-icmp	Cisco IOS XE Release 3.1S
Ipv6INIP	TCP/UDP	41	Ipv6 encapsulated	ipv6inip	Cisco IOS XE Release 3.1S
ipv6-NonXT	TCP/UDP	59	No Next Header for IPv6	ipv6-nonxt	Cisco IOS XE Release 3.1S
	Ipv6-OPTS	TCP/UDP	60	Destination Options for IPv6	ipv6-opts
Ipv6-Route	TCP/UDP	43	Routing Header for IPv6	ipv6-route	Cisco IOS XE Release 3.1S
IRC	TCP/UDP	194	インターネット リレーチャット	irc	Cisco IOS XE Release 3.1S
IRC-SERV	TCP/UDP	529	IRC-SERV	irc-serv	Cisco IOS XE Release 3.1S
IRTP	TCP/UDP	36	インターネット高信頼性トランザクション	irtp	Cisco IOS XE Release 3.1S
IS99C	TCP/UDP	379	TIA/EIA/IS-99 モデム クライアント	is99c	Cisco IOS XE Release 3.1S
IS99S	TCP/UDP	380	TIA/EIA/IS-99 モデム サーバ	is99s	Cisco IOS XE Release 3.1S
ISAKMP	UDP	500、4500	Internet Security Association & Key Management Protocol	isakmp	Cisco IOS XE Release 3.1S
ISI-GI	TCP/UDP	55	ISI Graphics Language	isi-gl	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ISIS	TCP/UDP	124	ISIS over IPv4	isis	Cisco IOS XE Release 3.1S
ISO-ILL	TCP/UDP	499	ISO ILL プロトコル	iso-ill	Cisco IOS XE Release 3.1S
ISO-IP	TCP/UDP	147	iso-ip	iso-ip	Cisco IOS XE Release 3.1S
ISO-TP0	TCP/UDP	146	iso-tp0	iso-tp0	Cisco IOS XE Release 3.1S
ISO-TP4	TCP/UDP	29	ISO トランスポート プロトコル クラス 4	iso-tp4	Cisco IOS XE Release 3.1S
ISO-TSAP	TCP/UDP	102	ISO-TSAP クラス 0	iso-tsap	Cisco IOS XE Release 3.1S
ISO-TSAP-C2	TCP/UDP	399	ISO トランスポート クラス 2 非制御	iso-tsap-c2	Cisco IOS XE Release 3.1S
ITM-MCELL-S	TCP/UDP	828	itm-mcell-s	itm-mcell-s	Cisco IOS XE Release 3.1S
IXP-IN-IP	TCP/UDP	111	IPX in IP	ixp-in-ip	Cisco IOS XE Release 3.1S
Jargon	TCP/UDP	148	Jargon	jargon	Cisco IOS XE Release 3.1S
	Kali	TCP/UDP	2213	Kali	kali
	K-Block	TCP/UDP	287	K-block	k-block
Keyserver	TCP/UDP	584	キー サーバ	keyserver	Cisco IOS XE Release 3.1S
KIS	TCP/UDP	186	KIS プロトコル	kis	Cisco IOS XE Release 3.1S
Klogin	TCP/UDP	543	klogin	klogin	Cisco IOS XE Release 3.1S
Knet-CMP	TCP/UDP	157	KNET/VM コマンド/メッセージ プロトコル	knet-cmp	Cisco IOS XE Release 3.1S
Konspire2b	TCP/UDP	6085	Konspire2b p2p ネットワーク	Konspire2b	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Kpasswd	TCP/UDP	464	Kpasswd	kpasswd	Cisco IOS XE Release 3.1S
Kryptolan	TCP/UDP	398	Kryptolan	kryptolan	Cisco IOS XE Release 3.1S
Kshell	TCP/UDP	544	Kshell	kshell	Cisco IOS XE Release 3.1S
L2TP	TCP/UDP	1701	l2tp	l2tp	Cisco IOS XE Release 3.1S
LA-Maint	TCP/UDP	51	IMP 論理アドレス メンテナンス	la-maint	Cisco IOS XE Release 3.1S
LANServer	TCP/UDP	637	lanserver	lanserver	Cisco IOS XE Release 3.1S
LARP	TCP/UDP	91	Locus アドレス解決プロトコル	larp	Cisco IOS XE Release 3.1S
LDAP	TCP/UDP	389	Lightweight Directory Access Protocol	ldap	Cisco IOS XE Release 3.1S
LDP	TCP/UDP	646	LDP	ldp	Cisco IOS XE Release 3.1S
Leaf-1	TCP/UDP	25	Leaf-1	leaf-1	Cisco IOS XE Release 3.1S
Leaf-2	TCP/UDP	26	Leaf-2	leaf-2	Cisco IOS XE Release 3.1S
Legent-1	TCP/UDP	373	Legent Corporation	legent-1	Cisco IOS XE Release 3.1S
	Legent-2	TCP/UDP	374	Legent Corporation	legent-2
LJK-Login	TCP/UDP	472	ljk-login	ljk-login	Cisco IOS XE Release 3.1S
Lockd	TCP/UDP	4045	NFS Lock Daemon Manager	lockd	Cisco IOS XE Release 3.1S
Locus-Con	TCP/UDP	127	Locus PC-Interface Conn Server	locus-con	Cisco IOS XE Release 3.1S
Locus-Map	TCP/UDP	125	Locus PC-Interface Net Map Ser	locus-map	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
MAC-SRVR-Admin	TCP/UDP	660	MacOS Server Admin	mac-srvr-admin	Cisco IOS XE Release 3.1S
Magenta-Logic	TCP/UDP	313	Magenta-logic	magenta-logic	Cisco IOS XE Release 3.1S
Mailbox-LM	TCP/UDP	505	Mailbox-lm	mailbox-lm	Cisco IOS XE Release 3.1S
Mailq	TCP/UDP	174	MAILQ	mailq	Cisco IOS XE Release 3.1S
Maitrd	TCP/UDP	997	Maitrd	maitrd	Cisco IOS XE Release 3.1S
MANET	TCP/UDP	138	MANET プロトコル	manet	Cisco IOS XE Release 3.1S
MasqDialer	TCP/UDP	224	Masqdialer	masqdialer	Cisco IOS XE Release 3.1S
Matip-Type-A	TCP/UDP	350	MATIP Type A	matip-type-a	Cisco IOS XE Release 3.1S
Matip-Type-B	TCP/UDP	351	MATIP Type B	matip-type-b	Cisco IOS XE Release 3.1S
MCIDAS	TCP/UDP	112	McIDAS データ伝送プロトコル	mcidas	Cisco IOS XE Release 3.1S
MCNS-Sec	TCP/UDP	638	mcns-sec	mcns-sec	Cisco IOS XE Release 3.1S
MDC-Portmapper	TCP/UDP	685	mdc-portmapper	mdc-portmapper	Cisco IOS XE Release 3.1S
MeComm	TCP/UDP	668	MeComm	mecomm	Cisco IOS XE Release 3.1S
	MeRegister	TCP/UDP	669	MeRegister	meregister
Merit-INP	TCP/UDP	32	MERIT ノード間プロトコル	merit-inp	Cisco IOS XE Release 3.1S
Meta5	TCP/UDP	393	Meta5	meta5	Cisco IOS XE Release 3.1S
Metagram	TCP/UDP	99	Metagram	metagram	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Meter	TCP/UDP	570	Meter	meter	Cisco IOS XE Release 3.1S
Mfcobol	TCP/UDP	86	Micro Focus Cobol	mfcobol	Cisco IOS XE Release 3.1S
MFE-NSP	TCP/UDP	31	MFE ネットワーク サービス プロトコル	mfe-nsp	Cisco IOS XE Release 3.1S
MFTP	TCP/UDP	349	mftp	mftp	Cisco IOS XE Release 3.1S
Micom-PFS	TCP/UDP	490	Micom-pfs	micom-pfs	Cisco IOS XE Release 3.1S
MICP	TCP/UDP	95	モバイル インターネットワーキング制御プロトコル	micp	Cisco IOS XE Release 3.1S
Micromuse-LM	TCP/UDP	1534	micromuse-lm	micromuse-lm	Cisco IOS XE Release 3.1S
MIT-DOV	TCP/UDP	91	MIT Dover Spooler	mit-dov	Cisco IOS XE Release 3.1S
MIT-ML-Dev	TCP/UDP	83	MIT ML Device	mit-ml-dev	Cisco IOS XE Release 3.1S
Mobile	TCP/UDP	55	IP モビリティ	mobile	Cisco IOS XE Release 3.1S
モバイル IP エージェント	TCP/UDP	434	mobileip-agent	mobileip-agent	Cisco IOS XE Release 3.1S
MobilIP-MN	TCP/UDP	435	mobilip-mn	mobilip-mn	Cisco IOS XE Release 3.1S
Mondex	TCP/UDP	471	Mondex	mondex	Cisco IOS XE Release 3.1S
Monitor	TCP/UDP	561	モニタ（Monitor）	monitor	Cisco IOS XE Release 3.1S
Mortgageware	TCP/UDP	367	Mortgageware	mortgageware	Cisco IOS XE Release 3.1S
	MPLS-IN-IP	TCP/UDP	137	MPLS-in-IP	mpls-in-ip
MPM	TCP/UDP	45	メッセージ処理モジュール	mpm	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
MPM-Flags	TCP/UDP	44	MPM FLAGS プロトコル	mpm-flags	Cisco IOS XE Release 3.1S
MPM-SND	TCP/UDP	46	MPM [default send]	mpm-snd	Cisco IOS XE Release 3.1S
MPP	TCP/UDP	218	Netix メッセージ投稿プロトコル	mpp	Cisco IOS XE Release 3.1S
MPTN	TCP/UDP	397	Multi Protocol Transport Network	mptn	Cisco IOS XE Release 3.1S
MRM	TCP/UDP	679	mrm	mrm	Cisco IOS XE Release 3.1S
MSDP	TCP/UDP	639	msdp	msdp	Cisco IOS XE Release 3.1S
MSExch-Routing	TCP/UDP	691	MS Exchange ルーティング	msexch-routing	Cisco IOS XE Release 3.1S
MSFT-GC	TCP/UDP	3268	Microsoft グローバル カタログ	msft-gc	Cisco IOS XE Release 3.1S
MSFT-GC-SSL	TCP/UDP	3269	LDAP/SSL を使用した Microsoft グローバル カタログ	msft-gc-ssl	Cisco IOS XE Release 3.1S
MSG-AUTH	TCP/UDP	31	msg-auth	msg-auth	Cisco IOS XE Release 3.1S
MSG-ICP	TCP/UDP	29	msg-icp	msg-icp	Cisco IOS XE Release 3.1S
MSNP	TCP/UDP	1863	msnp	msnp	Cisco IOS XE Release 3.1S
MS-OLAP	TCP/UDP	2393	Microsoft OLAP	ms-olap	Cisco IOS XE Release 3.1S
MSP	TCP/UDP	18	Message Send Protocol	msp	Cisco IOS XE Release 3.1S
MS-Rome	TCP/UDP	569	Microsoft rome	ms-rome	Cisco IOS XE Release 3.1S
MS-Shuttle	TCP/UDP	568	Microsoft shuttle	ms-shuttle	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
MS-SQLl-M	TCP/UDP	1434	Microsoft-SQL-Monitor	ms-sql-m	Cisco IOS XE Release 3.1S
	MS-wbt	TCP	3389/ヒューリスティック	Microsoft Windows ベース Terminal Services	ms-wbt
	MTP	TCP/UDP	92	マルチキャスト トランスポート プロトコル	mtp
Multiling-HTTP	TCP/UDP	777	Multiling HTTP	multiling-http	Cisco IOS XE Release 3.1S
Multiplex	TCP/UDP	171	Network Innovations Multiplex	multiplex	Cisco IOS XE Release 3.1S
Mumps	TCP/UDP	188	Plus Fives MUMPS	mumps	Cisco IOS XE Release 3.1S
MUX	TCP/UDP	18	多重化	mux	Cisco IOS XE Release 3.1S
Mylex-MAPD	TCP/UDP	467	mylex-mapd	mylex-mapd	Cisco IOS XE Release 3.1S
MySQL	TCP/UDP	3306	MySQL	mysql	Cisco IOS XE Release 3.1S
Name	TCP/UDP	54	ホスト ネーム サーバ	name	Cisco IOS XE Release 3.1S
NAMP	TCP/UDP	167	namp	namp	Cisco IOS XE Release 3.1S
NARP	TCP/UDP	54	NBMA アドレス解決プロトコル	narp	Cisco IOS XE Release 3.1S
NAS	TCP/UDP	991	ネットニュース管理システム	nas	Cisco IOS XE Release 3.1S
NCED	TCP/UDP	404	nced	nced	Cisco IOS XE Release 3.1S
NCLD	TCP/UDP	405	ncld	ncld	Cisco IOS XE Release 3.1S
NCP	TCP/UDP	524	NCP	ncp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
NDSAuth	TCP/UDP	353	NDSAUTH	ndsauth	Cisco IOS XE Release 3.1S
Nest-Protocol	TCP/UDP	489	Nest-protocol	nest-protocol	Cisco IOS XE Release 3.1S
Net8-CMAN	TCP/UDP	1830	Oracle Net8 CMan Admin	net8-cman	Cisco IOS XE Release 3.1S
Net-Assistant	TCP/UDP	3283	net-assistant	net-assistant	Cisco IOS XE Release 3.1S
Netblt	TCP/UDP	30	一括データ転送プロトコル	netblt	Cisco IOS XE Release 3.1S
	NetGW	TCP/UDP	741	netgw	netgw
	NetNews	TCP/UDP	532	readnews	netnews
NetRCS	TCP/UDP	742	ネットワーク ベース RCS	netrcs	Cisco IOS XE Release 3.1S
NetRJS-1	TCP/UDP	71	リモート ジョブ サービス	netrjs-1	Cisco IOS XE Release 3.1S
NetRJS-2	TCP/UDP	72	リモート ジョブ サービス	netrjs-2	Cisco IOS XE Release 3.1S
NetRJS-3	TCP/UDP	73	リモート ジョブ サービス	netrjs-3	Cisco IOS XE Release 3.1S
NetRJS-4	TCP/UDP	74	リモート ジョブ サービス	netrjs-4	Cisco IOS XE Release 3.1S
NETSC-Dev	TCP/UDP	155	NETSC	netsc-dev	Cisco IOS XE Release 3.1S
NETSC-Prod	TCP/UDP	154	NETSC	netsc-prod	Cisco IOS XE Release 3.1S
NetViewDM1	TCP/UDP	729	IBM NetView M	netviewdm1	Cisco IOS XE Release 3.1S
NetviewDM2	TCP/UDP	730	IBM NetView DM	netviewdm2	Cisco IOS XE Release 3.1S
NetviewDM3	TCP/UDP	731	IBM NetView DM	netviewdm3	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Netwall	TCP/UDP	533	緊急放送向け	netwall	Cisco IOS XE Release 3.1S
Netware-IP	TCP/UDP	396	Novell Netware over IP	netware-ip	Cisco IOS XE Release 3.1S
New-RWHO	TCP/UDP	550	new who	new-rwho	Cisco IOS XE Release 3.1S
NextStep	TCP/UDP	178	NextStep Window Server	nextstep	Cisco IOS XE Release 3.1S
NFS	TCP/UDP	2049	ネットワーク ファイル システム	nfs	Cisco IOS XE Release 3.1S
NicName	TCP/UDP	43	Who Is	nicname	Cisco IOS XE Release 3.1S
NI-FTP	TCP/UDP	47	NI FTP	ni-ftp	Cisco IOS XE Release 3.1S
NI-Mail	TCP/UDP	61	NI MAIL	ni-mail	Cisco IOS XE Release 3.1S
	Nlogin	TCP/UDP	758	nlogin	nlogin
	NMAP	TCP/UDP	689	nmap	nmap
NMSP（NMSP）	TCP/UDP	537	ネットワーク メディア ストリーミング プロトコル	nmsp	Cisco IOS XE Release 3.1S
NNSP	TCP/UDP	433	nnsp	nnsp	Cisco IOS XE Release 3.1S
Notes	TCP/UDP	1352	Lotus Notes(R)	notes	Cisco IOS XE Release 3.1S
NovaStorBakcup	TCP/UDP	308	Novastor Backup	novastorbakcup	Cisco IOS XE Release 3.1S
NPMP-GUI	TCP/UDP	611	npmp-gui	npmp-gui	Cisco IOS XE Release 3.1S
NPMP-Local	TCP/UDP	610	npmp-local	npmp-local	Cisco IOS XE Release 3.1S
NPMP-Trap	TCP/UDP	609	npmp-trap	npmp-trap	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
NPP	TCP/UDP	92	ネットワーク印刷プロトコル	npp	Cisco IOS XE Release 3.1S
NQS	TCP/UDP	607	nqs	nqs	Cisco IOS XE Release 3.1S
NS	TCP/UDP	760	ns	ns	Cisco IOS XE Release 3.1S
NSFNET-IGP	TCP/UDP	85	NSFNET-IGP	nsfnet-igp	Cisco IOS XE Release 3.1S
NSIIOPS	TCP/UDP	261	IIOP Name Service over TLS/SSL	nsiiops	Cisco IOS XE Release 3.1S
NSRMP	TCP/UDP	359	ネットワーク セキュリティ リスク マネジメント プロトコル	nsrmp	Cisco IOS XE Release 3.1S
NSS-Routing	TCP/UDP	159	NSS-Routing	nss-routing	Cisco IOS XE Release 3.1S
NSW-FE	TCP/UDP	27	NSW User System FE	nsw-fe	Cisco IOS XE Release 3.1S
Ntalk	TCP/UDP	518	Ntalk	ntalk	Cisco IOS XE Release 3.1S
NTP	TCP/ UDP	123	ネットワーク タイム プロトコル	ntp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S
	NVP-II	TCP/UDP	11	ネットワーク音声プロトコル	nvp-ii
NXEdit	TCP/UDP	126	nxedit	nxedit	Cisco IOS XE Release 3.1S
OBCBinder	TCP/UDP	183	ocbinder	ocbinder	Cisco IOS XE Release 3.1S
OBEX	TCP/UDP	650	obex	obex	Cisco IOS XE Release 3.1S
ObjCall	TCP/UDP	94	Tivoli Object Dispatcher	objcall	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
OCS_AMU	TCP/UDP	429	ocs_amu	ocs_amu	Cisco IOS XE Release 3.1S
OCS_CMU	TCP/UDP	428	ocs_cmu	ocs_cmu	Cisco IOS XE Release 3.1S
OCServer	TCP/UDP	184	ocserver	ocserver	Cisco IOS XE Release 3.1S
ODMR	TCP/UDP	366	odmr	odmr	Cisco IOS XE Release 3.1S
OHIMSRV	TCP/UDP	506	ohimsrv	ohimsrv	Cisco IOS XE Release 3.1S
OLSR	TCP/UDP	698	olsr	olsr	Cisco IOS XE Release 3.1S
OMGInitialRefs	TCP/UDP	900	omginitialrefs	omginitialrefs	Cisco IOS XE Release 3.1S
OMServ	TCP/UDP	764	omserv	omserv	Cisco IOS XE Release 3.1S
ONMUX	TCP/UDP	417	onmux	onmux	Cisco IOS XE Release 3.1S
Opalis-RDV	TCP/UDP	536	Opalis-rdv	opalis-rdv	Cisco IOS XE Release 3.1S
Opalis-Robot	TCP/UDP	314	oOpalis-robot	opalis-robot	Cisco IOS XE Release 3.1S
OPC-Job-Start	TCP/UDP	423	IBM Operations Planning and Control Start	opc-job-start	Cisco IOS XE Release 3.1S
OPC-Job-Track	TCP/UDP	424	IBM Operations Planning and Control Track	opc-job-track	Cisco IOS XE Release 3.1S
	Openport	TCP/UDP	260	Openport	openport
OpenVMS-Sysipc	TCP/UDP	557	Openvms-sysipc	openvms-sysipc	Cisco IOS XE Release 3.1S
OracleNames	TCP/UDP	1575	Oraclenames	oraclenames	Cisco IOS XE Release 3.1S
OracleNet8CMAN	TCP/UDP	1630	Oracle Net8 Cman	oraclenet8cman	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
ORA-Srv	TCP/UDP	1525	Oracle TCP/IP Listener	ora-srv	12.2(18)ZYA 12.2(18)ZYA Cisco IOS XE Release 3.1S
Orbix-Config	TCP/UDP	3076	Orbix 2000 Config	orbix-config	Cisco IOS XE Release 3.1S
Orbix-Locator	TCP/UDP	3075	Orbix 2000 Locator	orbix-locator	Cisco IOS XE Release 3.1S
Orbix-Loc-SSL	TCP/UDP	3077	Orbix 2000 Locator SSL	orbix-loc-ssl	Cisco IOS XE Release 3.1S
OSPF	TCP/UDP	89	Open Shortest Path First	ospf	Cisco IOS XE Release 3.1S
OSU-NMS	TCP/UDP	192	OSUネットワーク モニタリング システム	osu-nms	Cisco IOS XE Release 3.1S
Parsec-Game	TCP/UDP	6582	Parsec Gameserver	parsec-game	Cisco IOS XE Release 3.1S
Passgo	TCP/UDP	511	Passgo	passgo	Cisco IOS XE Release 3.1S
Passgo-Tivoli	TCP/UDP	627	Passgo-tivoli	passgo-tivoli	Cisco IOS XE Release 3.1S
Password-Chg	TCP/UDP	586	パスワードの変更	password-chg	Cisco IOS XE Release 3.1S
Pawserv	TCP/UDP	345	Perf Analysis Workbench	pawserv	Cisco IOS XE Release 3.1S
PCMail-SRV	TCP/UDP	158	PCMail サーバ	pcmail-srv	Cisco IOS XE Release 3.1S
PDAP	TCP/UDP	344	Prosperoデータ アクセス プロトコル	pdap	Cisco IOS XE Release 3.1S
Personal-link	TCP/UDP	281	Personal-link	personal-link	Cisco IOS XE Release 3.1S
PFTP	TCP/UDP	662	パラレル ファイル転送プロトコル	pftp	Cisco IOS XE Release 3.1S
	PGM	TCP/UDP	113	PGM 高信頼性トランスポート プロトコル	pgm

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Philips-VC	TCP/UDP	583	Philips ビデオ会議	philips-vc	Cisco IOS XE Release 3.1S
Phonebook	TCP/UDP	767	電話	phonebook	Cisco IOS XE Release 3.1S
Photuris	TCP/UDP	468	Photuris	photuris	Cisco IOS XE Release 3.1S
PIM	TCP/UDP	103	Protocol Independent Multicast	pim	Cisco IOS XE Release 3.1S
PIM-RP-DISC	TCP/UDP	496	PIM-RP-DISC	pim-rp-disc	Cisco IOS XE Release 3.1S
PIP	TCP/UDP	1321	pip	pip	Cisco IOS XE Release 3.1S
PIPE	TCP/UDP	131	Private IP Encapsulation within IP	pipe	Cisco IOS XE Release 3.1S
PIRP	TCP/UDP	553	pirp	pirp	Cisco IOS XE Release 3.1S
PKIX-3-CA-RA	TCP/UDP	829	PKIX-3 CA/RA	pkix-3-ca-ra	Cisco IOS XE Release 3.1S
PKIX-Timestamp	TCP/UDP	318	pkix-timestamp	pkix-timestamp	Cisco IOS XE Release 3.1S
PNNI	TCP/UDP	102	PNNI over IP	pnni	Cisco IOS XE Release 3.1S
Pop2	TCP/UDP	109	Post Office Protocol（POP）Version 2	pop2	Cisco IOS XE Release 3.1S
Pop3	TCP/UDP	110、ヒューリスティック	Post Office Protocol 3	pop3	Cisco IOS XE Release 3.1S
POV-Ray	TCP/UDP	494	pov-ray	pov-ray	Cisco IOS XE Release 3.1S
Powerburst	TCP/UDP	485	Air Soft Power Burst	powerburst	Cisco IOS XE Release 3.1S
PPStream	TCP/UDP	ヒューリスティック	P2P TV アプリケーション	ppstream	Cisco IOS XE リリース 3.3S
PPTP	TCP/UDP	1723	ポイントツーポイントトンネリング プロトコル	pptp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	プリンタ	TCP/UDP	515	spooler	printer
Print-SRV	TCP/UDP	170	Network PostScript	print-srv	Cisco IOS XE Release 3.1S
PRM	TCP/UDP	21	Packet Radio Measurement	prm	Cisco IOS XE Release 3.1S
PRM-NM	TCP/UDP	409	Prospero Resource Manager Node Man	prm-nm	Cisco IOS XE Release 3.1S
PRM-SM	TCP/UDP	408	Prospero Resource Manager Sys.Man	prm-sm	Cisco IOS XE Release 3.1S
Profile	TCP/UDP	136	PROFILE Naming System	profile	Cisco IOS XE Release 3.1S
Prospero	TCP/UDP	191	Prosper Directory Service	prospero	Cisco IOS XE Release 3.1S
PTCNameService	TCP/UDP	597	PTC Name Service	ptcnameservice	Cisco IOS XE Release 3.1S
PTP	TCP/UDP	123	Performance Transparency Protocol	ptp	Cisco IOS XE Release 3.1S
PTP-Event	TCP/UDP	319	PTP イベント	ptp-event	Cisco IOS XE Release 3.1S
PTP-General	TCP/UDP	320	PTP General	ptp-general	Cisco IOS XE Release 3.1S
Pump	TCP/UDP	751	Pump	pump	Cisco IOS XE Release 3.1S
PUP	TCP/UDP	12	PUP	pup	Cisco IOS XE Release 3.1S
Purenoise	TCP/UDP	663	purenoise	purenoise	Cisco IOS XE Release 3.1S
PVP	TCP/UDP	75	パケットビデオプロトコル	pvp	Cisco IOS XE Release 3.1S
PWDGen	TCP/UDP	129	Password Generator Protocol	pwdgen	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
QBIKGDP	TCP/UDP	368	qbikgdp	qbikgdp	Cisco IOS XE Release 3.1S
QFT	TCP/UDP	189	Queued File Transport	qft	Cisco IOS XE Release 3.1S
QMQP	TCP/UDP	628	qmqp	qmqp	Cisco IOS XE Release 3.1S
	QMTP	TCP/UDP	209	クイック メール転送プロトコル	qmtp
	QNX	TCP/UDP	106	QNX	qnx
QoTD	TCP/UDP	17	Quote of the Day	qotd	Cisco IOS XE Release 3.1S
QRH	TCP/UDP	752	qrh	qrh	Cisco IOS XE Release 3.1S
QUOTD	TCP/UDP	762	quotad	quotad	Cisco IOS XE Release 3.1S
r-commands	TCP	動的に割り当て	rsh、rlogin、rexec	rcmd	12.0(5)XE2 12.1(1)E 12.1(5) 12.2(18)ZYA1
RAP	TCP/UDP	38	ルートアクセスプロトコル	rap	Cisco IOS XE Release 3.1S
RCMD	TCP	512–514	BSD r-コマンド	rcmd	Cisco IOS XE リリース 3.3S
RCP	TCP/UDP	469	無線制御プロトコル	rcp	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisc IOS XE Release 3.1S
RDA	TCP/UDP	630	rda	rda	Cisco IOS XE Release 3.1S
RDB-DBS-DISP	TCP/UDP	1571	Oracle リモート データベース	rdb-dbs-disp	Cisco IOS XE Release 3.1S
RDP	TCP/UDP	27	高信頼性データ プロトコル	rdp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Realm-RUSD	TCP/UDP	688	ApplianceWare 管理プロトコル	realm-rusd	Cisco IOS XE Release 3.1S
RE-Mail-CK	TCP/UDP	50	リモート メール確認プロトコル	re-mail-ck	Cisco IOS XE Release 3.1S
RemoteFS	TCP/UDP	556	rfs サーバ	remotefs	Cisco IOS XE Release 3.1S
Remote-KIS	TCP/UDP	185	Remote-kis	remote-kis	Cisco IOS XE Release 3.1S
REPCMD	TCP/UDP	641	repcmd	repcmd	Cisco IOS XE Release 3.1S
REPSCMD	TCP/UDP	653	repscmd	repscmd	Cisco IOS XE Release 3.1S
RESCAP	TCP/UDP	283	rescap	rescap	Cisco IOS XE Release 3.1S
RIP	TCP/UDP	520	Routing Information Protocol	rip	Cisco IOS XE Release 3.1S
	RIPING	TCP/UDP	521	ripng	ripng
	RIS	TCP/UDP	180	Intergraph	ris
RIS-CM	TCP/UDP	748	Russell Info Sci Calendar Manager	ris-cm	Cisco IOS XE Release 3.1S
RJE	TCP/UDP	5	リモート ジョブ エントリ	rje	Cisco IOS XE Release 3.1S
RLP	TCP/UDP	39	リソース ロケーション プロトコル	rlp	Cisco IOS XE Release 3.1S
RLZDBASE	TCP/UDP	635	rlzdbase	rlzdbase	Cisco IOS XE Release 3.1S
RMC	TCP/UDP	657	rmc	rmc	Cisco IOS XE Release 3.1S
RMIActivation	TCP/UDP	1098	rmiactivation	rmiactivation	Cisco IOS XE Release 3.1S
RMIRegistry	TCP/UDP	1099	rmiregistry	rmiregistry	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
RMonitor	TCP/UDP	560	Rmonitord	rmonitor	Cisco IOS XE Release 3.1S
RMT	TCP/UDP	411	リモート MT プロトコル	rmt	Cisco IOS XE Release 3.1S
RPC2Portmap	TCP/UDP	369	rpc2portmap	rpc2portmap	Cisco IOS XE Release 3.1S
RRH	TCP/UDP	753	rrh	rrh	Cisco IOS XE Release 3.1S
RRP	TCP/UDP	648	Registry Registrar Protocol	rrp	Cisco IOS XE Release 3.1S
RSH-SPX	TCP/UDP	222	Berkeley rshd with SPX auth	rsh-spx	Cisco IOS XE Release 3.1S
RSVD	TCP/UDP	168	rsvd	rsvd	Cisco IOS XE Release 3.1S
RSVP_Tunnel	TCP/UDP	363	rsvp_tunnel	rsvp_tunnel	Cisco IOS XE Release 3.1S
RSVP-E2E-Ignore	TCP/UDP	134	RSVP-E2E-IGNORE	rsvp-e2e-ignore	Cisco IOS XE Release 3.1S
Rsync	TCP/UDP	873	Rsync	rsync	Cisco IOS XE Release 3.1S
RTelnet	TCP/UDP	107	Remote Telnet Service	rtelnet	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisc IOS XE Release 3.1S
	RTIP	TCP/UDP	771	Real Time Streaming Protocol	rtip
RTMP	TCP	ヒューリスティック	Real Time Messaging Protocol	rtmp	Cisco IOS XE リリース 3.4S
RTSPS	TCP/UDP	322	RTSPS	rtsps	Cisco IOS XE Release 3.1S
Rushd	TCP/UDP	696	Rushd	rushd	Cisco IOS XE Release 3.1S
RVD	TCP/UDP	66	MIT リモート仮想ディスクプロトコル	rvd	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
RXE	TCP/UDP	761	rxe	rxe	Cisco IOS XE Release 3.1S
SAFT	TCP/UDP	487	saft 簡易非同期ファイル転送	saft	Cisco IOS XE Release 3.1S
Sanity	TCP/UDP	643	Sanity	sanity	Cisco IOS XE Release 3.1S
SAT-EXPAK	TCP/UDP	64	SATNET and Backroom EXPAK	sat-expak	Cisco IOS XE Release 3.1S
SAT-Mon	TCP/UDP	69	SATNET モニタリング	sat-mon	Cisco IOS XE Release 3.1S
SCC-Security	TCP/UDP	582	scc-security	scc-security	Cisco IOS XE Release 3.1S
SCC-SP	TCP/UDP	96	Semaphore Communications Sec.Pro.	scc-sp	Cisco IOS XE Release 3.1S
SCO-DTMgr	TCP/UDP	617	SCOデスクトップ管理サーバ	sco-dtmgr	Cisco IOS XE Release 3.1S
SCOHELP	TCP/UDP	457	scohelp	scohelp	Cisco IOS XE Release 3.1S
SCOI2ODialog	TCP/UDP	360	scoi2odialog	scoi2odialog	Cisco IOS XE Release 3.1S
SCO-Inetmgr	TCP/UDP	615	Internet Configuration Manager	sco-inetmgr	Cisco IOS XE Release 3.1S
SCO-SysMgr	TCP/UDP	616	SCO システム管理サーバ	sco-sysmgr	Cisco IOS XE Release 3.1S
SCO-WebsrvrMg3	TCP/UDP	598	SCO Web Server Manager 3	sco-websrvrmg3	Cisco IOS XE Release 3.1S
SCO-WebsrvrMgr	TCP/UDP	620	SCO WebServer Manager	sco-websrvrmgr	Cisco IOS XE Release 3.1S
	SCPS	TCP/UDP	105	SCPS	scps
SCTP	TCP/UDP	132	Stream Control Transmission Protocol（SCTP）	sctp	Cisco IOS XE Release 3.1S
SCX-Proxy	TCP/UDP	470	scx-proxy	scx-proxy	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
SDNSKMP	TCP/UDP	558	SDNSKMP	sdnskmp	Cisco IOS XE Release 3.1S
SDRP	TCP/UDP	54	Source Demand Routing Protocol	sdrp	Cisco IOS XE Release 3.1S
Secure-ftp	TCP/UDP	990	ftp プロトコル、制御、TLS/SSL 上	secure-ftp	Cisco IOS XE Release 3.1S
Secure-IRC	TCP/UDP	994	irc protocol over TLS	secure-irc	Cisco IOS XE Release 3.1S
Secure-LDAP	TCP/UDP	636	ldap protocol over TLS	secure-ldap	Cisco IOS XE Release 3.1S
Secure-NNTP	TCP/UDP	563	nntp protocol over TLS	secure-nntp	Cisco IOS XE Release 3.1S
Secure-Pop3	TCP/UDP	995	pop3 protocol over TLS	secure-pop3	Cisco IOS XE Release 3.1S
Secure-Telnet	TCP/UDP	992	telnet protocol over TLS	secure-telnet	Cisco IOS XE Release 3.1S
Secure-VMTP	TCP/UDP	82	SECURE-VMTP	secure-vmtp	Cisco IOS XE Release 3.1S
Semantix	TCP/UDP	361	Semantix	semantix	Cisco IOS XE Release 3.1S
Send	TCP/UDP	169	SEND	send	Cisco IOS XE Release 3.1S
Server-IPX	TCP/UDP	213	Internetwork Packet Exchange Protocol	server-ipx	Cisco IOS XE Release 3.1S
Servstat	TCP/UDP	633	サービス ステータス更新	servstat	Cisco IOS XE Release 3.1S
SET	TCP/UDP	257	機密保護電子商取引	set	Cisco IOS XE Release 3.1S
SFS-Config	TCP/UDP	452	Cray SFS config server	sfs-config	Cisco IOS XE Release 3.1S
	SFS-SMP-Net	TCP/UDP	451	Cray Network Semaphore server	sfs-smp-net
SFTP	TCP/UDP	115	簡易ファイル転送プロトコル	sftp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
SGCP	TCP/UDP	440	sgcp	sgcp	Cisco IOS XE Release 3.1S
SGMP	TCP/UDP	153	sgmp	sgmp	Cisco IOS XE Release 3.1S
SGMP-Traps	TCP/UDP	160	sgmp-traps	sgmp-traps	Cisco IOS XE Release 3.1S
Shockwave	TCP/UDP	1626	Shockwave	shockwave	Cisco IOS XE Release 3.1S
Shrinkwrap	TCP/UDP	358	Shrinkwrap	shrinkwrap	Cisco IOS XE Release 3.1S
SIAM	TCP/UDP	498	siam	siam	Cisco IOS XE Release 3.1S
SIFT-UFT	TCP/UDP	608	送信者指定型/未承諾ファイル転送	sift-uft	Cisco IOS XE Release 3.1S
SILC	TCP/UDP	706	silc	silc	Cisco IOS XE Release 3.1S
SitaraDir	TCP/UDP	2631	Sitaradir	sitaradir	Cisco IOS XE Release 3.1S
SitaraMgmt	TCP/UDP	2630	Sitaramgmt	sitaramgmt	Cisco IOS XE Release 3.1S
Sitaraserver	TCP/UDP	2629	sitaraserver	sitaraserver	Cisco IOS XE Release 3.1S
SKIP	TCP/UDP	57	SKIP	skip	Cisco IOS XE Release 3.1S
SKRONK	TCP/UDP	460	skronk	skronk	Cisco IOS XE Release 3.1S
SM	TCP/UDP	122	SM	sm	Cisco IOS XE Release 3.1S
Smakynet	TCP/UDP	122	Smakynet	smakynet	Cisco IOS XE Release 3.1S
SmartSDP	TCP/UDP	426	Smartsdp	smartsdp	Cisco IOS XE Release 3.1S
SMP	TCP/UDP	121	簡易メッセージプロトコル	smp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	SMPNameRes	TCP/UDP	901	smpnameres	smpnameres
	SMSD	TCP/UDP	596	smsd	smsd
SMSP	TCP/UDP	413	ストレージ管理サービス プロトコル	smsp	Cisco IOS XE Release 3.1S
SMUX	TCP/UDP	199	SMUX	smux	Cisco IOS XE Release 3.1S
SNAGas	TCP/UDP	108	SNA ゲートウェイ アクセス サーバ	snagas	Cisco IOS XE Release 3.1S
Snare	TCP/UDP	509	Snare	snare	Cisco IOS XE Release 3.1S
S-Net	TCP/UDP	166	Sirius Systems	s-net	Cisco IOS XE Release 3.1S
SNP	TCP/UDP	109	Sitara ネットワーク プロトコル	snp	Cisco IOS XE Release 3.1S
SNPP	TCP/UDP	444	簡易ネットワーク ページング プロトコル	snpp	Cisco IOS XE Release 3.1S
SNTP-Heartbeat	TCP/UDP	580	SNTP HEARTBEAT	sntp-heartbeat	Cisco IOS XE Release 3.1S
SoftPC	TCP/UDP	215	Insignia Solutions	softpc	Cisco IOS XE Release 3.1S
Sonar	TCP/UDP	572	Sonar	sonar	Cisco IOS XE Release 3.1S
SPMP	TCP/UDP	656	spmp	spmp	Cisco IOS XE Release 3.1S
Sprite-RPC	TCP/UDP	90	Sprite RPC プロトコル	sprite-rpc	Cisco IOS XE Release 3.1S
SPS	TCP/UDP	130	セキュア パケット シールド	sps	Cisco IOS XE Release 3.1S
SPSC	TCP/UDP	478	spsc	spsc	Cisco IOS XE Release 3.1S
SQL*Net	TCP/UDP	66	Oracle SQL*NET	sql*net	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
SQLExec	TCP/UDP	9088	SQL Informix	sqlexec	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.1S
SQL-Net	TCP/UDP	150	SQL-NET	sql-net	Cisco IOS XE Release 3.1S
	SQLServ	TCP/UDP	118	SQL サービス	sqlserv
SQLServer	TCP/UDP	1433	Microsoft-SQL-Server	sqlserver	Cisco IOS XE Release 3.1S
SRC	TCP/UDP	200	IBM System Resource Controller	src	Cisco IOS XE Release 3.1S
SRMP	TCP/UDP	193	Spider リモート モニタリング プロトコル	srmp	Cisco IOS XE Release 3.1S
SRP	TCP/UDP	119	SpectraLink 無線プロトコル	srp	Cisco IOS XE Release 3.1S
SRSSend	TCP/UDP	362	srssend	srssend	Cisco IOS XE Release 3.1S
SS7NS	TCP/UDP	477	ss7ns	ss7ns	Cisco IOS XE Release 3.1S
SSCOPMCE	TCP/UDP	128	SSCOPMCE	sscopmce	Cisco IOS XE Release 3.1S
SSH	TCP/UDP	22	セキュア シェル プロトコル	ssh	Cisco IOS XE Release 3.1S
Sshell	TCP/UDP	614	SSLshell	sshell	Cisco IOS XE Release 3.1S
SST	TCP/UDP	266	SCSI on ST	sst	Cisco IOS XE Release 3.1S
ST	TCP/UDP	5	Stream	st	Cisco IOS XE Release 3.1S
StatSRV	TCP/UDP	133	Statistics Service	statsrv	Cisco IOS XE Release 3.1S
STMF	TCP/UDP	501	stmf	stmf	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
STP	TCP/UDP	118	スケジュール転送プロトコル	stp	Cisco IOS XE Release 3.1S
StreetTalk	TCP/UDP	566	Streettalk	streettalk	Cisco IOS XE Release 3.1S
Stun-NAT	TCP/UDP	3478	STUN	stun-nat	Cisco IOS XE Release 3.1S
STX	TCP/UDP	527	Stock IXChange	stx	Cisco IOS XE Release 3.1S
Submission	TCP/UDP	587	Submission	submission	Cisco IOS XE Release 3.1S
	Subntbcst_TFTP	TCP/UDP	247	subntbcst_tftp	subntbcst_tftp
SU-MIT-TG	TCP/UDP	89	SU/MIT Telnet ゲートウェイ	su-mit-tg	Cisco IOS XE Release 3.1S
Sun-DR	TCP/UDP	665	sun-dr	sun-dr	Cisco IOS XE Release 3.1S
Sun-ND	TCP/UDP	77	SUN ND PROTOCOL-Temporary	sun-nd	Cisco IOS XE Release 3.1S
SupDup	TCP/UDP	95	SUPDUP	supdup	Cisco IOS XE Release 3.1S
Surf	TCP/UDP	1010	Surf	surf	Cisco IOS XE Release 3.1S
Sur-Meas	TCP/UDP	243	Survey Measurement	sur-meas	Cisco IOS XE Release 3.1S
Svrloc	TCP/UDP	427	Server Location	svrloc	Cisco IOS XE Release 3.1S
Swift-RVF	TCP/UDP	97	Swift リモート仮想ファイルプロトコル	swift-rvf	Cisco IOS XE Release 3.1S
Swipe	TCP/UDP	53	IP with Encryption	swipe	Cisco IOS XE Release 3.1S
Synoptics-Trap	TCP/UDP	412	Trap Convention Port	synoptics-trap	Cisco IOS XE Release 3.1S
Synotics-Broker	TCP/UDP	392	SynOptics Port Broker Port	synotics-broker	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Synotics-Relay	TCP/UDP	391	SynOptics SNMP Relay Port	synotics-relay	Cisco IOS XE Release 3.1S
Systat	TCP/UDP	11	アクティブ ユーザ数	systat	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S
TACACS	TCP/UDP	49、65	Terminal Access Controller Access Control System	tacacs	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S
TAC News	TCP/UDP	98	TAC News	tacnews	Cisco IOS XE Release 3.1S
Talk	TCP/UDP	517	通話（Talk）	talk	Cisco IOS XE Release 3.1S
		TCF	TCP/UDP	87	TCF
TD-Replica	TCP/UDP	268	Tobit David Replica	td-replica	Cisco IOS XE Release 3.1S
TD-Service	TCP/UDP	267	Tobit David Service Layer	td-service	Cisco IOS XE Release 3.1S
Teedtap	TCP/UDP	559	Teedtap	teedtap	Cisco IOS XE Release 3.1S
Tell	TCP/UDP	754	送信（Send）	tell	Cisco IOS XE Release 3.1S
Telnet	TCP/UDP	23	Telnet	telnet	Cisco IOS XE Release 3.1S
Tempo	TCP/UDP	526	newdate	tempo	Cisco IOS XE Release 3.1S
Tenfold	TCP/UDP	658	Tenfold	tenfold	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Texar	TCP/UDP	333	Texar セキュリティ ポート	texar	Cisco IOS XE Release 3.1S
TICF-1	TCP/UDP	492	Transport Independent Convergence for FNA	ticf-1	Cisco IOS XE Release 3.1S
TICF-2	TCP/UDP	493	Transport Independent Convergence for FNA	ticf-2	Cisco IOS XE Release 3.1S
Timbuktu	TCP/UDP	407	Timbuktu	timbuktu	Cisco IOS XE Release 3.1S
Time	TCP/UDP	37	時刻（Time）	time	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisc IOS XE Release 3.1S
Timed	TCP/UDP	525	Timeserver	timed	Cisco IOS XE Release 3.1S
TINC	TCP/UDP	655	tinc	tinc	Cisco IOS XE Release 3.1S
TLISRV	TCP/UDP	1527	Oracle	tlisrv	Cisco IOS XE Release 3.1S
TLSP	TCP/UDP	72	トランスポート層セキュリティ プロトコル	tlsp	Cisco IOS XE Release 3.1S
TNETOS	TCP/UDP	377	日本電気株式会社	tnETOS	Cisco IOS XE Release 3.1S
TNS-CML	TCP/UDP	590	tns-cml	tns-cml	Cisco IOS XE Release 3.1S
TN-TL-FD1	TCP/UDP	476	tn-tl-fd1	tn-tl-fd1	Cisco IOS XE Release 3.1S
TP++	TCP/UDP	39	TP++ トランスポート プロトコル	tp++	Cisco IOS XE Release 3.1S
TPIP	TCP/UDP	594	tpip	tpip	Cisco IOS XE Release 3.1S
Trunk-1	TCP/UDP	23	Trunk-1	trunk-1	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Trunk-2	TCP/UDP	24	Trunk-2	trunk-2	Cisco IOS XE Release 3.1S
TServer	TCP/UDP	450	コンピュータ支援電気通信アプリケーション	tserver	Cisco IOS XE Release 3.1S
TTP	TCP/UDP	84	TTP	ttp	Cisco IOS XE Release 3.1S
UAAC	TCP/UDP	145	UAAC プロトコル	uaac	Cisco IOS XE Release 3.1S
UARPs	TCP/UDP	219	Unisys ARPs	uarps	Cisco IOS XE Release 3.1S
UDPLite	TCP/UDP	136	UDPLite	udplite	Cisco IOS XE Release 3.1S
UIS	TCP/UDP	390	uis	uis	Cisco IOS XE Release 3.1S
uLISTProc	TCP/UDP	372	List Processor	ulistproc	Cisco IOS XE Release 3.1S
ULP	TCP/UDP	522	ulp	ulp	Cisco IOS XE Release 3.1S
ULPNet	TCP/UDP	483	ulpnet	ulpnet	Cisco IOS XE Release 3.1S
Unidata-LDM	TCP/UDP	388	Unidata LDM	unidata-ldm	Cisco IOS XE Release 3.1S
Unify	TCP/UDP	181	Unify	unify	Cisco IOS XE Release 3.1S
UPS	TCP/UDP	401	無停電電源	ups	Cisco IOS XE Release 3.1S
	URM	TCP/UDP	606	Cray Unified Resource Manager	urm
	UTI	TCP/UDP	120	UTI	uti
Utime	TCP/UDP	519	Unixtime	utime	Cisco IOS XE Release 3.1S
UTMPCD	TCP/UDP	431	utmpcd	utmpcd	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
UTMPSD	TCP/UDP	430	utmpsd	utmpsd	Cisco IOS XE Release 3.1S
UUCP	TCP/UDP	540	uucpd	uucp	Cisco IOS XE Release 3.1S
UUCP-Path	TCP/UDP	117	UUCP Path Service	uucp-path	Cisco IOS XE Release 3.1S
UUCP-rLogin	TCP/UDP	541	uucp-rlogin	uucp-rlogin	Cisco IOS XE Release 3.1S
UUIDGEN	TCP/UDP	697	UUIDGEN	uuidgen	Cisco IOS XE Release 3.1S
VACDSM-App	TCP/UDP	671	VACDSM-APP	vacdsm-app	Cisco IOS XE Release 3.1S
VACDSM-SWS	TCP/UDP	670	VACDSM-SWS	vacdsm-sws	Cisco IOS XE Release 3.1S
VATP	TCP/UDP	690	Velazquez アプリケーション転送プロトコル	vatp	Cisco IOS XE Release 3.1S
VEMMI	TCP/UDP	575	vemmi	vemmi	Cisco IOS XE Release 3.1S
VID	TCP/UDP	769	vid	vid	Cisco IOS XE Release 3.1S
Videotex	TCP/UDP	516	videotex	videotex	Cisco IOS XE Release 3.1S
VISA	TCP/UDP	70	VISA プロトコル	visa	Cisco IOS XE Release 3.1S
VNC	TCP/UDP	5800、5900、5901	Virtual Network Computing	vnc	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
VMNet	TCP/UDP	175	vmnet	vmnet	Cisco IOS XE Release 3.1S
VMPWSCS	TCP/UDP	214	vmpwscs	vmpwscs	Cisco IOS XE Release 3.1S
VMTP	TCP/UDP	81	VMTP	vmtp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	VNAS	TCP/UDP	577	vnas	vnas
VPP	TCP/UDP	677	仮想実在プロトコル	vpp	Cisco IOS XE Release 3.1S
VPPS-QUA	TCP/UDP	672	vpps-qua	vpps-qua	Cisco IOS XE Release 3.1S
VPPS-VIA	TCP/UDP	676	vpps-via	vpps-via	Cisco IOS XE Release 3.1S
VRRP	TCP/UDP	112	Virtual Router Redundancy Protocol; 仮想ルータ冗長プロトコル	vrrp	Cisco IOS XE Release 3.1S
VSINet	TCP/UDP	996	vsinet	vsinet	Cisco IOS XE Release 3.1S
VSLMP	TCP/UDP	312	vslmp	vslmp	Cisco IOS XE Release 3.1S
WAP-Push	TCP/UDP	2948	WAP PUSH	wap-push	Cisco IOS XE Release 3.1S
WAP-Push-HTTP	TCP/UDP	4035	WAP Push OTA-HTTP port	wap-push-http	Cisco IOS XE Release 3.1S
WAP-Push-HTTPS	TCP/UDP	4036	WAP Push OTA-HTTP secure	wap-push-https	Cisco IOS XE Release 3.1S
WAP-Pushsecure	TCP/UDP	2949	WAP PUSH SECURE	wap-pushsecure	Cisco IOS XE Release 3.1S
WAP-VACL-S	TCP/UDP	9207	WAP vCal Secure	wap-vcal-s	Cisco IOS XE Release 3.1S
WAP-VCAL	TCP/UDP	9205	WAP vCal	wap-vcal	Cisco IOS XE Release 3.1S
WAP-VCARD	TCP/UDP	9204	WAP vCard	wap-vcard	Cisco IOS XE Release 3.1S
WAP-VCARD-S	TCP/UDP	9206	WAP vCard Secure	wap-vcard-s	Cisco IOS XE Release 3.1S
WAP-WSP	TCP/UDP	9200	WAP コネクションレス型セッション サービス	wap-wsp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
WAP-WSP-S	TCP/UDP	9202	WAP セキュア コネクションレス型セッションサービス	wap-wsp-s	Cisco IOS XE Release 3.1S
WAP-WSP-WTP	TCP/UDP	9201	WAP セッション サービス	wap-wsp-wtp	Cisco IOS XE Release 3.1S
WAP-WSP-WTP-S	TCP/UDP	9203	WAP セキュア セッション サービス	wap-wsp-wtp-s	Cisco IOS XE Release 3.1S
	WB-Expak	TCP/UDP	79	WIDEBAND EXPAK	wb-expak
WB-Mon	TCP/UDP	78	WIDEBAND モニタリング	wb-mon	Cisco IOS XE Release 3.1S
Webster	TCP/UDP	765	Webster	webster	Cisco IOS XE Release 3.1S
Webex Meeting	TCP	ヒューリスティック	Webex Meeting	webex-meeting	Cisco IOS XE リリース 3.4S
WhoAmI	TCP/UDP	565	whoami	whoami	Cisco IOS XE Release 3.1S
Whois++	TCP/UDP	63	whois++ サービス	whois++	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S
Windows Update	TCP	80、443、ヒューリスティック	Windows Update	windows-update	Cisco IOS XE リリース 3.4S
WorldFusion	TCP/UDP	2595	World Fusion	worldfusion	Cisco IOS XE Release 3.1S
WPGS	TCP/UDP	780	wpgs	wpgs	Cisco IOS XE Release 3.1S
WSN	TCP/UDP	74	Wang Span Network	wsn	Cisco IOS XE Release 3.1S
XAct-Backup	TCP/UDP	911	Xact-backup	xact-backup	Cisco IOS XE Release 3.1S
X-Bone-CTL	TCP/UDP	265	Xbone CTL	x-bone-ctl	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
XDMCP	TCP/UDP	177	X Display Manager Control Protocol	xdmcp	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S
XDTP	TCP/UDP	3088	拡張可能データ転送プロトコル	xdtp	Cisco IOS XE Release 3.1S
XFER	TCP/UDP	82	XFER ユーティリティ	xfer	Cisco IOS XE Release 3.1S
XNET	TCP/UDP	15	Cross Net Debugger	xnet	Cisco IOS XE Release 3.1S
XNS-Auth	TCP/UDP	72	XNS 認証	xns-auth	Cisco IOS XE Release 3.1S
XNS-CH	TCP/UDP	54	XNS Clearinghouse	xns-ch	Cisco IOS XE Release 3.1S
	XNS-Courier	TCP/UDP	165	Xerox	xns-courier
XNS-IDP	TCP/UDP	22	XEROX NS IDP	xns-idp	Cisco IOS XE Release 3.1S
XNS-Mail	TCP/UDP	58	XNS メール	xns-mail	Cisco IOS XE Release 3.1S
XNS-Time	TCP/UDP	52	XNS 時間プロトコル	xns-time	Cisco IOS XE Release 3.1S
XTP	TCP/UDP	36	XTP	xtp	Cisco IOS XE Release 3.1S
XVTTP	TCP/UDP	508	xvttp	xvttp	Cisco IOS XE Release 3.1S
XYPlex-Mux	TCP/UDP	173	Xyplex	xyplex-mux	Cisco IOS XE Release 3.1S
X Windows	TCP	6000 ～ 6003	X Window システム	xwindows	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
z39.50	TCP/UDP	210	ANSI Z39.50	z39.50	Cisco IOS XE Release 3.1S
Zannet	TCP/UDP	317	Zannet	zannet	Cisco IOS XE Release 3.1S
ZServ	TCP/UDP	346	Zebra サーバ	zserv	Cisco IOS XE Release 3.1S
AN	IP	107	Active Networks	an	Cisco IOS XE Release 3.1S
AOL-Protocol[16]		TCP	5190	America OnLine プロトコル	aol-protocol
ARGUS		IP	13	ARGUS	argus
ARIS		IP	104	ARIS	aris
AX25		IP	93	AX.25 フレーム	ax25
BBNR RCC Mon		IP	10	BBN RCC モニタリング	bbnrccmon
BLIZWOW		TCP、UDP	3724	World of Warcraft ゲーム プロトコル	blizwow
BNA		IP	49	BNA	bna
	BR-SAT-Mon	IP	76	Backroom SATNET モニタリング	br-sat-mon
	CBT	IP	7	CBT	cbt
CFTP	IP	62	CFTP	cftp	Cisco IOS XE Release 3.1S
Choas	IP	16	Chaos	chaos	Cisco IOS XE Release 3.1S
Compaq-Peer	IP	110	Compaq Peer Protocol	compaq-peer	Cisco IOS XE Release 3.1S
CPHB	IP	73	Computer Protocol Heart Beat	cphb	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
CPNX	IP	72	Computer Protocol Network Executive	cpnx	Cisco IOS XE Release 3.1S
CRTP	IP	126	Combat Radio Transport Protocol	crtp	Cisco IOS XE Release 3.1S
CRUDP	IP	127	Combat Radio User Datagram	crudp	Cisco IOS XE Release 3.1S
DCCP	IP	33	データグラム輻輳制御プロトコル	dccp	Cisco IOS XE Release 3.1S
DCN-Meas	IP	19	DCN 測定サブシステム	dcn-meas	Cisco IOS XE Release 3.1S
DDP	IP	37	データグラム送達プロトコル	ddp	Cisco IOS XE Release 3.1S
DDX	IP	116	D-II データ交換	ddx	Cisco IOS XE Release 3.1S
DGP	IP	86	異種ゲートウェイプロトコル	dgp	Cisco IOS XE Release 3.1S
DSR	IP	48	動的ソースルーティングプロトコル	dsr	Cisco IOS XE Release 3.1S
EGP	IP	8	エクステリアゲートウェイプロトコル	egp	Cisco IOS XE Release 3.1S
EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp	Cisco IOS XE Release 3.1S
EMCON	IP	18	EMCON	emcon	Cisco IOS XE Release 3.1S
Encap	IP	98	カプセル化ヘッダー	encap	15.1(3)T
EtherIP	IP	97	Ethernet-within-IP カプセル化	etherip	Cisco IOS XE Release 3.1S
	FC	IP	133	ファイバチャネル（Fibre Channel）	fc
FIRE	IP	125	FIRE	fire	Cisco IOS XE Release 3.1S
GGP	IP	3	ゲートウェイ間	ggp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
GMTP	IP	100	GMTP	gmtp	Cisco IOS XE Release 3.1S
GRE	IP	47	総称ルーティング カプセル化	gre	Cisco IOS XE Release 3.1S
HIP	IP	139	ホスト識別プロトコル	hip	Cisco IOS XE Release 3.1S
HMP	IP	20	ホスト モニタリング	hmp	Cisco IOS XE Release 3.1S
HopOpt	IP	0	IPv6 ホップバイホップ オプション	hopopt	Cisco IOS XE Release 3.1S
ICQ	TCP	80、ヒューリスティック	I seek you インスタント メッセージ プロトコル	icq	Cisco IOS XE リリース 3.3S
IATP	IP	117	インタラクティブ エージェント転送プロトコル	iatp	Cisco IOS XE Release 3.1S
ICMP	IP	1	インターネット制御メッセージ	icmp	Cisco IOS XE Release 3.1S
IDPR	IP	35	ドメイン間ポリシー ルーティング プロトコル	idpr	Cisco IOS XE Release 3.1S
IDPR-CMTP	IP	38	IDPR 制御メッセージ トランスポート プロトコル	idpr-cmtp	Cisco IOS XE Release 3.1S
IDRP	IP	45	ドメイン間ルーティング プロトコル	idrp	Cisco IOS XE Release 3.1S
IFMP	IP	101	Ipsilon フロー管理プロトコル	ifmp	Cisco IOS XE Release 3.1S
IGRP	IP	9	シスコ内部ゲートウェイ	igrp	Cisco IOS XE Release 3.1S
IL	IP	40	IL トランスポート プロトコル	il	Cisco IOS XE Release 3.1S
I-NLSP	IP	52	Integrated Net Layer Security TUBA	i-nlsp	Cisco IOS XE Release 3.1S
IMPCOMP	IP	108	IP ペイロード圧縮プロトコル	ipcomp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
	IPCU	IP	71	インターネット パケット コア ユーティリティ	ipcv
IPinIP	IP	4	IP in IP	ipinip	Cisco IOS XE Release 3.1S
IPIP	IP	94	IP-within-IP カプセル化プロトコル	ipip	Cisco IOS XE Release 3.1S
IPLT	IP	129	IPLT	iplt	Cisco IOS XE Release 3.1S
IPPC	IP	67	Internet Pluribus Packet Core	ippc	Cisco IOS XE Release 3.1S
IPv6-Frag	IP	44	Fragment Header for IPv6	ipv6-frag	Cisco IOS XE Release 3.1S
IPv6-ICMP	IP	58	IPv6 の ICMP	ipv6-icmp	Cisco IOS XE Release 3.1S
IPv6INIP	IP	41	Ipv6 encapsulated	ipv6inip	Cisco IOS XE Release 3.1S
IPv6-NONXT	IP	59	No Next Header for IPv6	ipv6-nonxt	Cisco IOS XE Release 3.1S
IPv6-Opts	IP	60	Destination Options for IPv6	ipv6-opts	Cisco IOS XE Release 3.1S
IPv6-Route	IP	43	Routing Header for IPv6	ipv6-route	Cisco IOS XE Release 3.1S
IRTP	IP	36	インターネット高信頼性トランザクション	irtp	Cisco IOS XE Release 3.1S
ISIS	IP	124	ISIS over IPv4	isis	Cisco IOS XE Release 3.1S
ISO-TP4	IP	29	ISO トランスポート プロトコル クラス 4	iso-tp4	Cisco IOS XE Release 3.1S
IXP-in-IP	IP	111	IPX in IP	ixp-in-ip	Cisco IOS XE Release 3.1S
LARP	IP	91	Locus アドレス解決プロトコル	larp	Cisco IOS XE Release 3.1S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Leaf-1	IP	25	Leaf-1	leaf-1	Cisco IOS XE Release 3.1S
6to4 IPv6 Tunneled	L3 Protocol	--	6to4 IPv6 Tunneled	6to4 IPv6 Tunneled	Cisco IOS XE Release 3.2S
	AYIYA IPv6 Tunneled	UDP	5072	AYIYA トラフィックに基づく IPv6 Tunneled	AYIYA IPv6 Tunneled
	BabelGum	TCP、UDP	80 + ヒューリスティック	BabelGum	BabelGum
Baidu ムービー	TCP、UDP	80 + ヒューリスティック	Baidu ムービー	Baidu ムービー	Cisco IOS XE Release 3.2S
DHCP	UDP	67、68	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	Cisco IOS XE Release 3.2S
DHT	UDP	ヒューリスティック	Distributed sloppy ハッシュテーブル プロトコル	DHT	Cisco IOS XE Release 3.2S
Filetopia	TCP	ヒューリスティック	Filetopia P2P ファイル共有	filetopia	Cisco IOS XE Release 3.2S
Fring-VoIP	UDP	ヒューリスティック	Fring VoIP	fring-voip	Cisco IOS XE リリース 3.3S
GoogleEarth	TCP	80 + ヒューリスティック	GoogleEarth	GoogleEarth	Cisco IOS XE Release 3.2S
Guruguru	TCP	ヒューリスティック	Guruguru	guruguru	Cisco IOS XE Release 3.2S
IMAP	TCP	143,220	Internet Mail Access Protocol	imap	Cisco IOS XE Release 3.2S
IRC	TCP	80 + ヒューリスティック	IRC	IRC	Cisco IOS XE Release 3.2S
ISATAP IPv6 Tunneled	L3 Protocol		Intra-Site Automatic Tunnel Addressing Protocol（ISATAP）IPv6 トンネル	ISATAP IPv6 Tunneled	Cisco IOS XE Release 3.2S
iTunes	TCP	80 + ヒューリスティック	iTunes	iTunes	Cisco IOS XE Release 3.2S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Kuro	TCP	ヒューリスティック	Kuro	kuro	Cisco IOS XE リリース 3.3S
Manolito	TCP、UDP	TCP - ヒューリスティックポート、UDP - 41170	Manolito P2P 音楽共有プロトコル	manolito	Cisco IOS XE Release 3.2S
MapleStory	TCP	ヒューリスティック	メイプルストーリーゲームプロトコル	MapleStory	Cisco IOS XE Release 3.2S
SIP	TCP、UDP	TCP/UDP - 5060 + ヒューリスティック	Session Initiation Protocol	sip	Cisco IOS XE Release 3.2S
	MGCP	TCP、UDP	UDP 2427/2727 - TCP 2427/2428/2727 + ヒューリスティック	Media Gateway Control Protocol	MGCP
Microsoft-DS	TCP、UDP	445	Microsoft-ds	microsoftds	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S
MSN Messenger	TCP	1080、1863、80、ヒューリスティック	MSN Messenger	msn-messenger	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S
MyJabber File Transfer	TCP	ヒューリスティック	MyJabber File Transfer	MyJabber File Transfer	Cisco IOS XE Release 3.2S
Napster	TCP	80 + ヒューリスティック	Napster	napster	Cisco IOS XE Release 3.2S
Netshow	TCP	1755 + ヒューリスティック	Netshow	netshow	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1
NNTP	TCP	TCP - 119 + ヒューリスティック、UDP -119	Network News Transfer Protocol	NNTP	Cisco IOS XE Release 3.2S
NTP	UDP	123	ネットワークタイムプロトコル	NTP	Cisco IOS XE Release 3.2S
Pando	TCP、UDP	TCP - 80 + ヒューリスティック、UDP - ヒューリスティック	Pando	Pando	Cisco IOS XE Release 3.2S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
POCO	TCP、UDP	ヒューリスティック	POCO ファイル共有アプリケーション	POCO	Cisco IOS XE Release 3.2S
POP3	TCP	110、ヒューリスティック	POP3	POP3	Cisco IOS XE Release 3.2S
PPTP	TCP	1723	ポイントツーポイントトンネリング プロトコル	pptp	Cisco IOS XE Release 3.2S
RADIUS	UDP	1812、1813	Remote Authentication Dial In User Service プロトコル	radius	Cisco IOS XE リリース 3.3S
	SCCP/Skinny	TCP	2000 ～ 2002	Skinny Call Control Protocol	skinny
	Soribada	TCP	TCP - 80 + ヒューリスティック、UDP - ヒューリスティック	Soribada、韓国の P2P 音楽共有プロトコル	soribada
	Soulseek	TCP	ヒューリスティック	SoulSeek インターネット ダウンロード マネージャ プロトコル	soulseek
	TeamSpeak	UDP	ヒューリスティック	TeamSpeak インターネットベース音声会議プロトコル	TeamSpeak
TelePresence	TCP/UDP	動的に割り当て	Cisco TelePresence System	telepresence-media	12.2(18)ZYA2
Telepresence-control	TCP、UDP	TCP-5060、UDP-ヒューリスティック	Telepresence-control	telepresence-control	Cisco IOS XE Release 3.2S
Teredo IPv6 Tunneled	TCP、UDP	TCP-ヒューリスティック、UDP - 3544 + ヒューリスティック	Teredo IPv6 Tunneled	teredo-ipv6-tunneled	Cisco IOS XE Release 3.2S
TFTP	UDP	69	トリビアルファイル転送プロトコル	tftp	Cisco IOS XE Release 3.2S
TomatoPang	TCP	ヒューリスティック	TomatoPang P2P 共有プロトコル	TomatoPang	Cisco IOS XE Release 3.2S
Tunnel-HTTP	TCP	80 + ヒューリスティック	HTTP トンネリング	tunnel-http	Cisco IOS XE Release 3.2S

カテゴリ	プロトコル	タイプ	WKP/IP プロトコル	説明	構文
Ventrilo	TCP、UDP	ヒューリスティック	Ventrilo VoIP プロトコル	Ventrilo	Cisco IOS XE Release 3.2S
Waste	TCP/UDP	ヒューリスティック	Waste	waste	Cisco IOS XE リリース 3.3S
WebThunder	TCP、UDP	TCP-80、UDP-ヒューリスティック	WebThunder ピアツーピアファイル共有	WebThunder	Cisco IOS XE Release 3.2S
Yahoo-Messenger	TCP	TCP-5050/5101/1080/119/80/ヒューリスティック	Yahoo Messenger	yahoo-messenger	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S
Yahoo-Messenger-VoIP	TCP/UDP	ヒューリスティック	Yahoo Messenger VoIP	yahoo-voip-messenger	Cisco IOS XE リリース 3.3S
Yahoo VoIP over SIP	TCP/UDP	5060/ヒューリスティック	Yahoo VoIP over SIP	yahoo-voip-over-sip	Cisco IOS XE リリース 3.4S

[9] Release 12.2(18)ZYA および Cisco IOS XE Release 2.5 Cisco では、Exchange 03 および 07 のみをサポートしています。MS クライアント アクセスは認識されますが、Web クライアント アクセスは認識されません。

[10] Release 12.3(4)T では、HTTP トラフィック用の NBAR Extended Inspection 機能が導入されました。この機能を使用すると、NBAR は不明な TCP ポートをスキャンし、そのルータを通過する HTTP トラフィックを識別できます。Cisco IOS XE Release 2.1 では、URL またはホスト名による HTTP トラフィックの分類はサポートされていません。Cisco IOS XE Release 2.5 は、URL またはホスト名による HTTP トラフィックの分類をサポートしています。

[11] Cisco IOS Release 12.4(4)T で Skype が導入されました。この導入により、Skype が Cisco IOS ソフトウェアに含まれるようになり、Cisco IOS リリース 12.4(4)T の新機能である NBAR インフラストラクチャを使用するようになりました。シスコ ソフトウェアは Skype 1.0、2.5、および 3.0 をサポートしています。Cisco IOS XE Release 2.1 では、Skype は TCP タイプでのみサポートされています。一部のハードウェア プラットフォームは Skype をサポートしていません。たとえば、Supervisor/PISA エンジンが搭載されている Catalyst 6500 シリーズ スイッチでは Skype はサポートされません。Cisco IOS XE Release 2.5 は、TCP および UDP タイプで Skype をサポートしています。

[12] Release 12.2(18)ZYA では、HTTP 経由の YouTube へのアクセスのみが認識されます。

[13] BitTorrent は、暗号化されていないトラフィックのみを分類します。

[14] eDonkey は、暗号化されていないトラフィックのみを分類します。

[15] Release 12.2(18)ZYA では、SIP および Skinny 電話接続（cisco-phone トラフィック接続）のみが認識されます。H.323 電話接続は認識されません。

[16] AOL-Protocol は、ICQ クライアントと AOL クライアントの間で共有されるトラフィックを分類します。

関連コマンド

Command	Description
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。

Command	Description
ipnbarcustom	NBAR Protocol Discovery 機能を拡張し、追加の静的ポート アプリケーションを分類および監視できます。または、NBAR はサポートしていない静的ポート トラフィックを分類できるようになります。
matchprotocol (NBAR)	Network-Based Application Recognition（NBAR）が認識するプロトコル タイプによりトラフィックを照合するように NBAR を設定します。

match protocol citrix

Citrix トラフィックを照合するように Network-Based Application Recognition（NBAR）を設定するには、クラスマップ コンフィギュレーション モードで **matchprotocolcitrix** コマンドを使用します。NBAR による Citrix トラフィックの照合を無効にするには、このコマンドの **no** 形式を使用します。

match protocol citrix [**app** *application-name-string*] [**ica-tag** *ica-tag-value*]
no match protocol citrix [**app** *application-name-string*] [**ica-tag** *ica-tag-value*]

構文の説明

app	（任意）アプリケーション名文字列の照合を指定します。
application-name-string	（任意）サブプロトコル パラメータとして使用する文字列を指定します。
ica-tag	（任意）Independent Computing Architecture（ICA）パケットのタギングを指定します。
ica-tag-value	（任意）ICA パケットのプライオリティ タグを指定します。プライオリティ タグの値の範囲は 0 ～ 3 です。

コマンド デフォルト

一致基準が指定されていません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(2)E	このコマンドが導入されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.1(13)E	このコマンドが、FlexWAN モジュールを備えていない Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
12.4(2)T	このコマンドが、ica-tag キーワードと *ica-tag-value* 引数を含むように変更されました。
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。

使用上のガイドライン

app キーワードを使用せずに **matchprotocolcitrix** コマンドを入力すると、すべての Citrix トラフィックが成功する一致基準として確立されます。

ica-tag キーワードを使用して **matchprotocolcitrix** コマンドを入力すると、Citrix ICA トラフィックが優先順位付けされます。プライオリティ タグの値は 0～ 3 の数字で、0 が最も優先順位が高く、3 が最も優先順位が低くなります。

例

次に、すべてのCitrixトラフィックを照合するようにNBARを設定する例を示します。

```
match protocol citrix
```

次に、アプリケーション名が packet1 の Citrix トラフィックを照合するように NBAR を設定する例を示します。

```
match protocol citrix app packet1
```

次に、Citrix ICA トラフィックに優先順位 1 を与えるように NBAR を設定する例を示します。

```
match protocol citrix ica-tag-1
```

match protocol fasttrack

FastTrack ピアツーピア トラフィックを照合するように Network-Based Application Recognition（NBAR）を設定するには、クラスマップ コンフィギュレーション モードで **matchprotocolfasttrack** コマンドを使用します。NBAR による FastTrack トラフィックの照合を無効にするには、このコマンドの **no** 形式を使用します。

match protocol fasttrack file-transfer *"regular-expression"*
no match protocol fasttrack file-transfer *"regular-expression"*

構文の説明

file-transfer	特定の FastTrack トラフィックを識別するために、正規表現が使用されることを示します。
" *regular-expression* **"**	特定の FastTrack トラフィックを識別するために使用される正規表現です。たとえば、正規表現として「cisco」と入力すると、文字列「cisco」を含むFastTrackトラフィックが、トラフィック ポリシーに一致すると分類されます。 トラフィック クラスですべてのFastTrackトラフィックを識別するには、正規表現として 「*」を使用します。

コマンド デフォルト

NBAR は、FastTrack ピアツーピア トラフィックを照合するように設定されていません

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(12c)E	このコマンドが導入されました。
12.1(13)E	このコマンドが、FlexWAN モジュールのない Catalyst 6000 ファミリ スイッチで使用できるようになりました。
12.2(2)T	このコマンドが Cisco IOS Release 12.2(2)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
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。

使用上のガイドライン

トラフィック クラスですべてのFastTrackトラフィックを識別するには、正規表現として 「*」を使用します。

FastTrackを使用するアプリケーションには、KaZaA、Grokster、およびMorpheusが含まれます（ただし、Morpheus の新しいバージョンは Gnutella を使用します）。

例

次に、すべての FastTrack トラフィックを照合するように NBAR を設定する例を示します。

```
match protocol fasttrack file-transfer "*"
```

次に、拡張子が「.mpeg」の FastTrack ファイルすべてをクラス マップ nbar に分類する例を示します。

```
class-map match-all nbar
 match protocol fasttrack file-transfer "*.mpeg"
```

次に、文字列「cisco」を含む FastTrack トラフィックを照合するように NBAR を設定する例を示します。

```
match protocol fasttrack file-transfer "*cisco*"
```

match protocol gnutella

Gnutella ピアツーピア トラフィックを照合するように Network-Based Application Recognition（NBAR）を設定するには、クラスマップ コンフィギュレーション モードで **matchprotocolgnutella** コマンドを使用します。NBAR による Gnutella トラフィックの照合を無効にするには、このコマンドの **no** 形式を使用します。

match protocol gnutella file-transfer *"regular-expression"*
no match protocol gnutella file-transfer *"regular-expression"*

構文の説明

file-transfer	特定の Gnutella トラフィックを識別するために、正規表現が使用されることを示します。
" *regular-expression* **"**	特定の Gnutella トラフィックを識別するために使用される正規表現です。たとえば、正規表現として「cisco」と入力すると、文字列「cisco」を含む Gnutella トラフィックが、トラフィック ポリシーに一致すると分類されます。 トラフィック クラスですべての Gnutella トラフィックを識別するには、正規表現として「*」を使用します。

コマンド デフォルト

動作または値は定義されていません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(12c)E	このコマンドが導入されました。
12.1(13)E	このコマンドが、FlexWAN モジュールのない Catalyst 6000 ファミリ スイッチで使用できるようになりました。
12.2(2)T	このコマンドが Cisco IOS Release 12.2(2)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
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。

使用上のガイドライン

トラフィック クラスですべての Gnutella トラフィックを識別するには、正規表現として「*」を使用します。

Gnutella を使用するアプリケーションは、次のとおりです。

- BearShare

- Gnewtellium
- Gnucleus
- Gtk-Gnutella
- JTella
- LimeWire
- Morpheus
- Mutella
- Phex
- Qtella
- Swapper
- XoloX
- XCache

例

次に、すべての Gnutella トラフィックを照合するように NBAR を設定する例を示します。

```
match protocol gnutella file-transfer “*”
```

次に、拡張子が「.mpeg」の Gnutella ファイルすべてをクラス マップ nbar に分類する例を示します。

```
class-map match-all nbar
 match protocol gnutella file-transfer "*.mpeg"
```

次に、文字「cisco」を含む Gnutella トラフィックのみを分類する例を示します。

```
class-map match-all nbar
 match protocol gnutella file-transfer “*cisco*”
```

match protocol http

URL、ホスト、Multipurpose Internet Mail Extension（MIME）タイプ、または HTTP パケット ヘッダーのフィールドにより、HTTP トラフィックを照合するように Network-Based Application Recognition（NBAR）を設定するには、クラスマップ コンフィギュレーション モードで **matchprotocolhttp** コマンドを使用します。NBAR による、URL、ホスト、MIME タイプ、または HTTP パケット ヘッダーのフィールドによる HTTP トラフィックの照合を無効にするには、このコマンドの **no** 形式を使用します。

match protocol http [{**url** *url-string*|**host** *hostname-string*|**mime** *MIME-type*|**c-header-field** *c-header-field-string*|**s-header-field** *s-header-field-string*}]
no match protocol http [{**url** *url-string*|**host** *hostname-string*|**mime** *MIME-type*|**c-header-field** *c-header-field-string*|**s-header-field** *s-header-field-string*}]
match protocol http [{**content-encoding** *content-encoding-name-string*|**from** *from-address-string*|**host** *hostname-string*|**location** *location-name-string*|**mime** *MIME-type*|**referer** *referer-address-string*|**server** *server-software-name-string*|**url** *url-string*|**user-agent** *user-agent-software-name-string*}]
no match protocol http [{**content-encoding** *content-encoding-name-string*|**from** *from-address-string*|**host** *hostname-string*|**location** *location-name-string*|**mime** *MIME-type*|**referer** *referer-address-string*|**server** *server-software-name-string*|**url** *url-string*|**user-agent** *user-agent-software-name-string*}]

構文の説明

url	（任意）URL による照合を指定します。
url-string	（任意）照合する HTTP トラフィックのユーザ指定の URL です。
host	（任意）ホスト名による照合を指定します。
hostname-string	（任意）照合するユーザ指定のホスト名です。
mime	（任意）MIME テキスト文字列による照合を指定します。
MIME-type	（任意）照合するユーザ指定の MIME テキスト文字列です。
c-header-field	（任意）HTTP クライアント メッセージのヘッダー フィールドの文字列による照合を指定します。 （注） HTTP クライアント メッセージは、HTTP 要求メッセージと呼ばれることもよくあります。
c-header-field-string	（任意）照合する HTTP クライアント メッセージ（HTTP 要求メッセージ）内のユーザ指定のテキスト文字列です。
s-header-field	（任意）HTTP サーバ メッセージのヘッダー フィールドの文字列による照合を指定します。 （注） HTTP サーバ メッセージは、HTTP 応答メッセージと呼ばれることもよくあります。

s-header-field-string	（任意）照合する HTTP サーバ メッセージ（HTTP 応答メッセージ）内のユーザ指定のテキストです。
Cisco IOS 15.1(2)T 以降のリリースおよび Supervisor 32/PISA エンジンが搭載されている Catalyst 6500 シリーズ スイッチ	
content-encoding	（任意）エンティティ ボディをパッケージ化するために使用されたエンコーディング メカニズムによる照合を指定します。
content-encoding-name-string	（任意）ユーザ指定の Content-Encoding 名です。
from	（任意）ユーザ エージェントの制御者の電子メール アドレスによる照合を指定します。
from-address-string	（任意）ユーザ指定の電子メール アドレスです。
location	（任意）要求のリソースの正確な場所による照合を指定します。
location-name-string	（任意）ユーザ指定のリソースの場所です。
referer	（任意）リソース要求の取得元のアドレスによる照合を指定します。
referer-address-name-string	（任意）ユーザ指定の参照元リソースのアドレスです。
server	（任意）要求を処理する元のサーバによって使用されるソフトウェアによる照合を指定します。
server-software-name-string	（任意）ユーザ指定のソフトウェア名です。
user-agent	（任意）要求を送信するエージェントによって使用されるソフトウェアによる照合を指定します。
user-agent-software-name-string	（任意）要求を送信するエージェントによって使用されるソフトウェアのユーザ指定の名前です。

コマンド デフォルト

NBAR は、URL、ホスト、MIME タイプ、または HTTP パケット ヘッダーのフィールドにより、HTTP トラフィックを照合しません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。

リリース	変更箇所
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(2)E	このコマンドが、*hostname-string* 引数を含むように変更されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.1(13)E	このコマンドが、FlexWAN モジュールのない Catalyst 6000 ファミリ スイッチで使用できるようになりました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合され、HTTP トラフィック用の NBAR Extended Inspection 機能が導入されました。この機能を使用すると、NBAR は不明な TCP ポートをスキャンし、そのポートを通過する HTTP トラフィックを識別できます。
12.4(2)T	このコマンドが Cisco IOS Release 12.4(2)T に統合され、**c-header-field***c-header-field-string* キーワードおよび引数と、**s-header-field***s-header-field-string* キーワードおよび引数を含むように変更されました。
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。
12.2(18)ZY2	このコマンドが Cisco IOS Release 12.2(18)ZY2 に統合され、Supervisor 32/PISA エンジンを搭載した Catalyst 6500 シリーズ スイッチのサポートが提供されました。 （注） この Cisco IOS リリースおよびプラットフォームでは、**c-header-field***c-header-field-string* キーワードおよび引数と、**s-header-field***s-header-field-string* キーワードおよび引数は使用できません。同じ機能を実現するには、Catalyst 6500 シリーズ スイッチ用の構文に示されているように、個別のキーワードおよび引数を使用します。
15.1(2)T	このコマンドが変更されました。**c-header-field***c-header-field-string* キーワードおよび引数と、**s-header-field***s-header-field-string* キーワードおよび引数が、サポートされなくなりました。**content-encoding**、**from**、**location**、**referrer**、および **user-agent** キーワードとそれぞれの引数が追加されました。
Cisco IOS XE Release 3.1S	このコマンドが、Cisco IOS XE リリース 3.1S に統合されました。

使用上のガイドライン ホスト、URL、または MIME による HTTP トラフィックの分類

Cisco IOS Release 12.3(4)T では、HTTP トラフィック用の NBAR Extended Inspection 機能が導入されました。この機能を使用すると、NBAR は不明な TCP ポートをスキャンし、そのポートを通過する HTTP トラフィックを識別できます。この機能は、**matchprotocolhttp** コマンドを含むサービス ポリシーがインターフェイスにアタッチされたときに、自動的に有効になります。

MIME タイプで照合する場合、MIME タイプにはユーザ指定のテキスト文字列を含めることができます。IANA に登録されている MIME タイプについては、次の Web ページを参照してください。

http://www.iana.org/assignments/media-types/

MIME タイプでマッチングすると、次の HTTP トランザクションまで、NBAR は MIME タイプとすべての後続パケットを含むパケットのマッチングを実行します。

ホストにより照合する場合、NBAR は HTTP パケット内のホスト フィールド コンテンツで正規表現一致を実行し、そのホストからのすべてのパケットを分類します。

HTTP クライアント要求の照合は、GET、PUT、HEAD、POST、DELETE、OPTIONS、CONNECT、および TRACE をサポートしています。URL により照合する場合、NBAR は URL を含む HTTP パケットを認識し、HTTP 要求の一部であるすべてのパケットを照合します。分類する URL を指定する場合は、**match** ステートメントに www.*hostname .domain* に続く URL の部分のみを含めます。たとえば、www.cisco.com/latest/whatsnew.html という URL の場合、**match** ステートメントに /latest/whatsnew.html のみを含めます（例：**matchprotocolhttpurl/latest/whatsnew.html**）。

（注） Supervisor 32/PISA が搭載された Cisco Catalyst 6500 シリーズ スイッチ上の Cisco IOS Release 12.2(18)ZY2（以降のリリース）では、**matchprotocolhttp** コマンドで、ルータ別プロトコル別に最大 56 個のパラメータまたは下位分類を指定できます。これらのパラメータまたは下位分類は、ホスト一致、MIME 一致、サーバ一致、URL 一致などの使用可能な一致選択肢の任意の組み合わせにできます。その他の Cisco IOS リリースおよびプラットフォームでは、ルータ別プロトコル別に最大 24 個のパラメータまたは下位分類を指定できます。

www.*anydomain* .com 部分を照合するには、ホスト名照合機能を使用します。パラメータ指定文字列は、次のオプションを持つ正規表現の形式を取ることができます。

オプション	説明
	この位置にある 0 文字以上の文字と一致します。
	この位置にある任意の 1 文字と一致します。
	選択した文字と一致します。
(|)	範囲内の選択した文字と一致します。たとえば、cisco.(gif|jpg) は cisco.gif または cisco.jpg と一致します。

[ ]	指定した範囲内の任意の文字、または特殊文字と一致します。たとえば、[0-9] はすべての数字です。[*] は「*」の文字で、[[] は「[」の文字です。

HTTP ヘッダー フィールドの分類

Cisco IOS Release 12.3(11)T では、HTTP ヘッダー フィールドの情報を使用して HTTP トラフィックを分類できる拡張機能が NBAR に導入されました。

HTTP はクライアント/サーバ モデルを使用して機能します。HTTP クライアントは HTTP サーバに要求メッセージを送信することで接続を開きます。HTTP サーバは HTTP クライアントに対して応答メッセージを返します（通常、この応答メッセージは、HTTP クライアントからの要求メッセージで要求されたリソースです）。HTTP サーバは応答の送信後に接続を閉じ、トランザクションは完了します。

HTTP ヘッダー フィールドは、HTTP 要求メッセージと応答メッセージに関する情報を提供するために使用されます。HTTP には多数のヘッダー フィールドがあります。HTTP ヘッダーの詳細については、RFC 2616『Hypertext Transfer Protocol--HTTP/1.1』のセクション 14 を参照してください。このドキュメントは、次の URL で参照できます。

http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

（クライアントからサーバへの）要求メッセージの場合、NBAR を使用して次の HTTP ヘッダー フィールドを識別できます。

- User-Agent
- Referer

（サーバからクライアントへの）応答メッセージの場合、NBAR を使用して次の ヘッダー フィールドを識別できます。

- Server
- Location
- Content-Encoding
- Content-Base

（注） これまで Content-Base フィールドの使用は HTTP コミュニティで実装されませんでした（詳細については、RFC 2616 を参照してください。）そのため、Supervisor 32/PISA エンジンが搭載された Catalyst 6500 シリーズ スイッチ上の NBAR では、Content-Base フィールドは識別されません。

NBAR 内では、要求メッセージを指定するには、**matchprotocolhttpc-header-field** コマンドを使用します（このコマンドの **c-header-field** 部分の「c」はクライアントの「c」です）。応答メッセージを指定するには、**matchprotocolhttps-header-field** コマンドを使用します（このコマンドの **s-header-field** 部分の「s」はサーバの「s」です）。

URL、ホスト、MIME タイプ、および HTTP ヘッダーの組み合わせは、NBAR 設定時に使用できることに注意してください。この組み合わせによって、ネットワーク要件に基づく特定の HTTP トラフィックの分類がさらに柔軟になります。

（注） Supervisor 32/PISA を搭載した Cisco Catalyst 6500 シリーズ スイッチ上の Cisco IOS Release 12.2(18)ZY2 以降のリリースと、Cisco IOS Release 15.1(2)T 以降のリリースでは、**matchprotocolhttp** コマンドの **c-header-field** キーワード、**s-header-field** キーワード、および関連する引数を使用することができません。

例

次の例では、クラスマップ class1 内で、後ろに 0 文字以上が続く文字列 whatsnew/latest を含む URL に基づいて HTTP パケットを分類します。

```
class-map class1
 match protocol http url whatsnew/latest*
```

次の例では、クラス マップ class2 内で、後ろに 0 文字以上が続く文字列 cisco を含むホスト名に基づいてパケットを分類します。

```
class-map class2
 match protocol http host cisco*
```

次の例では、クラス マップ class3 内で、JPEG MIME タイプに基づいてパケットを分類します。

```
class-map class3
 match protocol http mime "*jpeg"
```

次に、Content-Base（使用可能な場合）、Content-Encoding、Location、または Server ヘッダー フィールドに「gzip」を含む応答メッセージが、NBAR によって分類される例を示します。 通常、「gzip」のような形式の項目は、応答メッセージの Content-Encoding ヘッダー フィールドで見られます。

```
class-map class4
 match protocol http s-header-field "gzip"
```

次に、HTTP ヘッダー フィールドと URL を組み合わせてトラフィックを分類する例を示します。この例では、「CERN-LineMode/3.0」の User-Agent フィールドと「CERN/3.0」の Server フィールドと URL「www.cisco.com/routers」を含むトラフィックが、NBAR を使用して分類されます。

```
class-map match-all c-http
 match protocol http c-header-field "CERN-LineMode/3.0"
 match protocol http s-header-field "CERN/3.0"
 match protocol http url "www.cisco.com/routers"
```

Supervisor 32/PISA エンジンが搭載された Catalyst 6500 シリーズ ルータの例

次の 2 つの例では、（**c-header-field** および **s-header-field** キーワードの代わりに）個別のキーワードと関連する引数を使用して、トラフィックを指定します。

最初の例では、**user-agent**、**referrer**、および **from** キーワードが指定されています。2 番目の例では、server、location、および content-encoding キーワードが指定されています。

```
class-map match-all test1
 match protocol http user-agent Mozilla
 match protocol http referrer *10.0.10.50”
 match protocol http from *example.com”
class-map match-all test2
 match protocol http server Apache
 match protocol http location *example.com”
 match protocol http content-encoding compress
 match protocol http match protocol http content-base *exmaple.com”
```

関連コマンド

コマンド	説明
showipnbarprotocol-discovery	NBAR Protocol Discovery 機能によって収集された統計情報を表示します。

match protocol pppoe-discovery

コントロール プレーンに送信される PPP over Ethernet（PPPoE）コントロール プレーン パケットを照合して分類するには、QoS クラスマップ コンフィギュレーション モードで **matchprotocolpppoe-discovery** コマンドを使用します。この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 protocol pppoe-discovery
no match protocol pppoe-discovery

構文の説明

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

コントロール プレーンに送信される PPPoE コントロール パケットは、照合または分類されません。

コマンド モード

QoS クラスマップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 2.3	このコマンドは、Cisco ASR 1000 シリーズ アグリゲーション ルータで追加されました。

使用上のガイドライン

matchpppoe-discovery コマンドは、コントロール プレーン ポリシング（CoPP）などのコントロール プレーン関連の機能に関連付けられています。

クラス マップで使用する場合、**matchprotocolpppoe-discovery** コマンドは、入力 PPPoE コントロール プレーン パケットまたは出力 PPPoE コントロール プレーン パケットを分類して、指定されたトラフィック クラスに含めることができます。そして、ポリシー マップでそのクラスを設定して、必要な Quality of Service（QoS）機能（トラフィック ポリシングなど）を受けることができます。

（注） CSCts20715 では、**matchprotocolpppoe-discovery** コマンドは、ATM サブインターフェイスで設定された自動仮想回線（AutoVC）を介して受信された PPPoE Active Discovery Initiation（PADI）パケットを照合します。PADI パケットの各 ATM セルは、個別のパケットとしてパントされ、PPPOE_DISCOVERY パケット数に考慮されます。

例

次に、copplass-pppoe-discovery という名前のクラスマップで設定された **matchprotocolpppoe-discovery** コマンドの例を示します。一致基準を満たすと特定された PPPoE コントロール プレーン トラフィックが、coppclass-pppoe-discovery という名前のクラスに配置されます。

そして、coppclass-pppoe-discovery クラスは copp-policy-pppoe-discovery という名前のポリシー マップで設定され、**police** コマンドを使用して QoS トラフィック ポリシング機能が適用されます。

```
Router> enable
Router# configure terminal
Router(config)# class-map match-all coppclass-pppoe-discovery
Router(config-cmap)# match protocol pppoe-discovery
Router(config-cmap)# exit
Router(config)# policy-map copp-policy-pppoe-discovery
Router(config-pmap)# class coppclass-pppoe-discovery
Router(config-pmap-c)# police rate 8000 bps conform-action transmit exceed-action drop
Router(config-pmap-c-police)# end
```

関連コマンド

コマンド	説明
control-plane	ユーザが、装置のコントロールプレーンに関連付けられた属性またはパラメータ（サービス ポリシーなど）の関連付けおよび変更が許可されるコントロール プレーン コンフィギュレーション モードを開始します。
matchprotocol	指定されたプロトコルに基づいて、クラスマップの一致基準を設定します。
police rate	コントロール プレーン宛のトラフィックに対するトラフィック ポリシングを設定します。
show policy-mapcontrol-plane	集約または分散コントロール プレーン サービスのコントロール プレーンにアタッチされたポリシーマップ内にある、1つのトラフィック クラスまたはすべてのトラフィック クラスの設定と統計情報を表示します。
showpppoesession	現在アクティブな PPPoE セッションに関する情報を表示します。

match protocol rtp

Real-Time Transfer Protocol（RTP）トラフィックを照合するように Network-Based Application Recognition（NBAR）を設定するには、クラスマップ コンフィギュレーション モードで **matchprotocolrtp** コマンドを使用します。NBAR による RTP トラフィックの照合を無効にするには、このコマンドの **no** 形式を使用します。

match protocol rtp [{**audio**|**video**|**payload-type** *payload-string*}]
no match protocol rtp [{**audio**|**video**|**payload-type** *payload-string*}]

構文の説明

audio	（任意）オーディオペイロードタイプ値の範囲 0 ～ 23（オーディオ トラフィック用に予約）、動的ペイロード タイプ値の範囲 96 ～ 127 による照合を指定します。
video	（任意）ビデオ ペイロード タイプ値の範囲 24 ～ 33 による照合を指定します。このペイロード タイプ値がビデオ トラフィック用に予約されています。
payload-type	（任意）**audio** または **video** キーワードよりも詳細な情報を指定して、特定のペイロード タイプ値による照合を指定します。
payload-string	（任意）特定のペイロード タイプ値を含むユーザ指定の文字列です。 *payload-string* 引数には、ペイロード タイプ値を区切るためのカンマと、ペイロード タイプ値の範囲を示すためのハイフンを含めることができます。 *payload-string* 引数は、標準の数値に加えて、16 進数（値の前に 0x を付加）および 2 進数（値の前に b を付加）表記で指定できます。

コマンド デフォルト

一致基準が指定されていません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(8)T	このコマンドが導入されました。
12.1(11b)E	このコマンドが Cisco IOS Release 12.1(11b)E に統合されました。
12.1(13)E	このコマンドが、FlexWAN モジュールを備えていない Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
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。

使用上のガイドライン

他のキーワードを使用せずに **matchprotocolrtp** コマンドを入力すると、すべての RTP トラフィックが成功する一致基準として確立されます。

RTP はマルチメディア データ ストリームのパケット形式です。メディアオンデマンドやインタラクティブ サービス（インターネット テレフォニーなど）に使用できます。RTP はデータとコントロール部分から構成されます。コントロール部分は Real-Time Transport Control Protocol（RTCP）と呼ばれます。注意が必要なのは、NBAR RTP Payload Classification（RTP ペイロード分類）機能では RTCP パケットを識別しない点と、RTCP パケットは奇数ポートで実行され、RTP パケットは偶数ポートで実行される点です。

RTP パケットのペイロード タイプ フィールドは RTP ペイロードの形式を識別し、番号によって表されます。NBAR は、RTP パケットのこのフィールドに基づいて RTP トラフィックを照合します。RTP トラフィックを照合するように NBAR を設定する場合は、RTP および RTP ペイロード タイプの実用的な知識が役立ちます。RTP および RTP ペイロード タイプの詳細については、RFC 1889『*RTP: A Transport Protocol for Real-Time Applications*』を参照してください。

例

次に、すべての RTP トラフィックを照合するように NBAR を設定する例を示します。

```
Device(config)# class-map class1
Device(config-cmap)# match protocol rtp
```

次に、ペイロードタイプが 0、1、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、および 64 の RTP トラフィックを照合するように NBAR を設定する例を示します。

```
Device(config)# class-map class2
Device(config-cmap)# match protocol rtp payload-type "0, 1, 4-0x10, 10001b-10010b, 64"
```

match qos-group

特定の Quality of Service（QoS）グループ値を一致基準として識別するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchqos-group** コマンドを使用します。クラス マップから特定の QoS グループ値を削除するには、このコマンドの **no** 形式を使用します。

match qos-group *qos-group-value*
no match qos-group *qos-group-value*

構文の説明

qos-group-value	QoS グループ値の識別に使用される、0 ～ 99 の正確な値です。

コマンド デフォルト

一致基準は指定されていません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。
12.2(13)T	このコマンドが Cisco IOS Release 12.2(13)T に統合されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
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。
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ ルータに実装されました。
15.1(3)T	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーション モードにします。

matchqos-group コマンドはクラス マップで使用され、パケット上の特定の QoS グループ値マーキングを識別します。このコマンドは、受信したマルチプロトコル ラベル スイッチング（MPLS）の Experimental（EXP）フィールド値を出力インターフェイスに搬送するのにも使用できます。

qos-group-value 引数は、マーキングにのみ使用します。QoS グループ値に数学的な意味はありません。たとえば、2 という *qos-group-value* は 1 より大きいわけではありません。値は単に 2 という *qos-group-value* でマーキングされているパケットが 1 という *qos-group-value* でマーキングされているパケットとは異なるということを示しているに過ぎません。これらのパケットの処理は、ユーザが、QoS ポリシー マップ クラス コンフィギュレーション モードでの QoS ポリシーの設定を通じて定義します。

QoS グループ値は、ルータにローカルです。つまり、パケットにマーキングされている QoS グループ値は、パケットがそのルータを離れてもルータから離れません。パケット内に存在するマーキングが必要な場合は、IP 優先順位設定、IP Diffserv コード ポイント（DSCP）値、またはその他のパケット マーキング手法を使用してください。

このコマンドは、**random-detectdiscard-class-based** コマンドと併用できます。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、s**ervice-policytypeperformance-monitorinline** コマンドを入力する必要があります。

例

次に、priority50 という名前のサービス ポリシーを設定して、サービス ポリシー priority50 をインターフェイスに付加する例を示します。この例では、qosgroup5 という名前のクラス マップで、ファスト イーサネット インターフェイス 1/0/0 に入ってきたすべてのパケットについて、QoS グループ値が 5 かどうかを評価します。受信パケットが QoS グループ値 5 でマーキングされていれば、そのパケットはプライオリティ レベル 50 で処理されます。

```
Router(config)#

class-map qosgroup5
Router(config-cmap)
#
 match qos-group 5
Router(config)#

exit
Router(config)#

policy-map priority50
Router(config-pmap)#

class qosgroup5
Router(config-pmap-c)#

priority 50
Router(config-pmap-c)#
```

```
exit
Router(config-pmap)#

exit
Router(config)#

interface fastethernet1/0/0
Router(config-if)#

service-policy output priority50
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor用のサービス ポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過する、QoS 値 4 の基準に一致するパケットが、**fm-2** という名前のフロー モニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match qosgroup 4
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
random-detectdiscard-class-based	WRED の基礎をパケットのクラス廃棄値にします。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシーマップを対応付けます。
setprecedence	トラフィック クラス内のパケットの IP 優先順位値を指定します。
setqos-group	後からパケットの分類に使用できるグループ ID を設定します。

match source-address mac

一致基準として送信元MACアドレスを使用するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **matchsource-addressmac** コマンドを使用します。以前に一致基準として指定していた送信元 MAC アドレスを削除するには、このコマンドの **no** 形式を使用します。

match source-address mac *address-source*
no match source-address mac *address-source*

構文の説明

address-source	一致基準として使用される送信元MACアドレスです。

コマンド デフォルト

一致基準は設定されていません。

コマンド モード

クラスマップ コンフィギュレーション（config-cmap）
ポリシー インライン コンフィギュレーション（config-if-spolicy-inline）

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズに実装されました。
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 Cisco Performance Monitor 用に Cisco IOS Release 15.1(3)T に統合されました。ポリシー インライン コンフィギュレーション モードのサポートが追加されました。
12.2(58)SE	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 12.2(58)SE に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、異なるコマンドを使用して、このコマンドを発行するコンフィギュレーション モードにします。

このコマンドは、MAC アドレスを持つ入力インターフェイス（ファスト イーサネット インターフェイスやイーサネット インターフェイスなど）でのみ使用できます。

このコマンドは、MAC アドレスのない出力インターフェイス（シリアル インターフェイスや ATM インターフェイスなど）では使用できません。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

まず、s**ervice-policytypeperformance-monitorinline** コマンドを入力する必要があります。

例

次の例では、MAC アドレス mac 0.0.0 を一致基準として使用します。

```
Router(config)# class-map matchsrcmac
Router(config-cmap)
#
match source-address mac 0.0.0
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

次に、ポリシー インライン コンフィギュレーション モードを使用して Performance Monitor用のサービス ポリシーを設定する例を示します。このポリシーは、イーサネット インターフェイス 0/0 を通過する、指定された送信元 MAC アドレスに一致するパケットが、**fm-2** という名前のフローモニタ設定で指定されたパラメータに基づいてモニタされるように指定します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match source-address mac 0.0.0
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
service-policytypeperformance-monitor	Performance Monitor ポリシーをインターフェイスに関連付けます。

match start

（注） Cisco IOS Release 15.2(4)M では、Cisco IOS ソフトウェアで **match start** コマンドを使用できません。

データグラム ヘッダー（レイヤ2）またはネットワーク ヘッダー（レイヤ3）に基づいてクラス マップの一致基準を設定するには、クラスマップ コンフィギュレーション モードで **match start** コマンドを使用します。指定した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 start {**l2-start**|**l3-start**} **offset** *number* **size** *number* {**eq**|**neq**|**gt**|**lt**|**range** *range*|**regex** *string*} {*value* [*value2*][*string*]}
no match start {**l2-start**|**l3-start**} **offset** *number* **size** *number* {**eq**|**neq**|**gt**|**lt**|**range** *range*|**regex** *string*} {*value* [*value2*][*string*]}

構文の説明

l2-start	データグラム ヘッダーから一致基準が始まります。
l3-start	ネットワーク ヘッダーから一致基準が始まります。
offset *number*	任意のオフセットに従って一致基準を作成できます。
size *number*	照合を行うバイト数です。
eq	パケットが指定された値またはマスクと等しい場合に、一致基準が満たされます。
neq	パケットが指定された値またはマスクと等しくない場合に、一致基準が満たされます。
mask	（任意）**eq** または **neq** キーワードが発行された場合に使用できます。
gt	パケットが指定された値よりも大きい場合に、一致基準が満たされます。
lt	パケットが指定された値未満の場合に、一致基準が満たされます。
range *range*	一致基準は、下限および上限のプロトコルのフィールド範囲に基づきます。
regex *string*	一致基準は、照合される文字列に基づきます。
value	パケットが一致する必要がある値です。

コマンド デフォルト

一致基準は設定されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。
12.2(18)ZY	このコマンドが、Catalyst 6500 シリーズの Programmable Intelligent Services Accelerator（PISA）が搭載されているスイッチの Cisco IOS Release 12.2(18)ZY に統合されました。
Cisco IOS XE 2.2	このコマンドが、Cisco IOS XE Release 2.2 に統合されました。

使用上のガイドライン

Flexible Packet Matching に使用される一致基準には、まず **class-map** コマンドを入力して、一致基準を確立するクラスの名前を指定する必要があります。その後、次のいずれかのコマンドを入力できます。

- **match field**（プロトコル ヘッダー説明ファイル（PHDF）に定義されているフィールドに基づいて、クラス マップの一致基準を設定します）
- **match start**（PHDF がルータにロードされていない場合に使用できます）

例

次に、ブラスタ パケット用に FPM を設定する方法の例を示します。このクラス マップには、TCP ポート 135、4444 または UDP ポート 69、および IP ヘッダーの開始から 3 バイトでのパターン 0x0030 という一致基準が含まれています。

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
load protocol	PHDF をルータにロードします。
match field	PHDF に定義されているフィールドに基づいて、クラス マップの一致基準を設定します。

match tag (class-map)

クラスマップのタグ タイプに照合されるタグを指定するには、クラスマップ コンフィギュレーション モードで **matchtag** コマンドを使用します。タグを削除するには、このコマンドの **no** 形式を使用します。

match tag タグ名
no match tag タグ名

構文の説明

タグ名	タグの名前です。

コマンド デフォルト

照合タグは定義されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.4(6)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

Access Control Server（ACS）が、Cisco attribute-value（AV）ペアを使用して、ネットワーク アクセス デバイス（NAD）にタグ属性を送信します。（タグ属性は、IETF 属性 88 を使用して NAD に送信することもできます。）

例

次の例は、照合されるタグの名前が「healthy」であることを示しています。

```
Router(config)# class-map type tag healthy_class
Router(config-cmap)# match tag healthy
```

Router(config-cmap)# **end**

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラスマップを作成します。

match vlan (QoS)

仮想ローカルエリア ネットワーク（VLAN）の識別番号を基本にしてトラフィックの照合と分類を行うには、クラスマップ コンフィギュレーション モードで **matchvlan** コマンドを使用します。以前に一致基準として指定していた VLAN 識別番号を削除するには、このコマンドの **no** 形式を使用します。

match vlan *vlan-id-number*
no match vlan *vlan-id-number*

構文の説明

vlan-id-number	1 つの VLAN 識別番号、複数の VLAN 識別番号、または番号の範囲。指定できる VLAN 識別番号は、1 ～ 4095 の範囲内の値です。

コマンド デフォルト

VLAN 識別番号を基本にしたトラフィックの照合は行われません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(31)SB2	このコマンドが Cisco 10000 シリーズ ルータ専用のコマンドとして追加されました。.
15.1(1)T	このコマンドが変更されました。このコマンドのサポートが、Cisco 10000 シリーズ ルータに限定されなくなりました。
Cisco IOS XE Release 2.1	このコマンドが変更されました。このコマンドのサポートが、Cisco ASR 1000 シリーズ ルータに追加されました。

使用上のガイドライン

VLAN 識別番号の指定

単一の VLAN 識別番号、スペースで区切った複数の VLAN 識別番号（2 5 7 など）、またはハイフンで区切った VLAN 識別番号の範囲（25 ～ 35 など）を指定できます。

サポートの制限事項

matchvlan コマンドには、次の制限事項があります。

- **matchvlan** コマンドは、IEEE 802.1Q および Inter-Switch Link（ISL）VLAN カプセル化にのみサポートされています。
- Cisco IOS Release 12.2(31)SB2 の場合、**matchvlan** コマンドは Cisco 10000 シリーズ ルータでのみサポートされます。

例

次の設定例では、VLAN 識別番号の範囲を基本にしてトラフィックを分類および照合するために、**matchvlan** コマンドを有効にしています。25 ～ 50 の範囲内の VLAN 識別番号を持つパケットは、class1 というクラス内に置かれます。

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match vlan 25-50
```

Router(config-cmap)# **end**

（注） 一般に、その次の手順では、ポリシー マップ内で class1 を設定し、ポリシー マップ内で Quality of Service（QoS）機能をイネーブルにし（たとえば、クラスベース重み付け均等化キューイング（CBWFQ））、ポリシー マップをインターフェイスにアタッチします。ポリシーマップを設定するには、**policy-map** コマンドを使用します。CBWFQ を有効にするには、**bandwidth** コマンドを使用します（または、有効にする QoS 機能用のコマンドを使用します）。ポリシー マップをインターフェイスにアタッチするには、**service-policy** コマンドを使用します。一致基準に基づいたネットワーク トラフィックの分類の詳細については、『Cisco IOS Quality of Service Solutions Configuration Guide , Release 12.4T』の「Classification」パートを参照してください。

関連コマンド

コマンド	説明
bandwidth(policy-mapclass)	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。
class-map	指定したクラスへのパケットのマッチングに使用するクラスマップを作成します。
policy-map	1つまたは複数のインターフェイスにアタッチできるポリシーマップを作成または変更します。
service-policy	インターフェイスにポリシー マップをアタッチします。

match vlan inner

802.1Q タグ付きフレームの最も内側の VLAN ID を照合するようにクラス マップを設定するには、ATM インターフェイス コンフィギュレーション モードで **matchvlaninner** コマンドを使用します。802.1Q タグ付きフレームの最も内側の VLAN ID での照合を削除するには、このコマンドの **no** 形式を使用します。

match vlan inner *vlan-ids*
no match vlan inner *vlan-ids*

構文の説明

vlan-ids	照合する 1 つ以上の VLAN ID です。VLAN ID の有効範囲は 1 ～ 4095 で、VLAN ID のリストには次のいずれかまたはすべてを含めることができます。 • スペースで区切られた単一の VLAN ID。例：100 200 300 • スペースで区切られた 1 つ以上の VLAN ID の範囲。例：1-1024 2000-2499

コマンド デフォルト

パケットは着信 dot1q VLAN 内部 ID に基づいて照合されません。

コマンド モード

クラス マップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(18)SXF	このコマンドが Cisco 7600 シリーズ ルータに実装されました。

例

次に、VLAN ID が 100 ～ 300 のパケットを照合するクラス マップを作成する例を示します。

```
Router(config)#
cclass-map match-all vlan100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# class-map match-all vlan200
Router(config-cmap)# match vlan inner 200
Router(config-cmap)# exit
Router(config)# class-map match-all vlan300
Router(config-cmap)# match vlan inner 300
```

関連コマンド

コマンド	説明
clearceflinecard	1 つ以上のライン カード上の Cisco Express Forwarding（CEF）情報をクリアしますが、メイン ルート プロセッサ（RP）上の CEF 情報はクリアしません。これにより、ライン カード上の CEF 情報が RP 上の CEF 情報と同期されます。
matchqos-group	一致基準として特定の QoS グループ値を指定します。
mlsqostrust	保存する必要があるパケットの着信 QoS フィールドを決めるために、インターフェイスの信頼状態を設定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。
showplatformqospolicy-map	ルータに設定されているポリシーマップのタイプと数を表示します。

maximum（ローカル ポリシー）

リソース予約プロトコル（RSVP）リソースの制限を設定するには、ローカル ポリシー コンフィギュレーション モードで**maximum** コマンドを使用します。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。

maximum [{**bandwidth** [{**group**|**single**}] *bandwidth*|**senders** *maximum-senders*}]
no maximum [{**bandwidth** [{**group**|**single**}]|**senders**}]

構文の説明

bandwidth	（任意）RSVP 予約の帯域幅制限を示します。
group	（任意）ローカル ポリシーでカバーされるすべての予約で要求可能な帯域幅の量を kbps 単位で指定します。
single	（任意）ローカル ポリシーでカバーされる特定の RSVP 予約で要求可能な最大帯域幅を kbps 単位で指定します。
bandwidth	要求される帯域幅の上限（kbps 単位）です。範囲は 1 ～ 10000000 です。
senders	（任意）ルータで同時にアクティブにできる、ローカル ポリシーの影響を受ける RSVP 送信者の数を制限します。
maximum-senders	指定されたポリシーが許可する送信者の最大数です。範囲は 1 ～ 50000 で、デフォルトは 1000 です。

コマンド デフォルト

最大帯域幅制限は設定されず、RSVP 送信者も設定されません。

コマンド モード

ローカル ポリシー コンフィギュレーション（config-rsvp-local-if-policy）

コマンド履歴

リリース	変更箇所
12.0(29)S	このコマンドが導入されました。
12.4(6)T	このコマンドが、RESV メッセージに適用されるように変更されました。
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。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

アプリケーション ID の機能拡張の一環として、**maximumbandwidth** コマンドを RESV メッセージに適用します。この変更には、次の利点があります。

- 共有予約と非共有予約の両方に対する RSVP のアドミッション制御プロセスで、ローカル ポリシー帯域幅制限を使用できます。PATH メッセージのグループ帯域幅チェックを実行

していたリリースでは、帯域幅の共有が考慮できなかったため、ポリシー用により大きな最大グループ帯域幅を作成することで、共有を考慮する必要がありました。

- また、ポリシー帯域幅が不十分で着信 RESV メッセージのニーズを満たせない場合に、ローカル ポリシーでアドミッション コントロール機能中のプリエンプションをトリガーできます。

例

次に、最大帯域幅を、予約のグループおよび単一の予約用にそれぞれ指定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 1/0
Router(config-if)# ip rsvp policy local identity video
Router(config-rsvp-local-policy)# maximum bandwidth group 500
Router(config-rsvp-local-policy)# maximum bandwidth single 50
```

関連コマンド

コマンド	説明
iprsvppolicylocal	RSVP 要求に対する認証の実行方法を決定します。

maximum bandwidth ingress

入力ポリシープールの帯域幅パラメータを設定するには、ローカルポリシーコンフィギュレーション モードまたはローカル ポリシー インターフェイス コンフィギュレーション モードで **maximumbandwidthingress** コマンドを使用します。入力ポリシー プールの帯域幅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。

ローカル ポリシー コンフィギュレーション モードでのコマンド シンタックス

maximum bandwidth ingress {**group**|**single**} *bandwidth*
no maximum bandwidth ingress {**group**|**single**}

ローカル ポリシー インターフェイス コンフィギュレーション モードでのコマンド シンタックス

maximum bandwidth ingress {**group** *bandwidth*|**percent** {**group**|**single**} パーセント|**single** *bandwidth*}
no maximum bandwidth ingress {**group**|**percent** {**group**|**single**}|**single**}

構文の説明

group	ローカル ポリシーでカバーされるすべての予約で要求可能な最大入力帯域幅を kb/s 単位で指定します。
single	ローカル ポリシーでカバーされる特定の RSVP 予約で要求可能な最大入力帯域幅を kb/s 単位で指定します。
bandwidth	要求される入力帯域幅の上限（kb/s 単位）です。
percent {**group** | **single**}	インターフェイスの入力帯域幅のパーセンテージを、フローのグループまたは単一のフローで使用できる最大帯域幅として指定します。
パーセント	要求される帯域幅の上限（パーセント単位）です。

コマンド デフォルト

デフォルトでは、RSVP は無効になっています。そのため、最大帯域幅制限は設定されません。

コマンド モード

ローカル ポリシー コンフィギュレーション（config-rsvp-local-policy）
ローカル ポリシー インターフェイス コンフィギュレーション（config-rsvp-local-if-policy）

コマンド履歴

リリース	変更箇所
15.1(3)T	このコマンドが導入されました。
15.1(1)S	このコマンドが、Cisco IOS Release 15.1(1)S に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

maximumbandwidthingress コマンドを使用して、指定されたポリシーの最大帯域幅を設定できます。また、インターフェイスのRSVP入力帯域幅のパーセンテージを、ポリシーに一致するフローのグループまたは単一のフローで使用できる最大帯域幅として設定することもできます。最大帯域幅として設定されるRSVP帯域幅のパーセンテージは、グローバルベースのRSVPポリシーでは使用できませんが、インターフェイス RSVP ポリシーでは使用できます。

maximumbandwidthingresspercent コマンドは、**maximumbandwidthingressgroup** コマンドおよび **maximumbandwidthingresssingle** コマンドと相互に排他的です。つまり、**maximumbandwidthingresspercent** コマンドを使用して RSVP 入力帯域幅の最大パーセンテージを設定した場合、**maximumbandwidthingressgroup** コマンドおよび **maximumbandwidthingresssingle** コマンドを使用して作成された設定は削除されます。

例

次に、グローバルベースの RSVP ポリシーで、グループ予約とシングル予約のそれぞれの最大入力帯域幅を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip rsvp policy local identity rsvp-video
Device(config-rsvp-local-policy)# maximum bandwidth ingress group
 200
Device(config-rsvp-local-policy)# maximum bandwidth ingress single 100
The following example shows how to configure the maximum percentage of RSVP ingress
bandwidth of an interface for a group of reservations and for a single reservation,
respectively:
Device> enable
Device# configure terminal
Device(config)# interface tunnel 0
Device(config-if)# ip rsvp policy local identity rsvp-video
Device(config-rsvp-local-if-policy)# maximum bandwidth ingress percent group 50
Device(config-rsvp-local-if-policy)# maximum bandwidth ingress single 50
```

関連コマンド

コマンド	説明
showiprsvpingress	インターフェイスに設定された RSVP 入力帯域幅に関する情報を表示します。

maximum bandwidth percent

インターフェイスのリソース予約プロトコル（RSVP）帯域幅のパーセンテージを、フローのグループまたは単一のフローで使用できる最大帯域幅として設定するには、ローカルポリシーコンフィギュレーションモードで**maximumbandiwidthpercent**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。

maximum bandwidth percent {**group**|**single**} *bandwidth-percentage*
no maximum bandwidth percent {**group**|**single**}

構文の説明

group	ローカルポリシーでカバーされるすべての予約で要求可能な帯域幅の量を kb/s 単位で指定します。
single	ローカル ポリシーでカバーされる特定の RSVP 予約で要求可能な最大帯域幅を kb/s 単位で指定します。
bandwidth-percentage	要求される帯域幅の上限（kb/s 単位）です。

コマンド デフォルト

デフォルトでは、RSVP は無効になっています。そのため、パーセンテージ帯域幅は設定されません。

コマンド モード

ローカル ポリシー コンフィギュレーション（config-rsvp-local-if-policy）

コマンド履歴

リリース	変更箇所
15.1(2)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

maximumbandwidthpercent コマンドは、**maximumbandwidthgroup** コマンドおよび **maximumbandwidthsingle** コマンドと相互に排他的です。つまり、**maximumbandwidthpercent** コマンドを使用して RSVP の最大パーセンテージを設定した場合、**maximumbandwidthgroup** コマンドおよび **maximumbandwidthsingle** コマンドを使用して作成された設定は削除されます。**maximumbandwidthpercent** コマンドは、グローバル RSVP ポリシーにはありません。

フローのグループに設定されたRSVP帯域幅の最大パーセンテージは、ポリシーに一致するフローの RSVP コール アドミッション制御（CAC）を行うために使用されます。**maximumbandiwidthpercent** コマンドでは、オーバーサブスクリプションが可能です。つまり、100 パーセントを超える RSVP 帯域幅を、グループ予約の最大帯域幅または単一の予約の最大帯域幅として設定できます。

例

次に、インターフェイスの RSVP 帯域幅の最大パーセンテージを、予約のグループおよび単一の予約用にそれぞれ設定する例を示します。

```
Router> enable
```

```
Router# configure terminal
Router(config)# interface fastethernet 1/0
Router(config-if)# ip rsvp policy local identity video
Router(config-rsvp-local-policy)# maximum bandwidth percent group 50
Router(config-rsvp-local-policy)# maximum bandwidth single 50
```

関連コマンド

コマンド	説明
iprsvppolicylocal	RSVP要求に対する認証の実行方法を決定します。
maximum (local policy)	RSVP リソースの制限を設定します。

maximum header

圧縮された IP ヘッダーの最大サイズを指定するには、IPHC プロファイル コンフィギュレーション モードで **maximumheader** コマンドを使用します。圧縮された IP ヘッダーの最大サイズをデフォルト サイズに戻すには、このコマンドの **no** 形式を使用します。

maximum header *number-of-bytes*
no maximum header

構文の説明

number-of-bytes	最大ヘッダー サイズ（バイト単位）です。有効なエントリは 20 ～ 168 の数字です。デフォルトは 168 です。

コマンド デフォルト

圧縮された IP ヘッダーの最大サイズは 168 バイトです。

コマンド モード

IPHC 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	変更箇所
12.4(9)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

maximumheader コマンドを使用すると、圧縮されるパケットの IP ヘッダーの最大サイズを定義できます。この最大サイズを超える IP ヘッダーを持つパケットは、圧縮されずに送信されます。

圧縮される IP ヘッダーのサイズを制限するには、**maximumheader** コマンドの *number-of-bytes* 引数を使用します。

IPHC プロファイルでの使用目的

maximumheader コマンドは、IPHC プロファイルの一部として使用することを目的としています。IPHC プロファイルは、ネットワークでのヘッダー圧縮を有効および設定するために使用されます。IPHC プロファイルを使用してヘッダー圧縮を設定する詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、リリース 12.4T の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

前提条件

maximumheader コマンドを使用する前に、TCP ヘッダー圧縮または非 TCP ヘッダー圧縮のいずれかを有効にする必要があります。TCP ヘッダー圧縮を有効にするには、**tcp** コマンドを使用します。非 TCP ヘッダー圧縮を有効にするには、**non-tcp** コマンドを使用します。

例

profile2 という IPHC プロファイルの例を、次に示します。この例では、圧縮された IP ヘッダーの最大サイズが 75 バイトに設定されます。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# maximum header 75
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
iphc-profile	IPHC プロファイルを作成します。
non-tcp	IPHC プロファイルの非 TCP ヘッダー圧縮を有効にします。
tcp	IPHC プロファイル内の TCP ヘッダー圧縮を有効にします。

max-reserved-bandwidth

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**max-reservedbandwidth** コマンドは非表示です。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンド シーケンス）を使用する必要があります。詳細（代替コマンドのリストを含む）については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**max-reservedbandwidth** コマンドは、モジュラ QoS CLI（MQC）コマンド（または MQC コマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

リソース予約プロトコル（RSVP）、クラスベース重み付け均等化キューイング（CBWFQ）、低遅延キューイング（LLQ）、IP RTP プライオリティ、フレーム リレー IP RTP プライオリティ、フレーム リレー PVC インターフェイス プライオリティ キューイング（PIPQ）、または階層型キューイング フレームワーク（HQF）に割り当てられるインターフェイス帯域幅のパーセントを変更するには、インターフェイス コンフィギュレーション モードで **max-reservedbandwidth** 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。

max-reserved-bandwidth パーセント
no max-reserved-bandwidth

構文の説明

パーセント	RSVP、CBWFQ、LLQ、IP RTP プライオリティ、フレーム リレー IP RTP プライオリティ、フレーム リレー PIPQ、および HQF に割り当てられるインターフェイス帯域幅の量です。

コマンド デフォルト

この制限がない Cisco 7500 シリーズ ルータを除く、すべてのサポート対象プラットフォームで 75% 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	変更箇所
12.0(5)T	このコマンドが導入されました。
12.4(20)T	モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）を使用した HQF のサポートが追加されました。 （注） このリリースが、このコマンドがサポートされる最後の T リリースです。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

使用上のガイドライン

max-reserved-bandwidth コマンドは、Cisco IOS Release 12.2SR または 12.2SX ではサポートされていません。12.4T ではサポートされていますが、HQF 機能が統合された 12.4(20)T リリースまででのみサポートされています。

インターフェイス上のすべての帯域幅割り当ての合計が、インターフェイス上の使用可能な帯域幅の 75 パーセントを超えてはなりません。帯域幅の残りの 25 パーセントは、レイヤ 2 オーバーヘッド、制御トラフィック、およびベストエフォート型トラフィックなどのオーバーヘッドに使用されます。

RSVP、CBWFQ、LLQ、IP RTP プライオリティ、フレーム リレー IP RTP プライオリティ、フレーム リレー PIPQ、または HQF に 75% を超える割り当てが必要な場合には、**max-reserved-bandwidth** コマンドを使用できます。*percent* 引数は、使用できる合計インターフェイス帯域幅の最大パーセンテージを指定します。

max-reserved-bandwidth コマンドを使用する場合は、ベストエフォート型トラフィックと制御トラフィックから帯域幅が奪われすぎないようにしてください。

例

次の例では、**showpolicy-map** コマンドの出力に示されているように、policy1 という名前のポリシー マップが、合計 8 Mbps の帯域幅が設定されている 3 つのクラスに設定されています。

```
Router# show policy-map policy1
 Policy Map policy1
  Weighted Fair Queueing
    Class class1
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class2
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
```

```
    Class class3
      Bandwidth 3000 (kbps) Max Threshold 64 (packets)
```

service-policy コマンドを入力して 10-Mbps イーサネット インターフェイスにポリシー マップをアタッチしようとすると、次のようなエラー メッセージが生成されます。

```
I/f Ethernet1/1 class class3 requested bandwidth 3000 (kbps) Available only 2500 (kbps)
```

デフォルトの設定可能な最大帯域幅は使用可能なインターフェイス帯域幅の 75%（この例では 7.5 Mbps）であるため、このエラー メッセージが生成されます。設定可能な最大帯域幅を 80% に変更するには、インターフェイス コンフィギュレーション モードで **max-reserved-bandwidth** コマンドを使用します。

```
max-reserved-bandwidth 80
service output policy1
end
```

ポリシー マップがアタッチされたことを確認するには、**showpolicy-mapinterface** コマンドを入力します。

```
Router# show policy-map interface e1/1
 Ethernet1/1  output :policy1
  Weighted Fair Queueing
    Class class1
      Output Queue:Conversation 265
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class2
      Output Queue:Conversation 266
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class3
      Output Queue:Conversation 267
        Bandwidth 3000 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
```

仮想テンプレートの設定例

次に、CBWFQ による仮想テンプレート設定で完全プライオリティ キューを設定する例を示します。この **max-reserved-bandwidth** コマンドは、CBWFQ と IP RTP プライオリティの間に割り当てられる最大帯域幅を、デフォルト（75%）から 80% に変更します。

```
multilink virtual-template 1
interface virtual-template 1
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 ip rtp priority 16384 16383 25
 service-policy output policy1
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 max-reserved-bandwidth 80
 end
interface Serial0/1
 bandwidth 64
```

```
ip address 10.1.1.2 255.255.255.0
no ip directed-broadcast
encapsulation ppp
ppp multilink
end
```

（注） 仮想アクセス インターフェイスを正しく機能させるために、仮想テンプレートでは **bandwidth** コマンドを設定しないようにします。この例で示されているように、実際のインターフェイスで設定します。

関連コマンド

Command	Description
bandwidth(policy-mapclass)	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。
iprtppriority	UDP 宛先ポートの範囲に属する RTP パケット フロー セットについて、完全プライオリティ キューを予約します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showpolicy-map	指定したサービス ポリシーマップを構成する全クラスの設定、またはすべての既存ポリシーマップに関する全クラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

metadata application-params

メタデータ アプリケーション エントリ コンフィギュレーション モードにして、新しいメタデータ アプリケーション パラメータを作成するには、グローバル コンフィギュレーション モードで **metadata application-params** コマンドを使用します。以前に設定したメタデータ アプリケーション 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。

metadata application-params *app-param-name*

no metadata application-params *app-param-name*

構文の説明

app-param-name	プロビジョニング コントロール プレーン分類の一致基準として使用できるメタデータ アプリケーション名です。

コマンド デフォルト

メタデータベース分類用のアプリケーション パラメータは作成されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
15.2(1)T	このコマンドが導入されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

プロビジョニング コントロール プレーン分類の一致基準として使用できる新しいメタデータ アプリケーション パラメータを作成するには、**metadata application-params** コマンドを使用します。**metadata application-params** コマンドは、デバイスをメタデータ アプリケーション エントリ コンフィギュレーション モードにします。メタデータ アプリケーション エントリ コンフィギュレーション モードで次のコマンドを使用して、アプリケーションのプロパティを設定します。名前と ID の設定は必須です。

- **default**：指定されたアプリケーションの名前、説明、および ID のデフォルト プロパティです。
- **description** *description-text*：アプリケーションの説明です。55 文字までで指定します。
- **identifier** *id-value*：アプリケーション ID です。内部的にアプリケーション名にマッピングされます。範囲は 1 ～ 16777215 です。
- **name** *name*：アプリケーションの名前です。24 文字までで指定します。

すべてのメタデータ アプリケーションの詳細を表示するには、**show metadata application table** コマンドを使用します。

例

次に、適切なパラメータを使用して新しいメタデータ アプリケーションを作成する例を示します。

```
Device(config)# metadata application-params app1
Device(config-md-app-entry)# name instant-messaging-audio
Device(config-md-app-entry)# identifier 243
Device(config-md-app-entry)# description instant messaging audio recordings
```

次の **show metadata application table** コマンドの出力は、特定のエンドポイントで設定されたすべてのメタデータ アプリケーションの名前と ID を表示しています。

```
Device# show metadata application table

ID     Name                  Vendor                Vendor id
-------------------------------------------------------------------------------
113    telepresence-media    -                     -
114    telepresence-contr$   -                     -
478    telepresence-data     -                     -
414    webex-meeting         -                     -
56     citrix                -                     -
81     cisco-phone           -                     -
472    vmware-view           -                     -
473    wyze-zero-client      -                     -
61     rtp                   -                     -
64     h323                  -                     -
5060   sip                   -                     -
554    rtsp                  -                     -
496    jabber                -                     -
5222   xmpp-client           -                     -
```

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 *17 : show metadata application table* のフィールドの説明

フィールド	説明
ID	アプリケーションID。内部的にアプリケーション名にマッピングされます。
[名前（Name）]	アプリケーションの名前。

関連コマンド

コマンド	説明
debug metadata	メタデータ フローのデバッグを有効にします。
default	指定されたアプリケーションの名前、説明、および ID のデフォルト プロパティを表示します。
description	アプリケーションの説明を表示します。
identifier	アプリケーション ID を表示します。

コマンド	説明
name	アプリケーションの名前を表示します。
show metadata application table	デバイスに定義されているメタデータ アプリケーションのリストを表示します。
show metadata flow	メタデータ フロー情報を表示します。
name	アプリケーションの名前を表示します。

metadata flow

すべてのインターフェイスまたは特定のインターフェイスでメタデータを有効にするには、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 **metadata flow** コマンドを使用します。メタデ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。

metadata flow
no metadata flow

構文の説明

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

メタデータはインターフェイスで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）

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	変更箇所
15.2(1)T	このコマンドが導入されました。
Cisco IOS XE リリース 3.7S	このコマンドが、Cisco IOS XE Release 3.7S に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

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 **metadata flow** コマンドを使用した場合は、デバイス レベルでメタデータが有効になります。つまり、デバイスに設定されているすべてのインターフェイスで、メタデータが有効になります。インターフェイス コンフィギュレーション モードで **metadata flow** コマンドを使用した場合は、指定されたインターフェイスでのみメタデータが有効になります。インターフェイス コンフィギュレーション モードで **no metadata flow** コマンドを使用することで、1 つのインターフェイスでメタデータを無効にできます。ただし、他のインターフェイスから入ってくるメタデータ フローは、メタデータが無効になっているインターフェイスを通過できません。このような場合には、フローテーブルへの入力が行われず、分類が正常に完了しません。インターフェイスでメタデータを明示的に有効または無効にすると、Nonvolatile Generation（NVGEN）メソッドを使用して設定の詳細情報が取得され、設定に表示されます。

（注） Cisco IOS Release 15 .3(1)T からは、グローバル コンフィギュレーション モードで **no metadata flow** コマンドが設定されると、Nonvolatile Generation（NVGEN）メソッドを使用して設定の詳細情報が取得され、デバイスの実行コンフィギュレーションに表示されます。

例

次に、デバイス レベルでメタデータを有効にする例を示します。

```
Device(config)# metadata flow
```

次に、インターフェイスごとのレベルでメタデータを有効にする例を示します。

```
Device(config)# interface gigabitethernet 0/0
Device(config-if)# metadata flow
```

関連コマンド

コマンド	説明
metadata flow (troubleshooting)	メタデータ フローのテストとトラブルシューティングのためのフロー エントリを作成します。

metadata flow (troubleshooting)

メタデータのテストとトラブルシューティングのためにフローの作成をシミュレートするには、グローバル コンフィギュレーション モードで **metadata flow** コマンドを使用します。テストとトラブルシューティングのために作成されたフローを削除するには、このコマンドの **no** 形式を使用します。

Cisco IOS Release 15.1(1)SY 以降

metadata flow
no metadata flow

Cisco IOS Release 15.1(1)SY よりも前のリリース

metadata flow [{**entry** *entry-name*| **flow-specifier** *flow-specifier-name*| **session-params** *session-name*}]

no metadata flow [{**entry** *entry-name*| **flow-specifier** *flow-specifier-name*| **session-params** *session-name*}]

構文の説明

entry *entry-name*	指定した名前でフローエントリを作成します。
flow-specifier *flow-specifier-name*	送信元と宛先の情報を設定します。
session-params *session-name*	フローのセッションパラメータを設定します。

コマンド デフォルト

静的メタデータ フロー エントリは作成されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
15.2(1)T	このコマンドが導入されました。
15.1(1)SY	コマンドが変更されました。 **entry** *entry-name*、**flow-specifier** *flow-specifier-name*、および **session-params** *session-name* のキーワードおよび引数のペアが削除されました。

使用上のガイドライン

テストまたはトラブルシューティングの目的で仮想エンドポイントで構成される環境をシミュレートする必要がある場合は、関連付けられたキーワードとともに **metadata flow** コマンドを使用できます。

metadata flow entry *entry-name* コマンドを使用して、フローを作成します。正常なフローを作成するには、フロー指定子とセッション パラメータを指定します。

flow-specifier*flow-specifier-name* キーワードおよび引数のペアを使用することで、フロー指定子が作成され、デバイスがメタデータ コンフィギュレーション フロー指定子モードになります。

メタデータ コンフィギュレーション フロー指定子モードで次のコマンドを使用して、フローのフロー タプルを設定します。

- **dest-ip** *ip-address* **dest-port** *port-number*：エンドポイントの宛先 IPv4 アドレスと宛先ポート番号を指定します。
- **source-ip** *ip-address* **source-port** *port-number*：エンドポイントの送信元 IPv4 アドレスと送信元ポート番号を指定します。

session-params*session-name* キーワードおよび引数のペアを使用することで、メタデータ セッション パラメータ コンフィギュレーション モードでコマンドが実行されます。メタデータ セッション パラメータ コンフィギュレーション モードで次の関連コマンドを使用して、フローのセッション パラメータを設定します。

- **application name** *application-name*：指定されたアプリケーション名をセッションに関連付けます。

entry*entry-name* キーワードおよび引数のペアを使用することで、メタデータ エントリ コンフィギュレーション モードでコマンドが実行されます。メタデータ エントリ コンフィギュレーション モードで、以前に定義したフロー指定子を持つ **flow-specifier** キーワードと、以前に定義したセッション パラメータ名を持つ **session-params** キーワードを使用して、指定されたフロー エントリと関連付けます。

（注） Cisco IOS Release 15 .3(1)T からは、グローバル コンフィギュレーション モードで **no metadata flow** コマンドが設定されると、Nonvolatile Generation（NVGEN）メソッドを使用して設定の詳細情報が取得され、デバイスの実行コンフィギュレーションに表示されます。

例

次に、フロー エントリ、フロー指定子、およびセッション パラメータを作成し、フロー指定子とセッション パラメータをフロー エントリに関連付ける例を示します。

次に、フロー エントリを作成する設定を示します。

```
Device(config)# metadata flow entry e1
```

次に、送信元 IP アドレス、宛先 IP アドレス、および送信元と宛先のポート番号を使用して、フロー指定子を作成する例を示します。

```
Device(config)# metadata flow flow-specifier flow1
Device(config-md-flowspec)# source 209.165.201.3 source-port 1000
Device(config-md-flowspec)# destination 209.165.201.20 dest-port 1000
```

次に、セッション パラメータと、関連付けられたパラメータを作成する例を示します。

```
Device(config)# metadata flow session-params session1
Device(config-md-session-params)# application name webex-meeting
```

次に、フロー指定子とセッションパラメータをフローエントリに関連付ける例を示します。

```
Device(config)# metadata flow entry e1
Device(config-md-entry)# flow-specifier flow1
Device(config-md-entry)# session-params session1
```

関連コマンド

コマンド	説明
debug metadata	メタデータ フローのデバッグを有効にします。
show metadata application table	デバイスに定義されているメタデータ アプリケーションのリストを表示します。
show metadata flow	メタデータ フロー情報を表示します。

mls ip pbr

ポリシー ルーティング パケットのマルチレイヤ スイッチング（MLS）サポートを有効にするには、グローバル コンフィギュレーション モードで **mlsippbr** コマンドを使用します。ポリシー ルーティング パケットの MLS サポートを無効にするには、このコマンドの **no** 形式を使用します。

mls ip pbr [null0]
no mls ip pbr

構文の説明

null0	（任意）ルートマップのインターフェイス null0 へのハードウェア サポートを有効にします。

コマンド デフォルト

ポリシー ルーティング パケットへの MLS サポートはディセーブルです。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 で実装され、Cisco IOS Release 12.2(17d)SXB に導入されました。
12.2(18)SXE	このコマンドが、**null0** キーワードをサポートするように変更されました。
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。

使用上のガイドライン

このコマンドは、Supervisor Engine 720 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

（注） 同じインターフェイス上でポリシー ベース ルーティング（PBR）と SLB をイネーブルにしないでください。PBR ベースのパケットが正しく転送されなくなります。

mlsippbr コマンドを入力してハードウェア ポリシー ルーティングを有効にすると、ハードウェアですべてのポリシー ルーティングが行われ、ポリシー ルーティングにどのインターフェイスが設定されているかに関係なく、すべてのインターフェイスに適用されます。

ルートマップで **setinterfacenull0** 用のハードウェア サポートを有効にするためにのみトラフィックをルーティングしている場合は、**null0** キーワードを使用します。

例

次に、ポリシー ルーティング パケットの MLS サポートをイネーブルにする例を示します。

```
Router(config)#
mls ip pbr
```

関連コマンド

コマンド	説明
showtcaminterfacevlanacl	インターフェイスベースのTCAMに関する情報を表示します。

mls qos（グローバル コンフィギュレーション モード）から mpls experimental

- mls qos（グローバル コンフィギュレーション モード） （751 ページ）
- mls qos（インターフェイス コンフィギュレーション モード） （753 ページ）
- mls qos 10g-only （754 ページ）
- mls qos aggregate-policer （756 ページ）
- mls qos bridged （760 ページ）
- mls qos channel-consistency （761 ページ）
- mls qos cos （762 ページ）
- mls qos cos-mutation （765 ページ）
- mls qos dscp-mutation （766 ページ）
- mls qos exp-mutation （767 ページ）
- mls qos loopback （768 ページ）
- mls qos map （769 ページ）
- mls qos map cos-dscp （772 ページ）
- mls qos map cos-mutation （774 ページ）
- mls qos map dscp-cos （776 ページ）
- mls qos map dscp-exp （778 ページ）
- mls qos map dscp-mutation （780 ページ）
- mls qos map exp-dscp （782 ページ）
- mls qos map exp-mutation （784 ページ）
- mls qos map ip-prec-dscp （786 ページ）
- mls qos map policed-dscp （788 ページ）
- mls qos marking ignore port-trust （790 ページ）
- mls qos marking statistics （791 ページ）
- mls qos mpls trust experimental （792 ページ）
- mls qos police redirected （794 ページ）
- mls qos police serial （795 ページ）
- mls qos protocol （796 ページ）

- mls qos queueing-only （799 ページ）
- mls qos queue-mode mode-dscp （801 ページ）
- mls qos rewrite ip dscp （802 ページ）
- mls qos statistics-export（グローバル コンフィギュレーション） （804 ページ）
- mls qos statistics-export（インターフェイス コンフィギュレーション） （806 ページ）
- mls qos statistics-export aggregate-policer （808 ページ）
- mls qos statistics-export class-map （810 ページ）
- mls qos statistics-export delimiter （813 ページ）
- mls qos statistics-export destination （814 ページ）
- mls qos statistics-export interval （817 ページ）
- mls qos supervisor 10g-only （819 ページ）
- mls qos trust （821 ページ）
- mls qos trust extend （824 ページ）
- mls qos tunnel gre input uniform-mode （826 ページ）
- mls qos vlan-based （827 ページ）
- monitor pids （829 ページ）
- mpls experimental （830 ページ）

mls qos（グローバル コンフィギュレーション モード）

グローバルに Quality of Service（QoS）機能を有効にするには、グローバル コンフィギュレーション モードで **mlsqos** コマンドを使用します。QoS 機能をグローバルに無効にするには、このコマンドの **no** 形式を使用します。

mls qos
no mls qos

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

QoS はグローバルにディセーブルです。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

QoS がグローバルにイネーブルの場合は、QoS がディセーブル化されているインターフェイスを除いて、すべてのインターフェイスで QoS がイネーブルになります。QoS がグローバルにディセーブルの場合は、すべてのトラフィックが QoS パススルー モードで渡されます。

ポートキューイング モードでは、ポリシー フィーチャ カード（PFC）QoS（マーキングおよびポリシング）は無効になっており、PFC によってパケットのタイプ オブ サービス（ToS）とサービス クラス（CoS）は変更されません。受信および送信に関するすべてのキューイングは、着信パケットの QoS タグに基づいて行われます。この QoS タグは、着信 CoS に基づきます。

802.1Q または Inter-Switch Link（ISL）カプセル化ポート リンクでは、キューイングはパケット 802.1Q または ISL CoS に基づいて行われます。

ルータのメイン インターフェイスまたはアクセス ポートでは、キューイングは設定されたポート単位の CoS（デフォルト CoS は 0）に基づいて行われます。

このコマンドは、オフ状態のすべてのインターフェイス上で Ternary Content Addressable Memory（TCAM）QoS を有効または無効にできます。

例

次に、QoS をグローバルにイネーブルにする例を示します。

```
Router(config)# mls qos
Router(config)#
```

次に、Cisco 7600 シリーズ ルータで QoS をグローバルに無効にする例を示します。

```
Router(config)# no mls qos
Router(config)#
```

関連コマンド

コマンド	説明
mlsqos(interfaceconfigurationmode)	インターフェイスでのQoS機能をイネーブルにします。
showmlsqos	MLS QoS 情報を表示します。

mlsqos（インターフェイスコンフィギュレーションモード）

インターフェイスで Quality of Service（QoS）機能を有効にするには、インターフェイス コンフィギュレーション コマンド モードで **mlsqos** コマンドを使用します。インターフェイスで QoS 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。

mls qos
no mls qos

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

有効

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
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。

使用上のガイドライン

このコマンドは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータでは廃止されています。

CLI を使用すると、OC-12 ATM OSM の WAN ポートおよびチャネライズド OSM の WAN ポートに PFC ベースの QoS を設定できますが、PFC ベースの QoS はこれらの OSM の WAN ポートではサポートされていません。

QoS をグローバルにディセーブルにすると、すべてのインターフェイスでディセーブルになります。

このコマンドは、インターフェイスの TCAM QoS（分類、マーキング、およびポリシング）をイネーブルまたはディセーブルにします。

例

次に、インターフェイス上で QoS をイネーブルにする例を示します。

```
Router(config-if)# mls qos
```

関連コマンド

コマンド	説明
mlsqos(globalconfigurationmode)	QoS機能をグローバルにイネーブルにします。
showmlsqos	MLS QoS 情報を表示します。

mls qos 10g-only

スーパバイザ エンジンの 10 ギガビット イーサネット アップリンク ポートのみが使用される 10g-only モードで Quality of Service（QoS）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 **mls qos 10g-only** コマンドを使用します。1 ギガビット イーサネット ポートを含むすべてのアップリンク ポートを使用できるようにするには、このコマンドの **no** 形式を使用します。

mls qos 10g-only
no mls qos 10g-only

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

スーパバイザ エンジンですべてのポートがアクティブです。

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	変更箇所
12.2(33)SXH	このコマンドが Supervisor Engine 720 -10GE に導入されました。
15.1(1)SY	このコマンドが変更されました。モードスイッチングの要件が変更されました。

使用上のガイドライン

mls qos 10g-only コマンドを入力すると、1 ギガビットおよび 10 ギガビット イーサネット アップリンク ポートの両方を備えたスーパバイザ エンジンが、10 ギガビット イーサネット ポートのパフォーマンスを向上させるために、インターフェイス キュー容量を再割り当てします。スーパバイザ エンジンの 1 ギガビット イーサネット ポートが使用されない 10g-only モードでのみ、再割り当てができます。通常モードでは、すべてのスーパバイザ エンジン ポートがアクティブな場合、キュー構造は受信時は 2q4t で、送信時は 1p3q4t です。10g-only モードでは、キュー構造は受信時は 8q4t で、送信時は 1p7q4t です。

（注） キューの詳細情報を表示するには、**show queueing interface** コマンドを使用します。

通常モードと 10g-only モードを切り替えると、アップリンク ポートの既存の QoS 設定が失われるため、QoS を再設定する必要があります。また、移行中にポートでのサービスが一時的に失われます。

mls qos 10g-only コマンドを入力する前に、1 ギガビット イーサネット ポートをシャットダウンする必要があります。ポートをシャットダウンしないと、モードの変更は行われません。

10g-only モードから通常モードに切り替える場合は、各 1 ギガビット イーサネット ポートに対して **no shutdown** コマンドを入力して、これらのポートでの QoS サービスを再開する必要があります。

CSCty37687 では、10g-only モードから通常モードに切り替えるときに、1 ギガビット スーパバイザ エンジン アップリンク ポートで信頼状態とデフォルトのサービス クラス（CoS）値を削除する必要があります。

10g-only モードでは、1 ギガビット イーサネット ポートは表示されますが、管理上のダウン状態になります。

mls qos 10g-only コマンドはアクティブ スーパバイザとスタンバイ スーパバイザにのみ影響しますが、スーパバイザが 4 つある場合は、シャーシ内スタンバイ スーパバイザに適用する必要があります。

例

次に、スーパバイザ エンジンを 10g-only モードにする例を示します。

```
Router# configure terminal
Router(config)# mls qos 10g-only
```

関連コマンド

コマンド	説明
showmlsqosinterface	QoS 情報を表示します。
show queueing interface	インターフェイスのキューイングの統計情報を表示します。

mls qos aggregate-policer

ポリシー マップで使用する名前付き集約ポリサーを定義するには、グローバル コンフィギュレーションモードで**mlsqosaggregate-policer**コマンドを使用します。名前付き集約ポリサーを削除するには、このコマンドの **no** 形式を使用します。

mls qos aggregate-policer *name rate-bps* [**normal-burst-bytes** [{**maximum-burst-bytes**|**pir peak-rate-bps**|**action-type action**}]]
no mls qos aggregate-policer *name*

構文の説明

name	集約ポリサーの名前です。命名規則については、「使用上のガイドライン」を参照してください。
rate-bps	1 秒あたりの最大ビット数です。範囲は 32000 ～ 10000000000 です。
normal-burst-bytes	（任意）通常バーストのバイト数です。範囲は 1000 ～ 31250000 です。
maximum-burst-bytes	（任意）最大バーストのバイト数です。範囲は 1000 ～ 31250000 です（入力する場合は、normal-burst-bytes と等しい値に設定する必要があります）。
pir peak-rate-bps	（任意）最大情報レート（PIR）を設定するキーワードおよび引数です。範囲は 32000 ～ 10000000000 です。デフォルトは標準の（**cir**）レートと同じです。

action-type action	（任意）アクション タイプ キーワードです。複数のアクションを同時に設定するために、このコマンドには、複数のアクション タイプと、対応するアクションを含めることができます。有効な値は次のとおりです。
	• **conform-action**：レートを超えない場合に実行するアクションを指定するキーワードです。有効なアクションは次のとおりです。
	  • **drop**：パケットをドロップします。
	  • **set-dscp-transmit***value*：DSCP 値を設定し、パケットを送信します。有効なエントリは、0 ～ 63（差別化コード ポイント値）、af11 ～ af43（指定された AF DSCP とパケットを照合）、cs1 ～ cs7（指定された CS DSCP とパケットを照合）、default、または ef（EF DSCP とパケットを照合）です。
	  • **set-mpls-exp-imposition-transmit***number*：タグ インポジションでの Experimental（exp）ビットを設定します。有効な範囲は 0 ～ 7 です。
	  • **set-prec-transmit**：パケットの優先順位を書き換えて、パケットを送信します。
	  • **transmit**：パケットを送信します。これがデフォルトです。
	• **exceed-action**：QoS 値を超える場合に実行するアクションを指定するキーワードです。有効なアクションは次のとおりです。
	  • **drop**：パケットをドロップします。これがデフォルトです。
	  • **policed-dscp-transmit**：ポリシング済み DSCP マップに応じて DSCP 値を変更し、パケットを送信します。
	  • **transmit**：パケットを送信します。
	• **violate-action**：QoS 値に違反する場合に実行するアクションを指定するキーワードです。有効なアクションは次のとおりです。
	  • **drop**：パケットをドロップします。
	  • **policed-dscp-transmit**：ポリシング済み DSCP マップに応じて DSCP 値を変更し、パケットを送信します。
	  • **transmit**：パケットを送信します。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- **conform-action** は **transmit**
- **exceed-action** は **drop**
- **violate-action** は exceed-action と同じです。 **exceed-action**
- **pir** *peak-rate-bps* は標準の（**cir**）レートと同じです。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドが Supervisor Engine 720 に導入されました。
12.2(17d)SXB	このコマンドが、Cisco IOS Release 12.2(17d)SXB に統合されました。
12.3	このコマンドが、Cisco 6500 と Cisco 7600 に実装されました。
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。

使用上のガイドライン

このポリサーは、異なるポリシー マップ クラスおよび異なるインターフェイスで共有できます。Cisco 7600 シリーズ ルータでは、1023 までの集約規則および 1023 までのポリシング規則がサポートされます。

mlsqosaggregate-policer コマンドを使用すると、集約フローおよびその集約のポリシング ルールを設定できます。レートおよびバースト パラメータを入力すると、平均レートの範囲は 32 kbps ～ 10 Gbps（それぞれ 32000、10000000000 と入力）となり、バースト サイズの範囲は 1 KB（1000 と入力）～31.25 MB（31250000 と入力）となります。既存の集約レート制限エントリを変更すると、そのエントリが使用中の場合には、NVRAM および Cisco 7600 シリーズ ルータのエントリが変更されます。

（注） ハードウェア粒度のため、レート値が制限されます。そのため、設定したバースト値が使用されない場合があります。

既存のマイクロフローまたは集約レート制限を変更すると、使用中の場合には NVRAM および Cisco 7600 シリーズ ルータのエントリが変更されます。

集約ポリサー名を入力するときには、次の命名規則に従ってください。

- 最大 31 文字で、a ～ z、A ～ Z、0 ～ 9、ダッシュ文字（-）、アンダースコア（_）、ピリオド文字（.）を含むことができます。
- 英文字で始まり、すべてのタイプのすべての ACL で一意である必要があります。
- 大文字と小文字を区別します。
- 数字は使用できません。
- キーワードにしないようにします。避ける必要があるキーワードは、**all**、**default-action**、**map**、**help**、および **editbuffer.**

aggregate ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC2（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。**showmlsqosaggregatepolicer** コマンドを入力することで、DFC を装備したスイッチン

グ モジュール、PFC2、および PFC2 によりサポートされる DFC を装備していないスイッチング モジュールのそれぞれについて、集約ポリシングの統計情報を表示できます。

例

次の例では、QoS 集約ポリサーが最大 100000 ビット/秒および 10000 バイトの通常バースト サイズを許可し、これらのレートを超過しない場合には DSCP を 48 に設定し、これらのレートを超過した場合にはパケットをドロップするよう設定する方法を示します。

```
Router(config)# mls qos aggregate-policer micro-one 100000 10000 conform-action
set-dscp-transmit 48 exceed-action drop
```

関連コマンド

コマンド	説明
police（ポリシー マップ）	インターフェイス別のポリサーを作成して、それを使用するようにポリシー マップ クラスを設定します。
setipdscp(policy-mapconfiguration)	ToS バイトに IP DSCP を設定することにより、パケットにマーク付けします。
showmlsqosaggregatepolicer	MLS QoS の集約ポリサーに関する情報を表示します。

mls qos bridged

レイヤ 3 LAN インターフェイスでブリッジされたトラフィックのマイクロフロー ポリシ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 **mlsqosbridged** コマンドを使用します。ブリッジされたトラフィックのマイクロフローポリ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。

mls qos bridged
no mls qos bridged

構文の説明

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

無効

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

このコマンドをサポートするのは、SVI だけです。

Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータでは、ユーザ ポリシーが SVI にアタッチされている場合、IPv4 マルチキャスト パケットのマイクロフロー ポリシング用の SVI で、**mlsqosbridged** コマンドを有効にする必要があります。

例

次に、VLAN インターフェイスのブリッジド トラフィックに対してマイクロフローポリシングをイネーブルにする例を示します。

```
Router(config-if)# mls qos bridged
```

関連コマンド

コマンド	説明
showmlsqos	MLS QoS 情報を表示します。

mls qos channel-consistency

EtherChannel バンドリングに関する Quality of Service（QoS）ポート属性チェックを有効にするには、インターフェイス コンフィギュレーション モードで、**mlsqoschannel-consistency** コマンドを使用します。EtherChannel バンドリングに関する QoS ポート属性チェックを無効にするには、このコマンドの **no** 形式を使用します。

mls qos channel-consistency
no mls qos channel-consistency

構文の説明

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

有効

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

mlsqoschannel-consistency コマンドは、ポート チャネルでのみサポートされています。

例

次に、EtherChannel バンドリングに関する QoS ポート属性チェックをイネーブルにする例を示します。

```
Router(config-if)# mls qos channel-consistency
```

次に、EtherChannel バンドリングに関する QoS ポート属性チェックをディセーブルにする例を示します。

```
Router(config-if)# no mls qos channel-consistency
```

mls qos cos

ポートのデフォルト マルチレイヤ スイッチング（MLS）サービス クラス（CoS）値を定義する、またはポート上のすべての着信パケットにデフォルトCoS値を割り当てるには、インターフェイス コンフィギュレーション モードで **mlsqoscos** コマンドを使用します。デフォルトのCoS 設定に戻すには、このコマンドの no 形式を使用します。

Cisco 3660、3845、6500、7200、7400、および 7500 シリーズ ルータ
mls qos cos {*cos-value*|**override**}
no mls qos cos {*cos-value*|**override**}

Cisco 7600 シリーズ ルータ
mls qos cos *cos-value*
no mls qos cos *cos-value*

構文の説明

cos-value	デフォルト CoS 値をポートに割り当てます。ポートが CoS で信頼されていて、パケットがタグなしの場合、デフォルト CoS 値は、CoS/DSCP マップへのインデックスとして出力キューを 1 つ選択するために使用されます。指定できる CoS 範囲は 0 ～ 7 です。デフォルトは 0 です。
override	着信パケットの CoS を上書きし、ポートのデフォルト CoS 値をすべての着信パケットに適用します。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- ポートのデフォルト CoS 値（*cos-value*）は **0**
- CoS の上書きは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(6)EA2	このコマンドが導入されました。このコマンドで **switchportpriority** コマンドが置き換えられました。
12.2(14)SX	このコマンドのサポートが、Cisco 7600 シリーズ ルータに追加されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに実装されました。
12.2(17d)SXB	このコマンドが、Cisco 7600 シリーズ ルータに実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。

リリース	変更箇所
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
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。

使用上のガイドライン

Cisco 3660、3845、6500、7200、7400、および 7500 シリーズ ルータ

override キーワードを使用してポートを設定した場合は、そのポートに入るすべてのパケットにデフォルト CoS および Diffserv コード ポイント（DSCP）値を割り当てることができます。

特定のポートに届くすべての着信パケットに、他のポートからのパケットより高い、または低いプライオリティを与える場合には、**override** キーワードを使用します。以前に DSCP または CoS を信頼するようにポートを設定した場合でも、このコマンドはその信頼状態を上書きし、着信パケットの CoS 値はすべて、**mlsqoscos** コマンドで設定されたデフォルト CoS 値に変更されます。着信パケットがタグ付きの場合、パケットの CoS 値は入力ポートで修正されます。この値は、このポートのデフォルト CoS に変更されます。

設定を確認するには、**showmlsqosinterface** 特権 EXEC コマンドを使用します。

Cisco 7600 シリーズ ルータ

CoS 値は、物理 LAN ポートでのみ設定できます。

Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータでは、次の制限が適用されます。

- このコマンドは、Optical Service Module（OSM）上の WAN インターフェイスではサポートされていません。
- このコマンドは、4 ポート ギガビット イーサネット WAN ポートではサポートされていません。

例

Cisco 3660、3845、6500、7200、7400、および 7500 シリーズ ルータ

次に、デフォルト ポート CoS として 4 を割り当てる例を示します。

```
Router(config)# interface gigabitethernet
0/1
Router(config-if)# mls qos trust cos
Router(config-if)# mls qos cos 4
```

次に、ポートに入るすべてのパケットのデフォルト ポート CoS 値として 4 を割り当てる例を示します。

```
Router(config)# interface gigabitethernet
0/1
Router(config-if)# mls qos cos 4
Router(config-if)# mls qos cos override
```

Cisco 7600 シリーズ ルータ

次に、デフォルト QoS CoS 値を 6 に設定する例を示します。

```
Router(config)# interface gigabitethernet
0/1
Router(config-if)# mls qos cos 6
```

関連コマンド

コマンド	説明
mlsqosmap	CoS/DSCP マップまたは DSCP/CoS マップを定義します。
mlsqostrust	ポートの信頼状態を設定します。
showinterfacefax/yswitchport	スイッチ ポート インターフェイスを表示します。
showmlsqos	MLS QoS 情報を表示します。
showmlsqosinterface	QoS 情報を表示します。

mls qos cos-mutation

入力サービス クラス（CoS）変換マップをインターフェイスにアタッチするには、インターフェイス コンフィギュレーション モードで **mlsqoscos-mutation** コマンドを使用します。インターフェイスから入力 CoS 変換マップを削除するには、このコマンドの **no** 形式を使用します。

mls qos cos-mutation *cos-mutation-table-name*
no mls qos cos-mutation

構文の説明

cos-mutation-table-name	入力 CoS 変換テーブル名

コマンド デフォルト

入力 CoS 変換テーブルは定義されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(17b)SXA	このコマンドが Supervisor Engine 720 に導入されました。
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。

使用上のガイドライン

このコマンドは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

例

次に、入力 CoS 変換マップ（mutemap2）を付加する例を示します。

```
Router(config-if)# mls qos cos-mutation mutemap2
```

関連コマンド

コマンド	説明
mlsqosmapcos-mutation	パケットの CoS を新しい CoS 値にマッピングします。
showmlsqos	MLS QoS 情報を表示します。

mls qos dscp-mutation

出力 DiffServ コード ポイント（DSCP）変換マップをインターフェイスにアタッチするには、インターフェイス コンフィギュレーション モードで、**mlsqosdscp-mutation** コマンドを使用します。インターフェイスから出力 DSCP 変換マップを削除するには、このコマンドの **no** 形式を使用します。

mls qos dscp-mutation *dscp-mutation-table-name*
no mls qos dscp-mutation

構文の説明

dscp-mutation-table-name	出力 DSCP 変換テーブル名

コマンド デフォルト

テーブルは定義されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
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。

使用上のガイドライン

このコマンドは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

例

次に、出力 DSCP 変換マップ（mutemap1）を付加する例を示します。

```
Router(config-if)# mls qos dscp-mutation mutemap1
```

関連コマンド

コマンド	説明
mlsqosmapdscp-mutation	指定した DSCP 変換マップを定義します。
showmlsqos	MLS QoS 情報を表示します。

mls qos exp-mutation

インターフェイス コンフィギュレーション コマンド モードでインターフェイスに出力 EXP 変換マップをアタッチするには、**mlsqosexp-mutation** コマンドを使用します。インターフェイスから出力 EXP 変換マップを削除するには、このコマンドの **no** 形式を使用します。

mls qos exp-mutation *exp-mutation-table-name*
no mls qos exp-mutation

構文の説明

exp-mutation-table-name	出力 EXP 変換テーブル名

コマンド デフォルト

テーブルは定義されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(17a)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
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。

使用上のガイドライン

このコマンドをサポートするのは、PFC3BXL または PFC3B モードだけです。

このコマンドは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

例

次に、出力 EXP 変換マップ（mutemap2）を付加する例を示します。

```
Router(config-if)# mls qos exp-mutation mutemap2
Router(config-if)#
```

関連コマンド

コマンド	説明
mlsqosmapdscp-mutation	指定した DSCP 変換マップを定義します。
showmlsqosmpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos loopback

ループバック ケーブルを介したVLANのスイッチ仮想インターフェイス（SVI）フラッドからルータ ポートを削除するには、インターフェイス コンフィギュレーション モードで、**mlsqosloopback** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos loopback
no mls qos loopback

構文の説明

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

無効

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(17a)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

インターフェイスで **mlsqosloopback** が適用されると、パケットは宛先に転送されません。

mlsqosloopback コマンドを入力する前に、オプティカル サービス モジュール（OSM）インターフェイスの MAC アドレスを指定する必要があります。MAC アドレスは、PFC2 ハードウェア スイッチングに使用される LAN ルータの MAC アドレスとは異なるものを設定します。

例

次に、パケットをそのインターフェイスに対して転送しないようにする例を示します。

```
Router(config-if)# mls qos loopback
```

mls qos map

マルチレイヤ スイッチング（MLS）のサービス クラス（CoS）/Diffserv コード ポイント（DSCP）マップまたは DSCP/CoS マップを定義するには、グローバル コンフィギュレーション モードで **mlsqosmap** コマンドを使用します。デフォルト マップに戻すには、このコマンドの no 形式を使用します。

mls qos map {**cos-dscp** *dscp1...dscp8*|**dscp-cos** *dscp-list* **to** *cos*}
no mls qos map {**cos-dscp|dscp-cos**}

構文の説明

cos-dscp *dscp1...dscp8*	CoS/DSCP マップを定義します。 *dscp1...dscp8* には、CoS 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。連続する DSCP 値はそれぞれスペースで区切ります。 サポートされる DSCP 値は、0、8、10、16、18、24、26、32、34、40、46、48、および 56 です。
dscp-cos *dscp-list* **to** *cos*	DSCP/CoS マップを定義します。 *dscp-list* には、最大 13 個の DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。サポートされる DSCP 値は、0、8、10、16、18、24、26、32、34、40、46、48、および 56 です。 *cos* には、DSCP 値が対応する CoS 値を入力します。範囲：0 ～ 7。

コマンド デフォルト

次の表に、デフォルトの CoS/DSCP マップを示します。

表 *18* : デフォルトの *CoS/DSCP* マップ

CoSValue	0	1	2	3	4	5	6	7
DSCPValue	0	8	16	24	32	40	48	56

次の表に、デフォルトの DSCP/CoS マップを示します。

表 *19* : デフォルトの *DSCP/CoS* マップ

DSCPValues	0	8、10	16、18	24、26	32、34	40、46	48	56
CoSValue	0	1	2	3	4	5	6	7

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに実装されました。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
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。

使用上のガイドライン

すべての CoS/DSCP マップおよび DSCP/CoS マップは、グローバルに定義されます。すべてのマップをすべてのポートに適用します。

mlsqostrustcos コマンドを入力すると、デフォルトの CoS/DSCP マップが適用されます。

mlsqostrustdscp コマンドを入力すると、デフォルトの DSCP/CoS マップが適用されます。

デフォルトのマップを適用した後に引き続き **mlsqosmap** コマンドを入力して、CoS/DSCP または DSCP/CoS マップを定義できます。

mlsqostrustdscp コマンドが入力された場合に入力ポートに信頼できない DSCP 値を持つパケットが存在すると、パケット CoS 値は 0 に設定されます。

設定を確認するには、**showmlsqosmaps** 特権 EXEC コマンドを使用します。

例

次に、DSCP/CoS マップを定義する例を示します。DSCP 値 16、18、24、および 26 は、CoS 1 にマッピングされます。DSCP 値 0、8、および 10 は、CoS 0 にマッピングされます。

```
Router# configure terminal
Router(config)# mls qos map dscp-cos 16 18 24 26 to 1
Router(config)# mls qos map dscp-cos 0 8 10 to 0
```

次に、CoS/DSCP マップを定義する例を示します。CoS 値 0 ～ 7 は、DSCP 値 8、8、8、8、24、32、56、56 にマッピングされます。

```
R
outer# configure terminal
Router(config)# mls qos map cos-dscp 8 8 8 8 24 32 56 56
```

関連コマンド

コマンド	説明
mlsqoscos	デフォルトのポート CoS 値を定義するか、あるいはポートのすべての着信パケットにデフォルトの CoS 値を割り当てます。

コマンド	説明
mlsqostrust	ポートの信頼状態を設定します。
showmlsqosmaps	QoS のマッピング情報を表示します。

mls qos map cos-dscp

信頼されたインターフェイスに入力サービス クラス（CoS）/DiffServ コードポイント（DSCP）マップを定義するには、グローバル コンフィギュレーション モードで **mlsqosmapcos-dscp** コマンドを使用します。以前の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。

mls qos map cos-dscp *dscp1 ...dscp8*
no mls qos map cos-dscp

構文の説明

dscp1...dscp8	CoS/DSCP マップを定義します。 *dscp1...dscp8* には、CoS 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。連続する DSCP 値はそれぞれスペースで区切ります。 サポートされる DSCP 値は、0、8、10、16、18、24、26、32、34、40、46、48、および 56 です。

コマンド デフォルト

デフォルトの CoS/DSCP 設定を次の表に示します。

表 *20 :* デフォルトの *CoS/DSCP* マップ

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに実装されました。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

すべての CoS/DSCP マップおよび DSCP/CoS マップは、グローバルに定義されます。すべてのマップをすべてのポートに適用します。

mlsqostrustcos コマンドを入力すると、デフォルトの CoS/DSCP マップが適用されます。

mlsqostrustdscp コマンドを入力すると、デフォルトの DSCP/CoS マップが適用されます。

デフォルトのマップを適用した後に引き続き **mlsqosmap** コマンドを入力して、CoS/DSCP または DSCP/CoS マップを定義できます。

mlsqostrustdscp コマンドが入力された場合に入力ポートに信頼できない DSCP 値を持つパケットが存在すると、パケット CoS 値は 0 に設定されます。

設定を確認するには、**showmlsqosmaps** 特権 EXEC コマンドを使用します。

例

次に、CoS/DSCP マップを定義する例を示します。CoS 値 0 ～ 7 は、DSCP 値 8、8、8、8、24、32、56、56 にマッピングされます。

```
Router#
 configure terminal
Router(config)# mls qos map cos-dscp 8 8 8 8 24 32 56 56
```

関連コマンド

コマンド	説明
mlsqosmapdscp-cos	出力 DSCP/CoS マップを定義します。
mlsqosmapip-prec-dscp	信頼されたインターフェイスに入力 IP precedence/DSCP マップを定義します。
mlsqosmappoliced-dscp	ポリシング済み DSCP 値とマーキング済み DSCP 値のマップを設定します。
showmlsqosmaps	QoS マップ設定とランタイム バージョンに関する情報を表示します。

mls qos map cos-mutation

パケットの新しい CoS 値にサービス クラス（CoS）値をマッピングするには、グローバル コンフィギュレーションモードで**mlsqosmapcos-mutation** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します

mls qos map cos-mutation *name mutated-cos1 mutated-cos2 mutated-cos3 mutated-cos4 mutated-cos5 mutated-cos6 mutated-cos7 mutated-cos8*
no mls qos map cos-mutation 名前

構文の説明

名前	CoS マップ名
mutated-cos1 ...mutated-cos8	スペースで区切った、8 つの CoS 出力値。有効値は 0 ～ 7 です。詳細については、「使用上のガイドライン」を参照してください。

コマンド デフォルト

次の表に、CoS/CoS 変換マッピングが設定されていない場合のデフォルトの CoS/CoS 変換マッピングを示します。

表 *21 :* デフォルトの *CoS/CoS* マッピング

CoS-in	**01234567**
CoS-out	01234567

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(17b)SXA	このコマンドが Supervisor Engine 720 に導入されました。
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。

使用上のガイドライン

このコマンドは、Supervisor Engine 2 が搭載された Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータではサポートされません。

このコマンドは、次のモジュールが搭載された Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータでのみサポートされています。

- WS-X6704-10GE
- WS-X6724-SFP

- WS-X6748-GE-TX

CoS 変換は非 802.1Q トンネル ポートではサポートされません。

mlsqosmapcos-mutation コマンドを入力すると、変換された CoS 値は入力 CoS シーケンス番号にマッピングされます。たとえば、**mlsqosmapcos-mutation23456701** コマンドを入力すると、次のマップが設定されます。

CoS-in	0	1	2	3	4	5	6	7
CoS-out	2	3	4	5	6	7	0	1

8 つの CoS 値はスペースで区切ります。

マップをグローバル コンフィギュレーション モードで定義したあと、マップをポートに付加できます。

QoS がディセーブルにされていると、ポートは CoS 信頼モードおよび 802.1Q トンネリング モードになりません。ポートを CoS 信頼モードにし、ポートが 802.1Q トンネル ポートとして設定されれば、変更されます。

Release 12.2(17b)SXA 以降のリリースでは、802.1Q トンネル ポートでの入力 CoS 変換が、ポート グループ単位でのみサポートされています。

入力 CoS 変換コンフィギュレーションを失敗しないようにするには、すべてのメンバー ポートが入力 CoS 変換をサポートする EtherChannel だけを作成するか、またはどのメンバーも入力 CoS 変換をサポートしない EtherChannel だけを作成します。入力 CoS 変換のサポートと非サポートが混在するような EtherChannel を作成しないでください。

EtherChannel のメンバーであるポートに入力 CoS 変換を設定する場合、入力 CoS 変換はポートチャネル インターフェイスに適用されます。

入力 CoS 変換をポートチャネル インターフェイスに設定できます。

例

次に、CoS/CoS マップを定義する例を示します。

```
Router(config)# mls qos map cos-mutation test-map 1 2 3 4 5 6 7 1
```

関連コマンド

コマンド	説明
showmlsqosmaps	QoS マップ設定とランタイム バージョンに関する情報を表示します。

mls qos map dscp-cos

出力 DiffServ コード ポイント（DSCP）/サービス クラス（CoS）マップを定義するには、グローバル コンフィギュレーション モードで **mlsqosmapdscp-cos** コマンドを使用します。以前の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。

mls qos map dscp-cos *dscp-values* **to** *cos-values*
no mls qos map dscp-cos

構文の説明

dscp-values **to** *cos-values*	DSCP/CoS マップを定義します。 *dscp-list* には、最大 13 個の DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。サポートされる DSCP 値は、0、8、10、16、18、24、26、32、34、40、46、48、および 56 です。 *cos* には、DSCP 値が対応する CoS 値を入力します。範囲：0 ～ 7。

コマンド デフォルト

デフォルトの DSCP/CoS マップを次の表に示します。

表 *22:* デフォルトの *DSCP/CoS* マップ

DSCP	0 ～ 7	8 ～ 15	16 ～ 23	24 ～ 31	32 ～ 39	40 ～ 47	48 ～ 55	56 ～ 63
CoS	0	1	2	3	4	5	6	7

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに実装されました。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

DSCP/CoS マップは、最終 DSCP 分類を最終 CoS にマッピングする場合に使用します。この最終マップにより、パケットが割り当てられる出力キューおよびしきい値が決まります。CoS マップは、トランク インターフェイス上の送信済みパケットの Inter-Switch Link（ISL）ヘッダーまたは 802.1Q タグに書き込まれます。CoS マップには、64 個の DSCP 値およびこれに対応する CoS 値のテーブルが含まれます。Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータには、1 つのマップがあります。

すべての CoS/DSCP マップおよび DSCP/CoS マップは、グローバルに定義されます。すべてのマップをすべてのポートに適用します。

mlsqostrustcos コマンドを入力すると、デフォルトの CoS/DSCP マップが適用されます。

mlsqostrustdscp コマンドを入力すると、デフォルトの DSCP/CoS マップが適用されます。

デフォルトのマップを適用した後に引き続き **mlsqosmap** コマンドを入力して、CoS/DSCP または DSCP/CoS マップを定義できます。

mlsqostrustdscp コマンドが入力された場合に入力ポートに信頼できない DSCP 値を持つパケットが存在すると、パケット CoS 値は 0 に設定されます。

設定を確認するには、**showmlsqosmaps** 特権 EXEC コマンドを使用します。

例

次に、DSCP/CoS マップを定義する例を示します。DSCP 値 16、18、24、および 26 は、CoS 1 にマッピングされます。DSCP 値 0、8、および 10 は、CoS 0 にマッピングされます。

```
Router# configure terminal
Router(config)# mls qos map dscp-cos 16 18 24 26 to 1
Router(config)# mls qos map dscp-cos 0 8 10 to 0
```

関連コマンド

コマンド	説明
mlsqosmapcos-dscp	信頼されたインターフェイスに入力 CoS/DSCP マップを定義します。
showmlsqosmaps	QoS マップ設定とランタイム バージョンに関する情報を表示します。

mls qos map dscp-exp

最終 DiffServ コード ポイント（DSCP）値を最終 Experimental（EXP）値にマッピングするには、グローバル コンフィギュレーション モードで **mlsqosmapdscp-exp** コマンドを使用します。以前の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。

mls qos map dscp-exp *dscp-values* **to** *exp-values*
no mls qos map dscp-exp

構文の説明

dscp-values	DSCP 値です。有効値の範囲は 0 ～ 63 です。
to	マッピングを定義します。
exp-values	EXP 値。有効値は、0 ～ 7 です。

コマンド デフォルト

デフォルトの DSCP/EXP マップを次の表に示します。

表 *23 :* デフォルトの *DSCP/EXP* マップ

DSCP	**0 ～ 7**	**8 ～ 15**	**16 ～ 23**	**24 ～ 31**	**32 ～ 39**	**40 ～ 47**	**48 ～ 55**	**56 ～ 63**
EXP	0	1	2	3	4	5	6	7

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(17a)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	スーパーバイザ エンジン 2 上のこのコマンドのサポートが Release 12.2(17d)SXB に拡張されました。
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。

使用上のガイドライン

このコマンドをサポートするのは、PFC3BXL または PFC3B モードだけです。

DSCP/EXP マップは、最終 DSCP 値を最終 EXP 値にマッピングする場合に使用します。この最終マップにより、パケットが割り当てられる出力キューおよびしきい値が決まります。EXP マップには、64 個の DSCP 値およびこれに対応する EXP 値のテーブルが含まれます。Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータには、1 つのマップがあります。

スペースで区切ることにより最大 8 つの DSCP 値を入力できます。スペースで区切ることにより最大 8 つの EXP 値を入力できます。

例

次に、最終 DSCP 値を最終 EXP 値に設定する例を示します。

```
Router(config)# mls qos map dscp-exp 20 25 to 3
```

関連コマンド

コマンド	説明
showmlsqosmaps	QoS マップ設定とランタイム バージョンに関する情報を表示します。

mls qos map dscp-mutation

名前付き DiffServ コード ポイント（DSCP）変換マップを定義するには、グローバル コンフィギュレーション モードで **mlsqosmapdscp-mutation** コマンドを使用します。デフォルト マッピングに戻すには、このコマンドの **no** 形式を使用します。

mls qos map dscp-mutation *map-name input-dscp1* [*input-dscp2* [*input-dscp3* [**i** *nput-dscp4* [*input-dscp5* [*input-dscp6* [*input-dscp7* [*input-dscp8*]]]]]] **to** *output-dscp*
no mls qos map dscp-mutation *map-name*

構文の説明

map-name	DSCP 変換マップの名前です。
input-dscp#	内部 DSCP 値。有効値は 0～63 です。詳細については、「使用上のガイドライン」を参照してください。
to	マッピングを定義します。
output-dscp	出力 DSCP 値。有効値は 0～63 です。

コマンド デフォルト

output-dscp は *input-dscp* と同じです。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
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。

使用上のガイドライン

このコマンドは、Supervisor Engine 2 が搭載された Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータではサポートされません。

名前付き DSCP 変換マップを設定する場合、次のことに注意してください。

- 変換された DSCP 値にマッピングする入力 DSCP 値を、最大 8 つ入力できます。
- 複数のコマンドを入力して、追加の DSCP 値を変換された DSCP 値にマッピングできます。
- 変換された DSCP 値ごとに個別のコマンドを入力できます。

出力 DSCP 値として書き込まれる前に内部 DSCP 値を変換するために、15 個の出力 DSCP 変換マップを設定できます。ポリシー フィーチャ カード（PFC）QoS が対応する任意のインターフェイスに対して、出力 DSCP 変換マップをアタッチできます。

PFC QoS は、内部 DSCP 値から出力サービス クラス（CoS）値を取得します。出力 DSCP 変換を設定した場合は、PFC QoS は変換された DSCP 値から出力 CoS 値を取得しません。

例

ThisexampleshowshowtomapDSCP30tomutatedDSCPvalue8:

```
Router(config)# mls qos map dscp-mutation mutemap1 30 to 8
```

関連コマンド

コマンド	説明
showmlsqosmaps	QoSマップ設定とランタイムバージョンに関する情報を表示します。

mls qos map exp-dscp

内部 DiffServ コードポイント（DSCP）マップに入力 Experimental（EXP）値を定義するには、グローバル コンフィギュレーション モードで **mlsqosmapexp-dscp** コマンドを使用します。デフォルト マッピングに戻すには、このコマンドの **no** 形式を使用します。

mls qos map exp-dscp *dscp-values*
no mls qos map exp-dscp

構文の説明

dscp-values	内部 DSCP マップに入力 EXP 値を定義します。範囲：0 ～ 63。

コマンド デフォルト

デフォルトの EXP/DSCP マップを次の表に示します。

表 *24 :* デフォルトの *EXP/DSCP* マップ

EXP	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(17a)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

このコマンドをサポートするのは、PFC3BXL または PFC3B モードだけです。

これらのマップの DSCP とは、パケット DSCP ではなく内部 DSCP を意味します。

EXP/DSCP マップは、受信された EXP 値を内部 DSCP マップにマッピングする場合に使用します。この最終マップにより、パケットが割り当てられる出力キューおよびしきい値が決まります。EXP マップには、64 個の DSCP 値およびこれに対応する EXP 値のテーブルが含まれます。Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータには、1 つのマップがあります。

スペースで区切ることにより最大 8 つの DSCP 値を入力できます。

例

次に、受信された EXP を内部 DSCP 値に設定する例を示します。

```
Router(config)# mls qos map exp-dscp 20 25 30 31 32 32 33 34
```

関連コマンド

コマンド	説明
mlsqosmapexp-mutation	パケットの EXP を新しい EXP 値にマッピングします。
showmlsqosmpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos map exp-mutation

パケットの Experimental（EXP）値を新しい EXP 値にマッピングするには、グローバル コンフィギュレーション モードで **mlsqosmapexp-mutation** コマンドを使用します。デフォルト マッピングに戻すには、このコマンドの **no** 形式を使用します。

mls qos map exp-mutation *map-name mutated-exp1 mutated-exp2 mutated-exp3 mutated-exp4 mutated-exp5 mutated-exp6 mutated-exp7 mutated-exp8*
no mls qos map exp-mutation *map-name*

構文の説明

map-name	EXP 変換マップの名前です。
mutated-exp#	スペースで区切った、8 つの EXP 値です。有効値は 0 ～ 7 です。詳細については、「使用上のガイドライン」を参照してください。

コマンド デフォルト

次の表に、EXP/EXP 変換マッピングが設定されていない場合のデフォルトの EXP/EXP 変換マッピングを示します。

表 *25 :* デフォルトの *EXP/EXP* マップ

EXP-in	**01234567**
EXP-out	01234567

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(17a)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
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。

使用上のガイドライン

このコマンドは、Supervisor Engine 2 が搭載された Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータではサポートされません。

このコマンドをサポートするのは、PFC3BXL または PFC3B モードだけです。

mlsqosmapexp-mutation コマンドを入力すると、変換された EXP 値は EXP シーケンス番号にマッピングされます。たとえば、**mlsqosmapexp-mutation23456701** コマンドを入力すると、次の表に示されたマップが設定されます。

表 *26 : EXP* シーケンス値にマッピングされた変換された *EXP* 値

EXP-in	**01234567**
EXP-out	23456701

8 つの EXP 値はスペースで区切ります。

マップをグローバル コンフィギュレーション モードで定義したあと、マップをポートに付加できます。

入力 EXP 値として書き込まれる前に内部 EXP 値を変換するために、15 個の入力 EXP 変換マップを設定できます。ポリシー フィーチャ カード（PFC）Quality of Service（QoS）が対応する任意のインターフェイスに対して、入力 EXP 変換マップをアタッチできます。

PFC QoS は、内部 DiffServ コード ポイント（DSCP）値から出力 EXP 値を取得します。入力 EXP 変換を設定した場合は、PFC QoS は変換された EXP 値から入力 EXP 値を取得しません。

例

Thisexampleshowshowtomap次に、パケットの EXP 値を新しい EXP 値にマッピングする例を示します。**:**

```
Router(config)# mls qos map exp-mutation mutemap1 1 2 3 4 5 6 7 0
```

関連コマンド

コマンド	説明
mlsqosmapexp-dscp	内部 DSCP マップに入力 EXP 値を定義します。
showmlsqosmpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos map ip-prec-dscp

信頼されたインターフェイスの入力IPプレシデンス/DiffServコードポイント（DSCP）マップを定義するには、グローバル コンフィギュレーション モードで、**mlsqosmapip-prec-dscp** コマンドを使用します。以前の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。

mls qos map ip-prec-dscp *dscp-values*
no mls qos map ip-prec-dscp

構文の説明

dscp-values	IP プレシデンス値 0 ～ 7 に対応する DSCP 値。有効値は 0 ～ 63 です。

コマンド デフォルト

デフォルトの IP プレシデンス/DSCP 設定を次の表に示します。

表 *27 :* デフォルトの *IP* プレシデンス*/DSCP* マップ

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

mlsqosmapip-prec-dscp コマンドは、信頼されたインターフェイス（またはフロー）に着信した IP パケットの IP プレシデンスを、信頼タイプが trust-ipprec である DSCP にマッピングする場合に使用します。

スペースで区切ることにより最大 8 つの DSCP 値を入力できます。

このマップは、8 つの優先順位値（0 ～ 7）およびこれに対応する DSCP 値のテーブルです。Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータには、1 つのマップがあります。IP precedence 値は次のとおりです。

- network 7
- internet 6

- critical 5
- flash-override 4
- flash 3
- immediate 2
- priority 1
- routine 0

例

次に、信頼されたインターフェイスに入力 IP precedence/DSCP マッピングを設定する例を示します。

```
Router(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
```

関連コマンド

コマンド	説明
mlsqosmapcos-dscp	信頼されたインターフェイスに入力 CoS/DSCP マップを定義します。
mlsqosmapdscp-cos	出力 DSCP/CoS マップを定義します。
mlsqosmappoliced-dscp	ポリシング済み DSCP 値とマーキング済み DSCP 値のマップを設定します。
showmlsqosmaps	QoS マップ設定とランタイム バージョンに関する情報を表示します。

mls qos map policed-dscp

ポリシング済み DiffServ コード ポイント（DSCP）値とマークダウンされた DSCP 値のマッピ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、**mlsqosmappoliced-dscp** コマンドを使用します。以前の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。

mls qos map policed-dscp *dscp-list* **to** *policed-dscp*
no mls qos map policed-dscp

Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ
mls qos map policed-dscp {**normal-burst**|**max-burst**} *dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]] **to** *policed-dscp*
no mls qos map policed-dscp

構文の説明

normal-burst	**exceed-actionpoliced-dscp-transmit** キーワードによって使用されるマークダウンマップを設定します。
max-burst	**violate-actionpoliced-dscp-transmit** キーワードによって使用されるマークダウンマップを設定します。
dscp1	DSCP 値。範囲：0 ～ 63。
dscp2 ～ *dscp8*	（任意）DSCP 値です。範囲：0 ～ 63。
to	マッピングを定義します。
policed-dscp	ポリシング済み DSCP 値を指定します。有効値は、0 ～ 63 です。

コマンド デフォルト

マーキング済みの値は設定されていません。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

DSCP/ポリシング済みDSCPマップにより、不適合なフローに適用されるマーキング済みDSCP値が決定します。Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータには、1 つのマップがあります。

スペースで区切ることにより最大 8 つの DSCP 値を入力できます。

スペースで区切ることにより最大 8 つのポリシング済み DSCP 値を入力できます。

（注） シーケンス外パケットを避けるため、DSCP/ポリシング済み DSCP マップを設定して、マーキング済みパケットが適合トラフィックと同じキューに留まるようにします。

例

次の例では、複数の DSCP を単一のポリシング済み DSCP 値にマッピングする方法を示します。

```
Router(config)# mls qos map policed-dscp 20 25 43 to 4
```

関連コマンド

コマンド	説明
mlsqosmapcos-dscp	信頼されたインターフェイスに入力 CoS/DSCP マップを定義します。
mlsqosmapdscp-cos	出力 DSCP/CoS マップを定義します。
mlsqosmapin-prec-dscp	信頼されたインターフェイスに入力 IP precedence/DSCP マップを定義します。
showmlsqos	MLS QoS 情報を表示します。

mls qos marking ignore port-trust

インターフェイスが信頼されていてもパケットをマークするには、グローバル コンフィギュレーション モードで **mlsqosmarkingignoreport-trust** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos marking ignore port-trust
no mls qos marking ignore port-trust

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ポート信頼はイネーブルです。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(18)SXF5	このコマンドが導入されました。

使用上のガイドライン

インターフェイスが信頼されていてもパケットをマークするには、**mlsqosmarkingignoreport-trust** コマンドを使用します。

例

次に、インターフェイスが信頼されていてもパケットをマークする例を示します。

```
mls qos marking ignore port-trust
```

次に、ポート信頼を再度有効にする例を示します。

```
no mls qos marking ignore port-trust
```

関連コマンド

コマンド	説明
mlsqostrust	インターフェイスの信頼状態を設定します。

mls qos marking statistics

ポリサー トラフィック クラス ID の設定済みアクションへの割り当てを無効にするには、グローバル コンフィギュレーション モードで **mlsqosmarkingstatistics** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos marking statistics
no mls qos marking statistics

構文の説明

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

有効

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(17a)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(18)SXE	このコマンドが変更され、信頼状態を設定するポリシーの統計情報のコレクションが追加されました。
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。

使用上のガイドライン

このコマンドは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

ポリシーマップの統計情報を表示するには、**showpolicy-mapinterface** コマンドを使用します。

例

次に、ポリサー トラフィック クラス ID の設定済みアクションへの割り当てを無効にする例を示します。

```
Router(config)# mls qos marking statistics
```

次に、ポリサー トラフィック クラス ID の設定済みアクションへの割り当てを許可する例を示します。

```
Router(config)# no mls qos marking statistics
```

関連コマンド

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

mls qos mpls trust experimental

マルチプロトコル ラベル スイッチング（MPLS）パケットの信頼状態のみを設定するには、インターフェイス コンフィギュレーション モードで、**mlsqosmplstrustexperimental** コマンドを使用します。MPLS パケットの信頼状態を信頼不可に設定するには、このコマンドの **no** 形式を使用します。

mls qos mpls trust experimental
no mls qos mpls trust experimental

構文の説明

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

信頼状態がイネーブルである場合、デフォルトは次のとおりです。

- 信頼不可：パケットは 0 に、またはポリシーによってマークされます。
- trust-cos

信頼状態がディセーブルである場合、デフォルトは次のとおりです。

- trust-exp：ポートまたはポリシーの信頼状態は無視されます。
- パケットはポリシーによってマークされます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.2(18)SXF2	このコマンドが Supervisor Engine 720 に導入されました。

使用上のガイドライン

mlsqosmplstrustexperimental コマンドを入力して、サービス クラス（CoS）および出力キューイングの目的で（例：ポートまたはポリシーの信頼を適用するため）、MPLS パケットを他のレイヤ 2 パケットとして扱うことができます。すべての信頼されたケース（信頼 CoS/IP/DiffServ コード ポイント（DSCP））が、trust-cos として扱われます。

サービス クラス（CoS）：スイッチド ネットワークを通過するときに、イーサネット フレームのプライオリティを示す ISL ヘッダーまたは 802.1Q ヘッダーどちらかの 3 ビットのことです。802.1Q ヘッダーの CoS ビットは通常 802.1p ビットと呼ばれます。パケットがレイヤ 2 およびレイヤ 3 ドメインの両方を横断するときに QoS を維持するため、ToS 値と CoS 値は互いにマッピングすることができます。

例

次に、MPLS パケットの信頼状態を trust-cos に設定する例を示します。

```
Router(config-if)# mls qos mpls trust experimental
```

次に、MPLS パケットの信頼状態を信頼不可に設定する例を示します。

```
Router(config-if)# no mls qos mpls trust experimental
```

関連コマンド

コマンド	説明
showmlsqosmpls	ポリシーマップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos police redirected

アクセス コントロール リスト（ACL）リダイレクト パケットのポリシングをオンにするには、グローバル コンフィギュレーション モードで **mlsqospoliceredirected** コマンドを使用します。ACL リダイレクト パケットのポリシングをオフにするには、このコマンドの **no** 形式を使用します。

mls qos police redirected
no mls qos police redirected

構文の説明

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

有効

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(17b)SXA	このコマンドのサポートが Supervisor Engine 720 に追加されました。
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。

使用上のガイドライン

このコマンドは、PFC3BXL または PFC3B モードでのみサポートされています。Release 12.2(17b)SXA では、**showplatformearl-mode** コマンドを入力して PFC3 モードを表示します。

このコマンドは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

（QoS リダイレクト パケットを必要としない代わりに）NetFlow データ エクスポート（NDE）の精度を必要とする場合、**nomlsqospoliceredirected** コマンドを使用します。

例

次に、ACL リダイレクト パケットのポリシングをオンにする例を示します。

```
Router(config)# mls qos police redirected
```

次に、ACL リダイレクト パケットのポリシングをオフにする例を示します。

```
Router(config)# no mls qos police redirected
```

関連コマンド

コマンド	説明
showplatformearl-mode	プラットフォーム情報を表示します。

mls qos police serial

PFC3C または PFC3CXL で入出力ポリシング機能のシリアルモードを有効にするには、グローバル コンフィギュレーション モードで **mlsqospoliceserial** コマンドを使用します。ポリシングモードをパラレル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。

mls qos police serial
no mls qos police serial

構文の説明

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

このコマンドはデフォルトで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	変更箇所
12.2(33)SRB	このコマンドが導入されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

mlsqospoliceserial コマンドを使用して、PFC3C または PFC3CXL の入出力ポリサーが互いに独立して（シリアルモードで）動作するように設定することができます。通常、入出力のポリシング機能はパラレルモードで動作し、1 つのポリシング機能によるアクションが、他での対応するアクションを引き起こします。たとえば、出力ポリシング機能でパケットが破棄される場合、入力ポリシング機能でもパケットは数えられません。ただし、シリアルモードでは、片方のポリサーによるアクションにより、もう片方のポリサーでの対応するアクションが引き起こされません。

（注） このコマンドは、ポリサーを使用したマーキングには影響しません。

例

次に、PFC3C または PFC3CXL でシリアル ポリシング モードを有効にするコマンド例を示します。

```
Router(config)# mls qos police serial
```

mls qos protocol

ルーティング プロトコル パケット ポリシングを定義するには、グローバル コンフィギュレーション モードで mls qos protocol コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos protocol *protocol-name* {**pass-through**|**police** *rate* [*burst*]|**precedence** *value* [**police** *rate* [*burst*]]}
no mls qos protocol *protocol-name*

構文の説明

protocol-name	プロトコル名です。有効な値は次のとおりです。 • **arp** • **bfd-ctrl** • **bfd-echo** • **bgp** • **eigrp** • **glbp** • **igrp** • **isis** • **ldp** • **nd** • **ospf** • **rip** • **vrrp**
pass-through	パススルー モードを指定します。
police レート	ポリシングする最大の 1 秒あたりのビット数（bps）を指定します。有効な値は 32000 ～ 4000000000 です。
バースト	（任意）通常バーストのバイト数です。有効な値は 1000 ～ 31250000 です。
precedence *value*	書き換えるプロトコル パケットの IP プレシデンス値を指定します。有効な値は 0 ～ 7 です。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- *burst* は、1000 bps です。

- Quality of Service（QoS）が有効な場合、DiffServ コード ポイント（DSCP）値はゼロに書き換えられます。
- QoS がディセーブルの場合、ポートはパススルー モード（マーキングまたはポリシングなし）になります。

コマンド 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	変更箇所
12.2(17a)SX	このコマンドが Supervisor Engine 720 に導入されました。
12.2(17d)SXB	このコマンドが、ISIS プロトコルをサポートするように変更されました。
12.2(18)SXE	このコマンドが、Supervisor Engine 720 でのみ次のように変更されました。 • グローバル **mlsqosprotocol** QoS ポリシーのマーキングのサポートが追加されました。 • このコマンドのサポートが、Supervisor Engine 2 に導入されましたが、Address Resolution Protocol（ARP）、統合 Intermediate System-to-Intermediate System（ISIS）、または Enhanced Interior Gateway Routing Protocol（EIGRP）はサポートしていません。 • Neighbor Discovery Protocol パケットをサポートするために、**nd** キーワードが追加されました。 • **igrp** キーワードが削除されました。
12.2(18)SXF	このコマンドの **no** 形式が変更され、引数およびキーワードが削除されました。
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。
12.2(33)SRE1	このコマンドが変更されました。**bfd-ctrl**、**bfd-echo**、**glbp**、および **vrrp** 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、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータで ARP、ISIS、または EIGRP をサポートしていません。

police*rateburst* キーワードおよび引数を入力せずに、**precedence***value* キーワードおよび引数を入力した場合、信頼できないポートからのパケットのみがマークされます。

police*rate*, **pass-through**、または **precedence***value* キーワードおよび引数を入力すると、プロトコル パケットがインターフェイス単位のポリシー マップを回避するようにできます。

mlsqosprotocol コマンドにより、次のようにルーティング プロトコル パケット ポリシングを定義できます。

- **pass-through** モードを指定すると、DSCP 値は変更せず、ポリシングされません。

- **police***rate* を設定すると、DSCP 値は変更せず、ポリシングされます。
- **precedence***value* を指定すると、信頼できないポートからのパケットの DSCP 値は変更し、DSCP/CoS マップに基づくサービス クラス（CoS）値は変更し、トラフィックはポリシングされません。
- **precedence***value*and the **police***rate* を指定すると、DSCP 値は変更し、DSCP/CoS マップに基づく CoS 値は変更し、DSCP 値はポリシングされます。この場合、DSCP 値の変更は、ポートの信頼状態に基づきます。DSCP 値が変更されるのは、信頼できないポートからのパケットに対してだけです。
- **precedence***value* を入力しない場合、DSCP 値はマルチレイヤ スイッチング（MLS）QoS が有効であるかどうかに基づきます。詳細は、次のとおりです。
  - MLS QoS がイネーブルでポートが信頼できない場合、内部 DSCP 値は 0 に上書きされます。
  - MLS QoS がイネーブルでポートが信頼できる場合、着信 DSCP 値は維持されます。

パススルー モードを選択した場合、プロトコル パケットが完全にポリシングを避けるようにできます。ポリシングモードが選択された場合、指定された認定情報レート（CIR）が、すべての指定プロトコルのパケット（Cisco 7600 シリーズ ルータに着信または発信の両方）をポリシングするのに使用されるレートになります。

ARP ブロードキャストによりシステムを保護するには、**mlsqosprotocolarppolice***bps* コマンドを入力します。

例

次に、ルーティング プロトコル パケットのポリシングを定義する例を示します。

```
Router(config)# mls qos protocol arp police 43000
```

次に、ポリシングを完全に避けるようにする例を示します。

```
Router(config)# mls qos protocol arp pass-through
```

次に、プロトコル パケットの書き換え後の IP precedence 値を定義する例を示します。

```
Router(config)# mls qos protocol bgp precedence 4
```

次に、プロトコル パケットの書き換え後の IP-precedence 値を定義し、DSCP 値をポリシングする例を示します。

```
Router(config)# mls qos protocol bgp precedence 4 police 32000 1200
```

関連コマンド

コマンド	説明
showmlsqosprotocol	プロトコルパススルー情報を表示します。

mls qos queueing-only

ポートキューイング モードを有効にするには、グローバル コンフィギュレーション モードで **mlsqosqueueing-only** コマンドを使用します。ポートキューイング 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。

mls qos queueing-only
no mls qos queueing-only

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

Quality of Service（QoS）はグローバルに無効になっています。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

ポートキューイング モードでは、ポリシー フィーチャ カード（PFC）QoS（マーキングおよびポリシング）は無効になっており、PFC によってパケットのタイプ オブ サービス（ToS）とサービス クラス（CoS）は変更されません。受信および送信に関するすべてのキューイングは、着信パケットの QoS タグに基づいて行われます。この QoS タグは、着信 CoS に基づきます。

802.1Q または Inter-Switch Link（ISL）カプセル化ポート リンクでは、キューイングはパケット 802.1Q または ISL CoS に基づいて行われます。

ルータのメインインターフェイスまたはアクセス ポートでは、キューイングは設定されたポート単位の CoS（デフォルト CoS は 0）に基づいて行われます。

例

次に、ポートキューイング モードをグローバルにイネーブルにする例を示します。

```
Router(config)# mls qos queueing-only
```

次に、ポートキューイング モードをグローバルにディセーブルにする例を示します。

```
Router(config)# no mls qos queueing-only
```

関連コマンド

コマンド	説明
mlsqos(globalconfigurationmode)	QoS機能をグローバルにイネーブルにします。
showmlsqos	MLS QoS 情報を表示します。

mls qos queue-mode mode-dscp

インターフェイスのキューイング モードを DiffServ コード ポイント（DSCP）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、**mlsqosqueue-modemode-dscp** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos queue-mode mode-dscp
no mls qos queue-mode mode-dscp

構文の説明

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キューイング モードは、サービス クラス（CoS）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（config-if）

コマンド履歴

リリース	変更箇所
12.2(18)SXF5	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、10 ギガビット イーサネット ポートだけでサポートされます。

有効なレイヤ 3 DSCP を伝送するトラフィックを受信する場合にだけ、ポートを trust DSCP に設定する必要があります。

Release 12.2(18)SXF5 およびそれ以降では、DSCP ベースの入力キューとしきい値を WS-X6708-10GE ポートで有効にして、輻輳回避を提供します。

Release 12.2(18)SXF5 よりも前のリリースでは、入力ポート キューとしきい値はレイヤ 2 サービス クラス（CoS）のみを使用し、ポリシー フィーチャ カード（PFC）QoS は DSCP を信頼するように設定されたポートに入力ポート輻輳回避を実装しません。

信頼 DSCP ポートからのトラフィックの場合、ポリシー フィーチャ カード（PFC）QoS は、受信した DSCP 値を初期内部 DSCP 値として使用します。PFC QoS は、受信 DSCP を信頼するように設定された入力ポートのトラフィックをマークしません。

例

次の例は、インターフェイスでキューイング モードを DSCP に設定する方法を示しています。

```
mls qos queue-mode mode-dscp
```

関連コマンド

コマンド	説明
priority-queuequeue-limit	使用可能バッファ スペースをキューに割り当てます。
showmlsqos	MLS QoS 情報を表示します。

mls qos rewrite ip dscp

タイプ オブ サービス（ToS）から DiffServ コード ポイント（DSCP）への書き換えを有効にするには、グローバル コンフィギュレーション モードで、**mlsqosrewriteipdscp** コマンドを使用します。ToS から DSCP への書き換えを無効にするには、このコマンドの **no** 形式を使用します。

mls qos rewrite ip dscp [**slot** *slot1 slot2 slot3...*]
no mls qos rewrite ip dscp [**slot** *slot1 slot2 slot3...*]

構文の説明

slot *slot*	（任意）スロット番号を指定します。シャーシの有効なスロットを判断するには、mls qos rewrite ip dscp slot ? コマンドを使用します。

コマンド デフォルト

ToS から DSCP への書き換え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（config）

コマンド履歴

リリース	変更箇所
12.2(17a)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
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。
12.2(33)SRD3	このコマンドが変更されました。**slot***slot* キーワード/引数のペアが追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

ToS から DSCP への書き換えをディセーブルにして、QoS をグローバルにイネーブルした場合、次のようになります。

- 最終 ToS から DSCP への書き換えが無効になり、DSCP パケットはそのまま保持されます。
- ポリシングおよびマーキングは、QoS 設定に従って動作します。
- マークおよびマークダウンされたサービス クラス（CoS）がキューイングに使用されます。
- QoS ディセーブル モードでは、ToS および CoS はそのまま保持されます。

nomlsqosrewriteipdscp コマンドは、マルチプロトコル ラベル スイッチング（MPLS）とは非互換です。PFC3BXL または PFC3B がインポーズするラベルに正しい MPLS Experimental（EXP）値を割り当てられるように、デフォルトの **mlsqosrewriteipdscp** コマンドは、有効のままにする必要があります。この制限は、PFC3C または PFC3CXL の転送には適用されません。

mlsqosrewriteipdscpslot コマンドは、スーパバイザまたはDFCラインカードでのToSからDSCPへの書き換えを無効にするために使用できます。このコマンドは非 DFC ラインカード スロットでも受け入れられますが、そのスロットに DFC ラインカードが挿入されていない限り有効にはなりません。

非DFCラインカードに着信するパケットでの書き換えを無効にするには、スーパバイザ スロットでの書き換えを無効にします。これにより、システム上のすべての非 DFC ラインカードに着信するパケットでの書き換えが無効になることに注意してください。

例

次に、スロット 4 で ToS から DSCP への書き換えを有効にする例を示します。

```
Router(config)# mls qos rewrite ip dscp slot 4
```

次に、ポートキューイング モードをグローバルに無効にする例を示します。

```
Router(config)# no mls qos rewrite ip dscp
```

関連コマンド

コマンド	説明
mlsqos(globalconfigurationmode)	QoS機能をグローバルにイネーブルにします。
showmlsqos	MLS QoS 情報を表示します。

mls qos statistics-export（グローバル コンフィギュレーション）

Quality of Service（QoS）統計データのエクスポートをグローバルに有効にするには、グローバル コンフィギュレーション モードで **mlsqosstatistics-export** コマンドを使用します。QoS 統計データのエクスポートをグローバルに無効にするには、このコマンドの **no** 形式を使用します。

mls qos statistics-export
no mls qos statistics-export

構文の説明

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

無効

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

Cisco 7600 シリーズ ルータにデータ エクスポートを設定するには、データ エクスポートをグローバルに有効にする必要があります。

QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

QoS 統計データのエクスポートを正常に実行するには、エクスポートの宛先ホスト名または IP アドレス、および User Datagram Port（UDP）番号を設定する必要があります。

例

次に、データ エクスポートをグローバルにイネーブルにする例を示します。

```
Router(config)# mls qos statistics-export
```

次に、データ エクスポートをグローバルにディセーブルにする例を示します。

```
Router(config)# no mls qos statistics-export
```

関連コマンド

コマンド	説明
showmlsqosstatistics-exportinfo	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export（インターフェイス コンフィギュレーション）

ポート単位の Quality of Service（QoS）統計データのエクスポートを有効にするには、インターフェイス コンフィギュレーション モードで **mlsqosstatistics-export** コマンドを使用します。ポート単位の QoS 統計データのエクスポートを無効にするには、このコマンドの **no** 形式を使用します。

mls qos statistics-export
no mls qos statistics-export

構文の説明

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

無効

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

Cisco 7600 シリーズ ルータにデータ エクスポートを設定するには、ポートで、グローバルにデータ エクスポートを有効にする必要があります。

QoS 統計データのエクスポートを正常に実行するには、エクスポートの宛先ホスト名または IP アドレス、および User Datagram Port（UDP）番号を設定する必要があります。

QoS 統計データは、デリミタ区切りフィールドを使用してエクスポートされます。**mlsqosstatistics-exportdelimiter** コマンドを入力することで、デリミタを設定できます。

ポートの統計情報はエクスポートされますが、ポートの QoS 統計情報はエクスポートされません。データ エクスポートがイネーブルであるポートでは、次の情報がエクスポートされます。

- タイプ（1 はポート タイプを意味します）
- モジュール/ポート
- 着信パケット数（ハードウェアの累積カウンタ値）

- 着信バイト数（ハードウェアの累積カウンタ値）
- 発信パケット数（ハードウェアの累積カウンタ値）
- 発信バイト数（ハードウェアの累積カウンタ値）
- タイム スタンプ（1970 年 1 月 1 日 UTC を起点とする秒数）

たとえば、FastEthernet4/5 で QoS 統計データのエクスポートがイネーブルの場合、エクスポートされたレコードは次のようになります（この例では、デリミタは|（パイプ））。

```
|1|4/5|123|80|12500|6800|982361894|
```

例

次に、QoS 統計データ エクスポートをイネーブルにする例を示します。

```
Router(config-if)# mls qos statistics-export
```

次に、QoS 統計データ エクスポートをディセーブルにする例を示します。

```
Router(config-if)# no mls qos statistics-export
```

関連コマンド

コマンド	説明
mlsqosstatistics-exportdelimiter	QoS 統計データのエクスポート フィールドのデリミタを設定します。
showmlsqosstatistics-exportinfo	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export aggregate-policer

名前付き集約ポリサー上で Quality of Service（QoS）統計データのエクスポートを有効にするには、グローバル コンフィギュレーション モードで、**mlsqosstatistics-exportaggregate-policer** コマンドを使用します。名前付き集約ポリサー上で QoS 統計データのエクスポートを無効にするには、このコマンドの **no** 形式を使用します。

mls qos statistics-export aggregate-policer *policer-name*
no mls qos statistics-export aggregate-policer *policer-name*

構文の説明

policer-name	ポリサー名

コマンド デフォルト

共有集約ポリサーの場合はすべて無効です。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

QoS 統計データのエクスポートは、オプティカル サービス モジュール（OSM）インターフェイスではサポートされていません。

Cisco 7600 シリーズ ルータにデータ エクスポートを設定するには、共有集約ポリサーで、グローバルにデータ エクスポートを有効にする必要があります。

QoS 統計データは、デリミタ区切りフィールドを使用してエクスポートされます。**mlsqosstatistics-exportdelimiter** コマンドを入力することで、デリミタを設定できます。

データ エクスポートがイネーブルである共有集約ポリサーまたは名前付きポリサーごとに、統計データがポリサー単位、および EARL 単位でエクスポートされます。データ エクスポートがイネーブルである共有集約ポリサーまたは名前付きポリサーでは、次の情報がエクスポートされます。

- タイプ（3 は集約ポリサーのエクスポート タイプを意味します）
- 集約名
- 方向（着信または発信）
- Encoded Address Recognition Logic（EARL）識別情報

- 受け入れパケット数（ハードウェアの累積カウンタ値）
- 拒否標準レート パケット数（ハードウェアの累積カウンタ値）
- 拒否超過レート パケット数（ハードウェアの累積カウンタ値）
- タイム スタンプ（1970 年 1 月 1 日 UTC を起点とする秒数）

共有集約ポリサーがポリシーの両方の方向に付加されている場合、2つのレコードがエクスポートされます（各方向に 1 つずつ）。各レコードには、受け入れパケット、拒否標準レート パケット、および拒否超過レート パケットに関する同じカウンタ値が格納されます。

たとえば、次のように設定されているとします。

- 共有集約ポリサー「aggr_1」上で QoS 統計データのエクスポートが有効
- スロット 1 に装着されたスーパーバイザ エンジンに EARL が搭載
- スロット 3 に装着された分散型フォワーディング カード（DFC）に EARL が搭載

エクスポートされたレコードは、次のようになります（この例では、デリミタは|（パイプ））。

```
|3|agg_1|in|1|45543|2345|982361894|
|3|agg_1|in|3|45543|2345|982361894|
```

例

次に、共有集約ポリサー単位、または名前付きポリサー単位でデータ エクスポートを有効にする例を示します。

```
Router(config)# mls qos statistics-export aggregate-policer aggr1M
```

関連コマンド

コマンド	説明
mlsqosstatistics-exportdelimiter	QoS 統計データのエクスポート フィールドのデリミタを設定します。
showmlsqosstatistics-exportinfo	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export class-map

Quality of Service（QoS）統計データのエクスポートをクラス マップで有効にするには、グローバル コンフィギュレーション モードで **mlsqosstatistics-exportclass-map** コマンドを使用します。QoS 統計データのエクスポートをクラス マップで無効にするには、このコマンドの **no** 形式を使用します。

mls qos statistics-export class-map *classmap-name*
no mls qos statistics-export class-map *classmap-nam e*

構文の説明

classmap-name	クラス マップの名前。

コマンド デフォルト

無効

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

Cisco 7600 シリーズ ルータにデータ エクスポートを設定するには、クラス マップで、グローバルにデータ エクスポートを有効にする必要があります。

QoS 統計データは、デリミタ区切りフィールドを使用してエクスポートされます。**mlsqosstatistics-exportdelimiter** コマンドを入力することで、デリミタを設定できます。

データ エクスポートが有効であるクラス マップごとに、統計データがポリサー単位、およびインターフェイス単位でエクスポートされます。インターフェイスが物理インターフェイスの場合、次の情報がエクスポートされます。

- タイプ（4 はクラス マップ物理エクスポートを意味します）
- クラスマップ名
- 方向（着信または発信）
- モジュール/ポート
- 受け入れパケット数（ハードウェアの累積カウンタ値）

- 拒否標準レート パケット数（ハードウェアの累積カウンタ値）
- 拒否超過レート パケット数（ハードウェアの累積カウンタ値）
- タイム スタンプ（1970 年 1 月 1 日 UTC を起点とする秒数）

インターフェイスが Cisco 7600 シリーズ ルータ VLAN である場合は、次の情報がエクスポートされます。

- タイプ（5 はクラス マップ VLAN エクスポートを意味します）
- クラスマップ名
- 方向（着信または発信）
- Encoded Address Recognition Logic（EARL）識別情報（EARL が搭載されたスロット番号）
- VLAN 番号
- 受け入れパケット数（ハードウェアの累積カウンタ値）
- 拒否標準レート パケット数（ハードウェアの累積カウンタ値）
- 拒否超過レート パケット数（ハードウェアの累積カウンタ値）
- タイム スタンプ（1970 年 1 月 1 日 UTC を起点とする秒数）

インターフェイスが Cisco 7600 シリーズ ルータ ポート チャネルである場合は、次の情報がエクスポートされます。

- タイプ（6 はクラス マップ ポート チャネル エクスポートを意味します）
- クラスマップ名
- 方向（着信または発信）
- EARL 識別情報（EARL が搭載されたスロット番号）
- ポート チャネル番号
- 受け入れパケット数（ハードウェアの累積カウンタ値）
- 拒否標準レート パケット数（ハードウェアの累積カウンタ値）
- 拒否超過レート パケット数（ハードウェアの累積カウンタ値）
- タイム スタンプ（1970 年 1 月 1 日 UTC を起点とする秒数）

たとえば、次のように設定されているとします。

- クラス マップ「class_1」上で QoS 統計データ エクスポートが有効
- スロット 1 に装着されたスーパーバイザ エンジンに EARL が搭載
- スロット 3 に装着された分散型フォワーディング カード（DFC）に EARL が搭載
- ポリシー マップ「policy_1」内に Cisco 7600 シリーズ ルータがある

- policy_1 は、次のインターフェイスの入力方向に付加
  - FastEthernet4/5
  - VLAN 100
  - ポート チャネル 24

エクスポートされたレコードは、次のようになります（この例では、デリミタは|（パイプ））。

|4|class_1|in|4/5|45543|2345|2345|982361894|

|5|class_1|in|1|100|44000|3554|36678|982361894|

|5|class_1|in|3|100|30234|1575|1575|982361894|

例

次に、クラス マップの QoS 統計データ エクスポートをイネーブルにする例を示します。

```
Router(config)# mls qos statistics-export class-map class3
```

関連コマンド

コマンド	説明
mlsqosstatistics-exportdelimiter	QoS 統計データのエクスポート フィールドのデリミタを設定します。
showmlsqosstatistics-exportinfo	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export delimiter

Quality of Service（QoS）統計データのエクスポート フィールドのデリミタを設定するには、グローバル コンフィギュレーション モードで **mlsqosstatistics-exportdelimiter** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos statistics-export delimiter
no mls qos statistics-export delimiter

構文の説明

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

デフォルトのデリミタはパイプ記号（|）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	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

QoS 統計データのエクスポートは、Optical Service Module（OSM）インターフェイスではサポートされていません。

Cisco 7600 シリーズ ルータにデータ エクスポートを設定するには、データ エクスポートをグローバルに有効にする必要があります。

例

次に、QoS 統計データ エクスポート フィールドのデリミタ（カンマ）を設定し、設定を確認する例を示します。

```
Router(config)# mls qos statistics-export delimiter ,
```

関連コマンド

コマンド	説明
showmlsqosstatistics-exportinfo	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export destination

Quality of Service（QoS）統計データのエクスポートの宛先ホストと User Datagram Protocol（UDP）ポート番号を設定するには、グローバル コンフィギュレーション モードで **mlsqosstatistics-exportdestination** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos statistics-export destination {*host-namehost-ip-address*} {**port** *port-number*|**syslog**} [**facility** *facility-name*] [**severity** *severity-value*]

構文の説明

host-name	ホスト名。
host-ip-address	ホストの IP アドレス。
port *port-number*	UDP ポート番号を指定します。
syslog	Syslog ポートを指定します。
facility *facility-name*	（任意）エクスポートするファシリティタイプを指定します。有効値のリストについては、「使用上のガイドライン」を参照してください。
severity *severity-value*	（任意）エクスポートする重大度を指定します。有効値のリストについては、「使用上のガイドライン」を参照してください。

コマンド デフォルト

syslog を指定しないかぎり、デフォルトでは何も設定されません。**syslog** を指定した場合、デフォルトは次のとおりです。

- *port* は 514。
- *facility* は local6。
- *severity* は debug。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

QoS 統計データのエクスポートは、Optical Service Module（OSM）インターフェイスではサポートされていません。

有効な *facility* 値は次のとおりです。

- **authorization**：セキュリティ/認証メッセージ
- **cron**：クロック デーモン
- **daemon**：システム デーモン
- **kernel**：カーネル メッセージ
- **local0**：ローカル用 0
- **local1**：ローカル用 1
- **local2**：ローカル用 2
- **local3**：ローカル用 3
- **local4**：ローカル用 4
- **local5**：ローカル用 5
- **local6**：ローカル用 6
- **local7**：ローカル用 7
- **lpr**：ライン プリンタ サブシステム
- **mail**：メール システム
- **news**：ネットワーク ニュース サブシステム
- **syslog**：syslogd により内部で生成されるメッセージ
- **user**：ユーザレベル メッセージ
- **uucp**：UNIX 間コピー プログラム（UUCP）サブシステム

有効な *severity* レベルは次のとおりです。

- **alert**：即時対処が必要
- **critical**：クリティカルな状態
- **debug**：デバッグレベル メッセージ
- **emergency**：システムは使用不能
- **error**：エラー状態
- **informational**：情報
- **notice**：通常の状態だが、重要な状態
- **warning**：警告状態

例

次に、宛先ホスト アドレス、および UDP ポート番号として Syslog を指定する例を示します。

```
Router(config)# mls qos statistics-export destination 172.20.52.3 syslog
```

関連コマンド

コマンド	説明
showmlsqosstatistics-exportinfo	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export interval

ポートや集約ポリサーの Quality of Service（QoS）統計データの読み取り頻度およびエクスポート頻度を指定を指定するには、グローバル コンフィギュレーション モードで、**mlsqosstatistics-exportinterval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos statistics-export interval 間隔
no mls qos statistics-export interval

構文の説明

間隔	エクスポート時間。有効値は 30 ～ 65535 秒です。

コマンド デフォルト

300 秒

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

QoS 統計データのエクスポートは、Optical Service Module（OSM）インターフェイスではサポートされていません。

interval は、設定内のアクティビティによるカウンタ ラップアラウンドを防止できるように、十分短い値を設定する必要があります。

注意 QoS 統計のエクスポートは Cisco 7600 シリーズ ルータに大きな負荷をかけるため、間隔を小さくするときは注意が必要です。

例

次に、QoS 統計データ エクスポートのインターバルを設定する例を示します。

```
Router(config)# mls qos statistics-export interval 250
```

関連コマンド

コマンド	説明
showmlsqosstatistics-exportinfo	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos supervisor 10g-only

10GE アップリンク ポートでのみ QoS を実行するように Cisco 7600 RSP720-10GE 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、**mlsqossupervisor10g-only** コマンドを使用します。すべてのアップリンク ポート（10GE および 1GE）で QoS を実行するように RSP を再設定するには、このコマンドの no 形式を使用します。

mls qos supervisor 10g-only
no mls qos supervisor 10g-only

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドはデフォルトで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	変更箇所
12.2(33)SRC	このコマンドが Cisco 7600 シリーズ ルータに追加されました。

使用上のガイドライン

RSP720-10GE には、10GE アップリンク ポートと 1GE アップリンク ポートの両方があります。すべてのアップリンク ポート（混合モード）または 10GE ポートだけで QoS 機能を実行するように、RSP720-10GE を設定できます。QoS に使用できるキューの数は、使用されるモードによって異なります。

- 混合モード（10 GE ポートと 1 GE ポート）で QoS に使用できるキューは、デフォルトで 4 つだけです。

1GE ポートの固定モードの QoS ポート アーキテクチャ（Rx/Tx）は、**2q8t/1p3q8t** です。

- 10GE だけのモードで QoS に使用できるキューは、8 つです。

10 GE だけのモードの QoS ポート アーキテクチャ（Rx/Tx）は、次のとおりです。

- **8q8t/1p7q8t**（CoS）
- **16q8t/1p15q8t**（DSCP）
- **16q1t/1p15q1t**（VLAN）

混合モードの QoS と 10GE だけのモードを切り替えると、RSP720-10GE アップリンクで一時的にサービスが失われます。また、モードを切り替えると、アップリンク上の既存の QoS 設定が失われます。QoS を再度設定する必要があります。

10GE だけのモードから混合モードの QoS に切り替える場合は、3 つの 1GE ポートの QoS サービスを再開するために、ポートごとに **noshutdown** コマンドを発行する必要があります。

10 GE だけのモードでは、1 GE ポートは表示されますが、管理上のダウン状態になります。

（注） キューの詳細を取得するには、**showqueueinginterface** コマンドを使用します。

例

次に、10GE ポートのみで QoS を実行するように、RSP720-10GE を設定する例を示します。

```
Router(config)# mls qos supervisor 10g-only
The following ports will be shut to enable 10g-only mode:
Gix/1 Gix/2 Gix/3
```

次に、冗長設定（高可用性）で、冗長リンクが使用されていない場合でも、両方のスーパバイザで 1GE アップリンク ポートがシャットダウンされる例を示します。

```
Router(config)# mls qos supervisor 10g-only
The following ports will be shut to enable 10g-only mode:
Gi6/1 Gi6/2 Gi6/3 Gi5/1 Gi5/2 Gi5/3
```

関連コマンド

コマンド	説明
mlsqos(interfaceconfiguration)	インターフェイスのトラフィックに関する情報を表示します。

mls qos trust

Quality of Service（QoS）ポートの信頼状態を設定し、サービス クラス（CoS）値またはDiffServ コードポイント（DSCP）値を検査してトラフィックを分類するには、インターフェイス コンフィギュレーション モードで **mlsqostrust** コマンドを使用します。ポートを信頼しない状態に戻すには、このコマンドの **no** 形式を使用します。

mls qos trust [{**cos**|**device cisco-phone**|**dscp**|**ip-precedence**}]
no mls qos trust

構文の説明

cos	（任意）パケット CoS 値を持つ着信パケットを分類します。着信フレームの CoS ビットは信頼されます。内部 DSCP 値は CoS ビットから取得されます。ポート デフォルト CoS 値は、タグなしパケットに使用する必要があります。
devicecisco-phone	（任意）Cisco IP Phone がポートに接続されているかどうかを検出するように、Cisco Discovery Protocol（CDP）を設定します。 • CDP により Cisco IP Phone が検出された場合は、設定された **mlsqostrustdscp**、**mlsqostrustip-precedence**、または**mlsqostrustcos** インターフェイス コマンドが QoS により適用されます。 • CDP が Cisco IP Phone を検出しない場合、QoS は、設定されているデフォルト以外の信頼状態をすべて無視します。
dscp	（任意）パケット DSCP 値（8 ビットの service-type フィールドのうち最上位 6 ビット）を持つ着信パケットを分類します。着信パケットのタイプ オブ サービス（ToS）ビットには、DSCP 値が含まれます。非 IP パケットの場合、パケット CoS 値は 0 です。キーワードを入力しない場合は、**mlsqostrustdscp** とみなされます。
ip-precedence	（任意）着信パケットの ToS ビットに IP precedence 値が含まれることを指定します。内部 DSCP 値は IP-precedence ビットから取得されます。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- グローバル QoS がイネーブルの場合、ポートは信頼できない状態です。
- キーワードが指定されていない、またはグローバルQoSが無効の場合、デフォルトは**dscp** です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.1(6)EA2	このコマンドが導入されました。
12.2(14)SX	このコマンドが変更されました。このコマンドのサポートが、Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータに導入されました。
12.2(15)ZJ	このコマンドが、Cisco 2600 シリーズ ルータ、Cisco 3600 シリーズ ルータ、および Cisco 3700 シリーズ ルータのプラットフォームに実装されました。
12.2(17d)SXB	このコマンドが、Cisco 7600 シリーズ ルータに実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(33)SXI	このコマンドが変更されました。**devicecisco-phone** キーワードが追加されました。

使用上のガイドライン

QoS ドメインに入るパケットは、そのエッジで分類されます。パケットがエッジで分類されるため、QoS ドメイン内のスイッチ ポートを信頼状態に設定できます。ドメイン内ではスイッチごとにパケットを分類する必要はありません。インターフェイスの信頼状態を設定し、パケットのどのフィールドをトラフィックの分類に使用するかを指定するには、**mlsqostrust** コマンドを使用します。

ポートに信頼 DSCP または信頼 IP precedence が設定され、着信パケットが非 IP パケットの場合は、CoS/DSCP マップを使用して、CoS 値から対応する DSCP 値が導き出されます。CoS は、トランク ポートの場合はパケット CoS、非トランク ポートの場合はデフォルトのポート CoS となります。

DSCP が信頼されている場合、IP パケットの DSCP フィールドは変更されません。ただし、パケットの CoS 値を（DSCP/CoS マップに基づいて）変更することは可能です。

CoS が信頼されている場合、パケットの CoS フィールドは変更されませんが、IP パケットである場合には（CoS/DSCP マップに基づいて）DSCP を変更することはできます。

devicecisco-phone キーワードで実装されるシスコ デバイス検証機能による信頼境界は、Cisco IP Phone をサポートするように設定されたスイッチ ポートに電話以外のデバイスをユーザが接続した場合に、セキュリティ上の問題を防ぎます。スイッチおよび IP Phone に接続されたポートで、CDP をグローバルに有効にする必要があります。Cisco IP Phone が検出されない場合、QoS は設定されたデフォルト以外のトラストの設定を適用しないため、ハイ プライオリティ キューの誤使用を防ぐことができます。

DSCP または IP precedence の信頼設定を行うと、着信パケットの DSCP 値または IP precedence 値が信頼されます。IP Phone に接続するスイッチ ポートで **mlsqoscosoverride** インターフェイス コンフィギュレーション コマンドを設定すると、スイッチは着信音声およびデータ パケットの CoS を無効にし、デフォルトの CoS 値をそれらに割り当てます。

QoS ドメイン間境界の場合は、ポートを DSCP 信頼状態に設定し、DSCP 値が QoS ドメイン間で異なる場合は DSCP/DSCP 変換マップを適用することができます。

ポートの信頼状態を使用する分類（mls qos trust [**cos** | **dscp** | **ip-precedence**] など）とポリシーマップを使用する分類（**service-policyinput***policy-map-name* など）は、相互に排他的です。最後に行われた設定により、前の設定が上書きされます。

Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータで実行される **mlsqostrust** コマンドには、次の条件が適用されます。

- **Thecos** キーワードは、**pos** または **atm** インターフェイス タイプではサポートされていません。
- 信頼状態は、FlexWAN モジュールに適用されません。
- 信頼状態は、ギガビット イーサネット ポートを除く 1q4t LAN ポートに適用されません。
- 4 ポート ギガビット イーサネット WAN モジュールで **mlsqostrustcos** コマンドを入力した場合、着信キューの廃棄しきい値は実装されません。

（注） **setqos-group** コマンドを使用して、Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのレイヤ 2 WAN インターフェイスで信頼状態を設定します。

例

次に、インターフェイスの信頼状態を IP precedence に設定する例を示します。

```
Router(config-if)# mls qos trust ip-precedence
```

次に、ポートに接続された Cisco IP Phone を検出するように、CDP を設定する例を示します。

```
Router(config-if)# mls qos trust device cisco-phone
```

関連コマンド

コマンド	説明
mlsqoscos	デフォルトのポート CoS 値を定義するか、あるいはポートのすべての着信パケットにデフォルトの CoS 値を割り当てます。
mlsqosmap	CoS/DSCP マップまたは DSCP/CoS マップを定義します。
showmlsqosinterface	QoS 情報を表示します。

mls qos trust extend

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

mls qos trust extend [**cos** *value*]
no mls qos trust extend

構文の説明

cos *value*	（任意）PC からのパケットに設定するために使用されるサービス クラス（CoS）値を指定します。有効値は 0 ～ 7 です。

コマンド デフォルト

デフォルト設定は、次のとおりです。

- モードは untrusted です。
- **cos** *value* は 0 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

このコマンドは、WAN モジュールではサポートされません。

電話が信頼モードに設定されている場合、PC から着信したすべてのパケットはそのまま電話を経由して、Cisco 7600 シリーズ ルータに直接送信されます。電話が非信頼モードに設定されている場合、PC から着信したすべてのトラフィックは、所定の CoS 値に設定されてから、Cisco 7600 シリーズ ルータに送信されます。

mlsqostrustextend コマンドを入力するたびに、モードが変更されます。たとえば、モードが信頼に設定されている場合にコマンドを入力すると、モードは非信頼に変わります。現在の信頼モードを表示するには、**showqueueinginterface** コマンドを入力します。

例

次に、スイッチ ポートに接続された電話を信頼モードで設定する例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend
```

次に、モードを非信頼に変更して、CoS 値を 3 に設定する例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend cos 3
```

次に、設定をデフォルト モードに設定する例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# no mls qos trust extend
```

関連コマンド

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

mls qos tunnel gre input uniform-mode

入力パケットの元の Quality of Service（QoS）マーキングを、入力パケットの DiffServ コードポイント（DSCP）フィールドおよび Generic Routing Encapsulation（GRE）ヘッダーにコピーできるようにするには、インターフェイス コンフィギュレーション モードで、**mlsqostunnelgreinputuniform-mode** コマンドを使用します。コピー操作を無効にするには、このコマンドの **no** 形式を使用します。

mls qos tunnel gre input uniform-mode
no mls qos tunnel gre input uniform-mode

構文の説明

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

着信パケットまたは GRE ヘッダーに対して、マーキング操作は実行されません。

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	変更箇所
12.2(33)SXI	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、PFC3C モードまたは PFC3CXL モードでのみサポートされています。

showmlsqos コマンドを入力して、設定を確認します。

例

次に、入力パケットの元の QoS マーキングを、DSCP フィールドおよび GRE ヘッダーにコピーできるようにする例を示します。

```
Router(config-if)# mls qos tunnel gre input uniform-mode
```

関連コマンド

コマンド	説明
showmlsqos	MLS QoS 情報を表示します。

mls qos vlan-based

レイヤ 2 インターフェイスの VLAN 単位の Quality of Service（QoS）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 **mlsqosvlan-based** コマンドを使用します。レイヤ 2 インターフェイスの VLAN 単位の QoS を無効にするには、このコマンドの **no** 形式を使用します。

mls qos vlan-based
no mls qos vlan-based

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

無効

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

このコマンドは、スイッチポートおよびポートチャネルインターフェイスだけでサポートされます。

VLAN ベースのモードでは、レイヤ 2 インターフェイスに対応付けられたポリシー マップは無視され、QoS は対応する VLAN インターフェイスに対応付けられたポリシー マップによって機能します。

VLAN 単位の QoS は、レイヤ 2 インターフェイス上だけで設定できます。

（注） レイヤ 3 インターフェイスは常にインターフェイスベースのモードです。レイヤ 3 VLAN インターフェイスは常に VLAN ベースのモードです。

例

次の例では、レイヤ 2 インターフェイスの VLAN 単位の QoS をイネーブルにする方法を示します。

```
Router(config-if)# mls qos vlan-based
```

関連コマンド

コマンド	説明
mlsqosbridged	レイヤ 3 LAN インターフェイスでのブリッジされたトラフィックのマイクロフロー ポリシングを有効にします。
mlsqoscos	インターフェイスのデフォルト CoS 値を定義します。
showqueueinginterface	キューイング情報を表示します。

monitor pids

メディア配信インデックス（MDI）フローでモニタされるプログラム識別子（PID）を設定するには、モニタ メトリック MDI モードで **monitorpids** コマンドを使用します。PID を自動学習するには、このコマンドの **no** 形式を使用します。

monitor pids *pid1* [*pid2*] [*pid3*] [*pid4*] [*pid5*]
no monitor pids

構文の説明

pid1 [*pid2*] [*pid3*] [*pid4*] [*pid5*	MDI フローでモニタする PID です。PID 値の範囲は 2 ～ 8190 です。（対応する 16 進数形式の PID の範囲は 0x2 ～ 0x1FFE です）

コマンド デフォルト

PID は設定されていません。

コマンド モード

（config-pmap-c-metric）#

コマンド履歴

リリース	変更箇所
15.1(1)S	このコマンドが導入されました。

使用上のガイドライン

monitorpids コマンドを使用して、MDI フローでモニタする PID を設定します。デフォルトでは、新しい MDI フロー ストリームの最初の 5 つの PID が、モニタリングのために記録されます。これらの PID は、ビデオ、オーディオ、またはキャプションの PID です。ただし、オーディオまたはキャプション データの PID をモニタすることは、インライン ビデオ モニタリングを実装するカスタマーにとっては優先事項ではなく、オプションです。

例

次に、PID を設定する例を示します。

```
router(config-pmap-c-metric)# monitor pids 4050 4678 8902
```

関連コマンド

Command	Description
showpolicy-maptypeperformance-traffic	ポリシーマップ情報と、設定されている場合はモニタされる PID を表示します。

mpls experimental

VC バンドルに割り当てて、そのバンドルのすべての VC メンバーに適用することができる仮想回線（VC）クラスのマルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）レベルを設定するには、VC-class コンフィギュレーション モードで **mplsexperimental** コマンドを使用します。VC クラスから MPLS EXP 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。

バンドルの VC メンバーの MPLS EXP レベルを設定するには、バンドル VC コンフィギュレーション モードで **mplsexperimental** コマンドを使用します。VC から MPLS EXP 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。

mpls experimental [{**other***range*}]
no mpls experimental

構文の説明

other	（任意）明示的に設定されない、0 ～ 7 の範囲の任意の MPLS EXP レベルを指定します。これがデフォルトです。
range	（任意）0 ～ 7 の数字として指定された単一の MPLS EXP レベル、またはハイフンで示された範囲として指定されたレベルの範囲です。

コマンド デフォルト

デフォルトは **other** で、明示的に設定されない、0 ～ 7 の範囲の任意の MPLS EXP レベルです。

コマンド モード

VC クラス用の VC クラス コンフィギュレーション（config-vc-class）
ATM VC バンドル メンバー用のバンドル VC コンフィギュレーション（config-if-atm-member）

コマンド履歴

リリース	変更箇所
12.2(8)T	このコマンドが導入されました。
12.0(26)S	このコマンドが Cisco 10000 シリーズ ルータに実装されました。
12.0(29)S	このコマンドが、Cisco IOS Release 12.0(29)S に統合されました。
12.2(16)BC	このコマンドが ESR-PRE2 に実装されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。

使用上のガイドライン

MPLS EXP レベルを VC バンドル メンバーに割り当てることで、異なる VC バンドル メンバーに MPLS EXP レベルを配布できるため、差別化サービスを作成できます。単一のレベルまたはレベルの範囲をバンドルの個々の VC にマッピングできます。これにより、バンドルの VC が、さまざまなレベルによってマーク付けされたパケットを伝送できます。または、**mplsexperimentalother** コマンドを使用して VC を設定し、具体的に設定されていないレベルによってマーク付けされたトラフィックを伝送することを示すことができます。

mplsexperimentalother コマンドを使用して、指定されいていないすべてのレベルを伝送するように設定できるバンドルの VC は 1 つのみです。この VC がデフォルト VC とみなされます。

このコマンドを VC-class コンフィギュレーション モードで使用するには、このコマンドを入力する前に **vc-classatm** 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。コマンドを含む VC クラスがスタンドアロン VC（バンドル メンバーではない VC）に付加されている場合、このコマンドは効果がありません。

バンドル VC コンフィギュレーション モードでこのコマンドを使用して個々のバンドル メンバーを設定するには、まず **bundle** コマンドを入力して、設定対象の VC メンバーを追加または変更するバンドルのバンドル コンフィギュレーション モードにします。その後、**pvc-bundle** コマンドを使用して、作成または変更する VC を指定し、バンドル VC コンフィギュレーション モードにします。

VC バンドルの VC は、次の設定継承ガイドラインに従います（次に高い MPLS EXP レベルの順にリストされています）。

- bundle-VC モードの VC 設定
- バンドル モードのバンドル設定（および、割り当てられた VC クラス コンフィギュレーションの影響）
- サブインターフェイス モードのサブインターフェイス設定

（注） ATM インターフェイスを使用している場合は、バンドルにすべての MPLS EXP レベル（0 ～ 7 の範囲）を設定する必要があります。この設定では、**mplsexperimentalother** コマンドを使用して、バンドルの単一のメンバーを設定することをお勧めします。**other** キーワードのデフォルトは、明示的に設定されない、0 ～ 7 の範囲の任意の MPLS EXP レベルです。

例

次の例では、バンドルに適用されると、そのバンドルのすべての VC メンバーが MPLS EXP レベル 7 のトラフィックを伝送するように設定する、**mplsexperimental** コマンドを含む、control-class という名前のクラスを設定します。このバンドルの VC メンバーは、その後にバンドル VC レベルで **mplsexperimental** コマンドを使用して個々に設定できます。

```
vc-class atm control-class
 mpls experimental 7
```

次の例では、control-class という名前の相手先固定接続（PVC）401 を設定して、MPLS EXP レベル 4 ～ 2 のトラフィックを伝送し、VC-class コンフィギュレーションで VC に設定されたレベル マッピングを上書きします。

```
pvc-bundle control-class 401
 mpls experimental 4-2
```

関連コマンド

Command	Description
bump	VC バンドルに割り当てることができる VC クラスのバンピング ルールを設定します。
bundle	バンドルを作成するか、既存のバンドルを変更して、バンドル コンフィギュレーション モードにします。
class-vc	VC クラスを ATM PVC、SVC、または VC バンドル メンバーに割り当てます。
protect	VC バンドル メンバーへのアプリケーションの保護されたグループまたは保護された VC ステータスを持つ VC クラスを設定します。
pvc-bundle	VC をメンバーとしてバンドルに追加し、バンドル VC コンフィギュレーション モードにして、その VC バンドル メンバーを設定します。
ubr	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レートを指定します。
vbr-nrt	VBR-nRT QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーに関する出力ピーク セル レート、出力平均セル レート、および出力最大バースト セル サイズを指定します。
vc-classatm	ATM PVC、SVC、または ATM インターフェイス用に VC クラスを作成し、VC-class コンフィギュレーション モードを開始します。

N から P

- non-tcp （835 ページ）
- non-tcp contexts （836 ページ）
- oam-bundle （838 ページ）
- platform ip features sequential （841 ページ）
- platform ipsec fips-mode （844 ページ）
- platform ipsec llq （845 ページ）
- platform punt-police queue （846 ページ）
- platform qos marker-statistics （849 ページ）
- platform qos match-statistics per-ace （851 ページ）
- platform qos match-statistics per-filter （853 ページ）
- platform qos-port-channel_aggregator （855 ページ）
- platform qos-port-channel_multiple_active （856 ページ）
- platform vfi dot1q-transparency （857 ページ）
- plim qos input （859 ページ）
- plim qos input map （862 ページ）
- plim qos input map cos（VLAN の CoS 値を分類） （868 ページ）
- police （871 ページ）
- police (EtherSwitch) （882 ページ）
- police（percent） （884 ページ）
- police（ポリシー マップ） （892 ページ）
- police（2 つのレート） （900 ページ）
- police rate（コントロールプレーン） （908 ページ）
- police rate pdp （914 ページ）
- policy-map （918 ページ）
- policy-map copp-peruser （926 ページ）
- precedence （927 ページ）
- precedence（WRED グループ） （931 ページ）
- preempt-priority （934 ページ）
- priority （936 ページ）

- priority（10000 シリーズ） （940 ページ）
- priority（SIP400） （943 ページ）
- priority-group （946 ページ）
- priority level （949 ページ）
- priority-list default （952 ページ）
- priority-list interface （954 ページ）
- priority-list protocol （956 ページ）
- priority-list queue-limit （961 ページ）
- priority-queue cos-map （963 ページ）
- priority-queue queue-limit （965 ページ）
- pvc-bundle （967 ページ）

non-tcp

IP ヘッダー圧縮（IPHC）プロファイル内で非 Transmission Control Protocol（非 TCP）ヘッダー圧縮を有効にするには、IPHC プロファイル コンフィギュレーション モードで **non-tcp** コマンドを使用します。IPHC プロファイル内で非 TCP ヘッダー圧縮を無効にするには、このコマンドの **no** 形式を使用します。

non-tcp
no non-tcp

構文の説明

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

非 TCP ヘッダー圧縮は有効になっています。

コマンド モード

IPHC 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	変更箇所
12.4(9)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

IPHC プロファイルでの使用目的

non-tcp コマンドは、IPHCプロファイルの一部として使用することを目的としています。IPHC プロファイルは、ネットワーク上でヘッダー圧縮を有効にして設定するために使用されます。IPHC プロファイルを使用したヘッダー圧縮の設定の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、Release 12.4T の「Header Compression」モジュールと「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

例

次に、profile2 という名前の IPHC プロファイルを設定する例を示します。この例では、非 TCP ヘッダー圧縮が設定されます。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
iphc-profile	IPHCプロファイルを作成します。

non-tcp contexts

非 Transmission Control Protocol（TCP）ヘッダー圧縮に使用できるコンテキストの数を設定するには、IPHC プロファイル コンフィギュレーション モードで **non-tcpcontexts** コマンドを使用します。以前に設定したコンテキストの数を削除するには、このコマンドの **no** 形式を使用します。

non-tcp contexts {**absolute** *number-of-connections*|**kbps-per-context** *kbps*}
no non-tcp contexts

構文の説明

absolute	圧縮された非TCPコンテキストの最大数が、固定（絶対）数に基づくことを示します。
number-of-connections	非 TCP 接続の数です。範囲は 1 ～ 1000 です。
kbps-per-context	圧縮された非TCPコンテキストの最大数が、使用可能な帯域幅に基づくことを示します。
kbps	各コンテキストに許可する kbps 数です。範囲は 1 ～ 100 です。

コマンド デフォルト

non-tcpcontexts コマンドは、帯域幅に基づいてコンテキストの数を計算し、コンテキストごとに 4 kbps を割り当てます。

コマンド モード

IPHC 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	変更箇所
12.4(9)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

non-tcpcontexts コマンドを使用して、非 TCP ヘッダー圧縮に使用できるコンテキストの数を設定します。コンテキストとは、コンプレッサがヘッダーの圧縮に使用し、デコンプレッサがヘッダーの圧縮解除に使用する状態です。コンテキストは、送信された最終ヘッダーの非圧縮バージョンであり、パケットの圧縮と圧縮解除に使用する情報が含まれます。

IPHC プロファイルでの使用目的

non-tcpcontexts コマンドは、IPHC プロファイルの一部として使用することを目的としています。IPHC プロファイルは、ネットワークでのヘッダー圧縮を有効および設定するために使用されます。IPHC プロファイルを使用してヘッダー圧縮を設定する詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、リリース 12.4T の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

絶対数としてのコンテキストの数の設定

non-tcpcontexts コマンドにより、コンテキストの数を絶対数として設定できます。コンテキストの数を絶対数として設定するには、1 ～ 1000 の数を入力します。

帯域幅に基づくコンテキストの数の計算

non-tcpcontexts コマンドにより、IPHC プロファイルが適用されるネットワーク リンクで使用できる帯域幅に基づいて、コンテキストの数を計算できます。

使用できる帯域幅に基づいて計算されたコンテキストの数を得るには、**kbps-per-context** キーワードに続けて *kbps* 引数の値を入力します。このコマンドは、使用できる帯域幅を、指定された kbps で割ります。たとえば、ネットワーク リンクの帯域幅が 3000 kbps で、*kbps* 引数に 5 を入力すると、このコマンドは 600 のコンテキストを算出します。

例

profile2 という IPHC プロファイルの例を、次に示します。この例では、非 TCP コンテキストの数が 75 に設定されています。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp contexts absolute 75
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
iphc-profile	IPHCプロファイルを作成します。

oam-bundle

バンドル、またはVCバンドルに適用できるVCクラスのすべての仮想回線（VC）メンバーについて、エンドツーエンドF5運用管理および保守（OAM）ループバック セル生成およびOAM管理を有効にするには、SVC-bundle コンフィギュレーション モードまたは VC-class コンフィギュレーション モードで **oam-bundle** コマンドを使用します。バンドルまたはクラスの設定から OAM 管理を削除するには、このコマンドの **no** 形式を使用します。

バンドルのすべての VC メンバーについて、エンドツーエンド F5 OAM ループバック セル生成およびOAM管理を有効にするには、バンドル コンフィギュレーション モードで **oam-bundle** コマンドを使用します。バンドルから OAM 管理を削除するには、このコマンドの **no** 形式を使用します。

oam-bundle [manage] [*frequency*]
no oam-bundle [manage] [*frequency*]

構文の説明

manage	（任意）OAM 管理を有効にします。このキーワードを省略すると、ループバック セルは送信されますが、バンドルは管理されません。
frequency	（任意）送信される OAM ループバック セル間の秒数です。間隔の範囲は、0 ～ 600 秒です。*frequency* 引数のデフォルト値は 10 秒です。

コマンド デフォルト

エンドツーエンドF5 OAM ループバック セル生成およびOAM管理は無効になっていますが、OAM セルが受信されるとループバックされます。

コマンド モード

SVC-bundle コンフィギュレーション（SVC バンドル用）
VC-class コンフィギュレーション（VC クラス用）
バンドル コンフィギュレーション（ATM VC バンドル用）

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
12.0(26)S	このコマンドが Cisco 10000 シリーズ ルータに追加されました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。
12.2(4)T	このコマンドが、SVC バンドル コンフィギュレーション モードで使用できるようになりました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。

リリース	変更箇所
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

このコマンドは、VC バンドルが OAM 管理されるかどうかを定義します。このコマンドがバンドルに設定された場合、バンドルのすべての VC メンバーが OAM 管理されます。OAM 管理が有効になっている場合は、**oamretry** コマンドを使用して、OAM 管理の追加の制御を設定できます。

コマンドを含む VC クラスがスタンドアロン VC（バンドル メンバーではない VC）に付加されている場合、このコマンドは効果がありません。この場合、属性は VC によって無視されます。

VC-class コンフィギュレーション モードでこのコマンドを使用するには、まず **vc-classatm** 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。

バンドル コンフィギュレーション モードでこのコマンドを使用するには、まず **bundle** サブインターフェイス コンフィギュレーション コマンドを入力してバンドルを作成するか、既存のバンドルを指定します。

VC バンドルの VC は、次の設定継承規則に従います（次に高い優先順位の順にリストされています）。

- bundle-VC モードの VC 設定
- バンドル モードのバンドル設定（および、割り当てられた VC-class コンフィギュレーションの影響）

例

次の例では、「bundle 1」という名前のバンドルの OAM 管理を有効にします。

```
bundle bundle1
 oam-bundle manage
```

関連コマンド

Command	Description
broadcast	ブロードキャスト パケットの複製と、ATM VC クラス、PVC、SVC、または VC バンドルへの送信を設定します。
bundle	バンドル コンフィギュレーション モードに入って、バンドルを作成するか、または既存のバンドルを変更します。
class-bundle	指定された VC クラスに含まれるバンドル レベルのコマンドで VC バンドルを設定します。
encapsulation	インターフェイスで使用するカプセル化方式を設定します。

Command	Description
inarp	ATM PVC、VC クラス、または VC バンドルの Inverse ARP の時間を設定します。
oamretry	ATM PVC、SVC、VC クラス、または、VC バンドルの OAM 管理に関連するパラメータを設定します。
protocol(ATM)	ATM PVC、SVC、VC クラス、または VC バンドルのスタティック マップを設定します。次に、直接 PVC 上、VC バンドル上、または VC クラス内で Inverse ARP を設定することによって、ATM PVC の Inverse ARP または Inverse ARP ブロードキャストを有効にします（IP および IPX プロトコルだけに適用）。
vc-classatm	ATM 相手先固定接続（PVC）、相手先選択接続（SVC）、または ATM インターフェイス用の仮想回線（VC）クラスを作成します。

platform ip features sequential

Internet Protocol（IP）プレシデンスベースまたは DiffServ コード ポイント（DSCP）ベースの出力 Quality of Service（QoS）フィルタリングを有効にして、入力ポリシー フィーチャ カード（PFC）QoS によって行われる IP プレシデンスまたは DSCP ポリシングまたはマーキングの変更を使用するには、インターフェイス コンフィギュレーション モードで、**platformipfeaturessequential** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

platform ip features sequential [**access-group** {*ip-acl-nameip-acl-number*}]
no platform ip features sequential [**access-group** {*ip-acl-nameip-acl-number*}]

構文の説明

access-group *ip-acl-name*	（任意）再循環パケットの一致条件を指定するために使用される ACL の名前を指定します。
access-group *ip-acl-number*	（任意）再循環パケットの一致条件を指定するために使用される ACL の番号を指定します。有効値は 1 ～ 199 と 1300 ～ 2699 です。

コマンド デフォルト

IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングは、受信した IP precedence または DSCP 値を使用し、ポリシングまたはマーキングの結果として入力 QoS によって加えられた IP precedence または DSCP の変更を使用しません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.2(50)SY	このコマンドが導入されました。
12.2(18)SXE	このコマンドのサポートが Supervisor Engine 720 に追加されました。
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。

使用上のガイドライン

注意 スイッチが、再マーキングされた DSCP に対する出力 ACL サポートを設定したが PFC3A モードで動作している場合は、PFC3 はトラフィックを処理して入力 PFC QoS を適用する際、入力 PFC QoS フィルタリングおよび入力 PFC QoS を適用し、入力インターフェイスに設定されたすべての出力 QoS フィルタリングおよび出力 PFC QoS を不正に適用します。この結果、再マーキングされた DSCP に対する出力 ACL サポートが有効になっているインターフェイス上で QoS フィルタリングが設定された場合に、予期しない動作が発生します。この問題は、他の PFC3 モードでは発生しません。

強化出力 QoS フィルタリングにより、IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングで入力 QoS によって加えられた IP precedence または DSCP ポリシング/マーキングの変更を使用することができます。

強化されていない出力 QoS フィルタリングの動作は、QoS がハードウェアで適用されたときの通常の Cisco 7600 シリーズ ルータまたは Catalyst 6500 シリーズ スイッチ動作です。

PFC3 は、出力レイヤ 3 インターフェイス（レイヤ 3 インターフェイスとして設定された LAN ポートまたは VLAN インターフェイス）上のレイヤ 3 スイッチドおよびルーテッド トラフィックについてだけ、出力 PFC QoS を提供します。

強化出力 QoS フィルタリングは、入力レイヤ 3 インターフェイス（レイヤ 3 インターフェイスとして設定された LAN ポートまたは VLAN インターフェイス）上で設定します。

特定の標準、拡張名前付き、または拡張番号付き IP ACL によってフィルタされたトラフィックについてだけ強化出力 QoS フィルタリングをイネーブルにするには、IP ACL の名前または番号を入力します。

IP ACL の名前または番号を入力しなかった場合、強化出力 QoS フィルタリングはインターフェイス上のすべての IP 入力 IP トラフィックについてイネーブルになります。

（注） 強化出力 QoS フィルタリングを設定すると、PFC3A はトラフィックを処理して、入力 PFC QoS を適用します。PFC3A は、入力 QoS フィルタリングおよび Cisco 7600 シリーズ ルータまたは Catalyst 6500 シリーズ スイッチ ハードウェア入力 QoS を適用します。PFC3A は、入力インターフェイス上で設定される出力 QoS フィルタリングおよび Cisco 7600 シリーズ ルータまたは Catalyst 6500 シリーズ スイッチ ハードウェア出力 QoS を誤って適用します。

（注） 入力 QoS マーキングによって変更された IP プレシデンスまたは DSCP のマッチングを行うために、レイヤ 2 機能を使用するインターフェイス上で強化出力 QoS フィルタリングを設定した場合、パケットはリダイレクトまたは破棄されて、出力 QoS によって処理されません。

（注） 強化出力 QoS フィルタリングをイネーブルにした場合、再帰 ACL、NAT、TCP インターセプトなどの NetFlow ベース機能のハードウェア アクセラレーションはディセーブルになります。

設定を確認するには、**showrunning-configinterface** コマンドを使用します。

例

次に、強化出力 QoS フィルタリングを有効にする例を示します。

```
Router(config-if)# platform ip features sequential

Router(config-if)#
```

次に、強化出力 QoS フィルタリングを無効にする例を示します。

```
Router(config-if)# no platform ip features sequential

Router(config-if)#
```

関連コマンド

コマンド	説明
showrunning-configinterface	現在の実行コンフィギュレーション ファイルの内容を表示します。

platform ipsec fips-mode

連邦情報処理標準（FIPS）とハードウェア エントロピーを有効にするには、グローバル コンフィギュレーション モードで **platform ipsec fips-mode** コマンドを使用します。FIPS とハードウェア エントロピ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。

platform ipsec fips-mode
no platform ipsec fips-mode

構文の説明

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

グローバル設定

コマンド履歴

リリース	変更箇所
Cisco IOS XE Release 3.7.3S	このコマンドが、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。

例

次に、**platform ipsec fips-mode** コマンドを使用して、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータで FIPS モードとハードウェア エントロピーを有効にする例を示します。

```
Router(config)# platform ipsec fips-mode

 enable FIPS mode will take effect after reboot!
```

関連コマンド

コマンド	説明
show crypto entropy status	

platform ipsec llq

Quality of Service（QoS）グループの低遅延キューイング（LLQ）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 **platform ipsec llq** コマンドを使用します。LLQ を無効にするには、このコマンドの **no** バージョンを使用します。

platform ipsec llq qos-group *group-number*
no platform ipsec llq qos-group *group-number*

構文の説明

qos-group	LLQ を有効化する QoS グループを指定します。
group-number	グループを識別する番号です。有効な値は 1 ～ 99 です。

コマンド デフォルト

LLQ 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	変更箇所
Cisco IOS XE Release 2.4	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、トンネル保護が使用されているトンネル インターフェイスの IPsec に、指定した QoS グループを高優先順位として設定できます。これにより、優先順位の高いパケットがデフォルト キューにキューイングされることを防ぎ、オーバーサブスクリプション時の遅延とトラフィックの損失を低減します。

例

次の例では、QoS グループ 1 で低遅延キューイングを設定する方法を示します。

```
ASR1006-1(config)# platform ipsec llq qos-group 1
```

関連コマンド

コマンド	説明
set qos-group	後からパケットの分類に使用できる QoS グループ ID を設定します。

platform punt-police queue

キューのパント ポリシングを有効にして、キュー単位で最大パント レートとバースト 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、**platformpunt-policequeue** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

platform punt-police queue *queue-id max-punt-rate max-burst-rate*
no platform punt-police queue *queue-id*

構文の説明

queue-id	キューを識別する一意の番号です。有効値の範囲は 0 ～ 28 です。
max-punt-rate	パケット/秒（pps）単位のキューの最大パントレートです。有効値の範囲は 10 ～ 10000 です。
max-burst-rate	パケット/秒（pps）単位のキューの最大バーストレートです。有効値の範囲は 1000 ～ 10000 です。

コマンド デフォルト

キューのパント ポリシングは有効になっています。各キューのデフォルトのリストについては、「使用上のガイドライン」のセクションにある表を参照してください。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
Cisco IOS XE 3.5S	このコマンドが、Cisco ASR 903 ルータに追加されました。

使用上のガイドライン

パント ポリシングは、ルート プロセッサ（RP）が重要でないトラフィックを処理せずに済むようにします。トラフィックは、さまざまな条件に基づいて異なる CPU キューに配置されます。その後、キュー単位で最大パント レートを設定できます。デフォルトでは、キューに対して明示的なポリシングは行われません。

（注） 特定の CPU キューのトラフィックは、設定されたパント レートとは無関係に、キューのプライオリティ、キューのサイズ、またはトラフィック パント レートに基づいて破棄されることがあります。

設定を確認するには、**show platform software infrastructure punt statistics** コマンドを使用します。

パントポリシングは、デフォルトで有効になっています。次の表は、各キューのデフォルトのパント ポリシング設定を示しています。

表 *28* : デフォルトのパント ポリシング設定

リング/キュー	キュー名	パント レート（pps）	バースト レート（pps）
0	SW FORWARDING Q	500	1000
1	ROUTING PROTOCOL Q	500	1000
2	ICMP Q	500	1000
3	HOST Q	1000	2000
4	ACL LOGGIN Q	500	1000
5	STP Q	3000	6000
6	L2 PROTOCOL Q	1000	2000
7	MCAST CONTROL Q	1000	2000
8	BROADCAST Q	500	1000
9	REP Q	3000	6000
10	CFM Q	3000	6000
11	CONTROL Q	1000	2000
12	IP MPLS TTL Q	1000	2000
13	DEFAULT MCAST Q	500	1000
14	MCAST ROUTE DATA Q	500	1000
15	MCAST MISMATCH Q	500	1000
16	RPF FAIL Q	500	1000
17	ROUTING THROTTLE Q	500	1000
18	MCAST Q	500	1000
19	MPLS OAM	1000	2000
20	IP MPLS MTU	500	1000
21	PTP Q	3000	6000
22	LINUX ND Q	500	1000
23	KEEPALIVE Q	1000	2000

リング/キュー	キュー名	パント レート（pps）	バースト レート（pps）
24	ESMC Q	3000	6000
25	FPGA BFD Q	3000	6000
26	FPGA CCM Q	3000	6000
27	FPGA CFE Q	3000	6000
28	L2PT DUP Q	4000	8000

例

次に、キュー 20 のパント ポリシングを有効にして、最大パント レートを 9000 pps に設定し、最大バースト レートを 10000 pps に設定する例を示します。

```
Router(config)# platform punt-police queue 20 9000 10000
```

関連コマンド

コマンド	説明
show platform hardware pp active infrastructure pi npd rx policer	すべてのキューのパント ポリシング統計情報を表示します。
show platform software infrastructure punt statistics	キューベースのパント ポリシングが有効になっているかどうかを表示します。

platform qos marker-statistics

システム全体（プラットフォーム）レベルで、変更されたヘッダーを持ち、ローカルルータ処理のカテゴリに分類されたパケット数を表示するには、グローバル コンフィギュレーション モードで **platformqosmarker-statistics** コマンドを使用します。QoS パケット マーキング統計情報機能の表示を無効にするには、このコマンドの **no** 形式を使用します。

platform qos marker-statistics
no platform qos marker-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

無効になっています（パケット マーキング統計情報は表示されません）。

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	変更箇所
Cisco IOS XE リリース 3.3S	このコマンドが導入されました。

使用上のガイドライン

システムでポリシーマップがインターフェイスに関連付けられていないことを確認します。関連付けられている場合は、システムによって次のメッセージが返されます。

```
Either a) A system RELOAD or
       b) Remove all service-policies, re-apply the change
            to the statistics, re-apply all service-policies
   is required before this command will be activated.
```

QoS パケット マーキング統計情報機能を有効にすると、拡張設定では CPU 使用率が増加する可能性があります。QoS パケット マーキング統計情報機能を有効にする前に、統計情報の利点とシステムの CPU 使用率の増加とを比較して検討する必要があります。

例

次の例に、以下をどのように実行するかを示します。

- QoS パケット マーキング統計情報機能の有効化
- 入力インターフェイスでの入力サービス ポリシーの設定
- 設定されたクラスへのトラフィックの分類
- IP プレシデンスを 1 に設定するためのクラスでのマーキングの設定
- **showpolicy-mapinterface** コマンドの出力の表示

```
Router#
platform qos marker-statistics
```

```
class-map test_class
    match access-group 101
  policy-map test_policy
    class test_class
       set ip precedence 1
Interface POS2/0/1
  service-policy input test_policy
Router#
show policy-map interface
POS2/0/1
  Service-policy input: test_policy
    Class-map: test_class (match-all)
      6644560 packets, 757479840 bytes
      5 minute offered rate 8720000 bps, drop rate 0000 bps
      Match:  precedence 5
      QoS Set
        precedence 1
          Packets marked 6644560
    Class-map: class-default (match-any)
      18 packets, 1612 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

関連コマンド

コマンド	説明
showplatformhardwareqfpactivefeatureqosconfigglobal	QoS パケット マーキング統計情報機能が有効になっているかどうかを表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。
showpolicy-mapsession	PPPoE セッションに対して有効な QoS ポリシー マップを表示します。

platform qos match-statistics per-ace

Quality of Service（QoS）パケット一致統計情報を有効にして、QoS ポリシーで使用される個々のアクセス制御要素（ACE）に一致するパケット数とバイト数をカウントするには、グローバル コンフィギュレーション モードで **platform qos match-statistics per-ace** コマンドを使用します。ACE 単位の QoS パケット一致統計情報を無効にするには、このコマンドの **no** 形式を使用します。

platform qos match-statistics per-ace
no platform qos match-statistics per-ace

構文の説明

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

無効になっています（QoS の ACE 統計情報は増えません）。

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	変更箇所
Cisco IOS XE Release 3.10S	このコマンドが導入されました。

使用上のガイドライン

platform qos match-statistics per-ace コマンドを設定して QoS の ACE 単位のパケット一致統計情報を有効にする前に、**platform qos match-statistics per-filter** コマンドを設定して QoS のフィルタ単位のパケット一致統計情報を有効にする必要があります。

システムでポリシーマップがインターフェイスに関連付けられていないことを確認します。ある場合は、システムによって次のメッセージが返されます。

```
Either a) A system RELOAD or
       b) Remove all service-policies, re-apply the change
          to the statistics, re-apply all service-policies
   is required before this command will be activated.
```

ACE 単位の QoS 統計情報機能をイネーブルにすると、拡張設定では CPU 使用率が増加する可能性があります。この機能を有効にする前に、統計情報の利点とシステムの CPU 使用率の増加とを比較して検討する必要があります。

例

次に、QoS ポリシー マップに ACE 単位のフィルタを設定する例を示します。

```
Device(config)# platform qos match-statistics per-filter
Device(config)# platform qos match-statistics per-ace
```

関連コマンド

コマンド	説明
class-map match-any	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
platformqos match-statistics per-filter	システム全体（プラットフォーム）レベルで、QoS のフィルタ単位のパケット一致統計情報を有効にします。
showaccesslists	QoS サービス ポリシーで使用される ACL を含む、すべての設定済み ACL の ACE 統計情報を表示します。
showplatformhardwareqfpactivefeatureqosconfigglobal	QoS パケット一致統計情報機能が有効になっているかどうかを表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

platform qos match-statistics per-filter

システム全体（プラットフォーム）レベルで QoS パケット フィルタを定義して、そのフィルタに一致するパケット数とバイト数を表示するには、グローバル コンフィギュレーション モードで **platformqosmatch-statisticsper-filter** コマンドを使用します。フィルタリングを停止するには、このコマンドの **no** 形式を使用します。

platform qos match-statistics per-filter
no platform qos match-statistics per-filter

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

無効になっています（パケット一致統計情報は表示されません）。

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	変更箇所
Cisco IOS XE リリース 3.3S	このコマンドが導入されました。

使用上のガイドライン

システムでポリシーマップがインターフェイスに関連付けられていないことを確認します。関連付けられている場合は、システムによって次のメッセージが返されます。

```
Either a) A system RELOAD or
       b) Remove all service-policies, re-apply the change
            to the statistics, re-apply all service-policies
   is required before this command will be activated.
```

QoS パケット一致統計情報機能を有効にすると、拡張設定では CPU 使用率が増加する可能性があります。QoS パケット一致統計情報を有効にする前に、統計情報の利点とシステムの CPU 使用率の増加とを比較して検討する必要があります。

```
Ensure you have defined a filter using the class-map
 command with the match-any
 keyword.
```

例

次の例は、このコマンドの使用方法を示しています。

```
Router>
enable
Router#
configure terminal
Router(config)#
platform qos match-statistics per-filter
Router# end
```

関連コマンド

コマンド	説明
class-map match-any	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
showplatformhardwareqfpactivefeatureqosconfigglobal	QoS パケット一致統計情報機能が現在有効になっているかどうかを表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

platform qos-port-channel_aggregator

ポート チャネルで QoS 適用ポリシーを有効にするには、グローバル コンフィギュレーション モードで **lacp max-bundle** とともに **platform qos-port-channel_aggregator** コマンドを使用します。

platform qos-port-channel_aggregator *port-channel-number***enable**

構文の説明

port-channel-number	ポート チャネルの情報を表示します。
enable	QoS ポリシー設定を有効にします。

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

グローバル設定

コマンド履歴

リリース	変更箇所
XE 3.18 SP	このコマンドのサポートが ASR 900 シリーズ ルータに追加されました。

例

次の例は、ポートチャネル アクティブ/アクティブ モードを有効にする方法を示しています。

```
enable
configure terminal
platform qos-port-channel_aggregator 1
end
```

関連コマンド

コマンド	説明
show policy-map interface port-channel	EFP のポリシー マップ コンフィギュレーションを検証します。

platform qos-port-channel_multiple_active

バンドルごとにアクティブなポートチャネルを設定するには、グローバル コンフィギュレーション モードで **platform qos-port-channel_multiple_active** コマンドを使用します。

platform qos-port-channel_multiple_active *port-channel*

構文の説明

port-channel	ポート チャネルの情報を表示します。

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

グローバル設定

コマンド履歴

リリース	変更箇所
XE 3.18.1 SP	このコマンドのサポートが ASR 900 シリーズ ルータに追加されました。

使用上のガイドライン

アクティブ アクティブ モードで作成されるポート チャネルを指定する必要があります。

例

次の例は、ポートチャネル アクティブ/アクティブ モードを有効にする方法を示しています。

```
enable
configure terminal
platform qos-port-channel_multiple_active  10
end
```

関連コマンド

コマンド	説明
show sdm prefer current	ポートチャネルアクティブ/アクティブモードを有効にした後で設定を検証します。
show etherchannel summary	ポートチャネル概要の詳細を検証します。
show policy-map interface brief	ポートチャネルインターフェイスでアタッチしたポリシーマップを検証します。

platform vfi dot1q-transparency

802.1Q 透過性モードを有効にするには、グローバル コンフィギュレーション モードで **platformvfidot1q-transparency** コマンドを使用します。802.1Q 透過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。

platform vfi dot1q-transparency
no platform vfi dot1q-transparency

構文の説明

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

802.1Q 透過性モードは無効になっています。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(18)SXF2	このコマンドが Supervisor Engine 720 に導入されました。

使用上のガイドライン

このコマンドは、オプティカル サービス モジュール（OSM）でのみサポートされています。

802.1Q 透過性により、サービス プロバイダーは、仮想プライベート LAN サービス（VPLS）のカスタマー 802.1p ビットを変更せずに、コアベース QoS ポリシーのマルチプロトコル ラベル スイッチング Experimental（MPLS EXP）ビットを変更できます。

Cisco IOS Release 12.2(18)SXF1 よりも前のリリースでは、すべてに一致して MPLS EXP ビットを設定するサービス ポリシーを VLAN インターフェイスに適用すると、内部ゲートウェイ プロトコル（IGP）ラベルと VC ラベルの両方に影響しました。受信した仮想回線（VC）MPLS EXP ビットに基づいて出力プロバイダー エッジ（PE）で 802.1p ビットが書き換えられたため、VPLS カスタマーの 802.1p ビットが変更されました。

EoMPLS の Dot1q 透過性機能では、VLAN に適用されたポリシーが IGP ラベル（コア QoS 用）にだけ影響し、VC ラベル EXP ビットと 802.1p ビットを同じにします。一方、出力 PE では、802.1p ビットは受信した VC EXP ビットに基づいて書き換えられますが、EXP ビットは入力 802.1p ビットに一致しているため、VPLS カスタマーの 802.1p ビットは変更されません。

グローバル コンフィギュレーションは、Cisco 7600 シリーズ ルータに設定されたすべての仮想転送インスタンス（VFI）およびスイッチ仮想インターフェイス（SVI）の EoMPLS VC に適用されます。

相互運用性を確保するには、接続されているすべての PE ルータに EoMPLS の Dot1q 透過性機能を適用する必要があります。

例

次に、802.1Q 透過性をイネーブルにする例を示します。

```
platform vfi dot1q-transparency
```

次に、802.1Q 透過性をディセーブルにする例を示します。

```
no platform vfi dot1q-transparency
```

関連コマンド

コマンド	説明
showcwanvfidot1q-transparency	802.1Q透過性モードを表示します。

plim qos input

Packet over SONET（POS）SPA、チャネライズド SPA、およびクリアチャネル SPA のインターフェイスに入力分類テンプレートをアタッチするには、インターフェイス コンフィギュレーション モードで **plim qos input class-map** *class-map index* コマンドを使用します。クリアチャネル SPA のインターフェイス上の低プライオリティ パケットに超過重み値を割り当てるには、**plim qos input** *weight weight-value* コマンドを使用します。指定したインデックスの入力分類テンプレートの割り当てを削除するには、**plim qos input class-map** コマンドの **no**形式を使用します。低プライオリティ パケットの超過スケジューリングをインターフェイスから削除するには、 **plim qos input weight** コマンドの **no** 形式を使用します。

plim qos input {**class-map** *class-map index*|**weight** *weight-value*}
no plim qos input {**class-map** *class-map index*|**weight**}

構文の説明

class-map	入力分類テンプレートのクラス マップをインターフェイスにマッピングします。
class-map index	分類基準がインターフェイスに適用されるインデックス分類テンプレート番号です。
weight	低プライオリティ パケット間で超過帯域幅を共有するためにインターフェイスに割り当てられる重みをスケジュールします。
weight-value	低プライオリティ パケット間で超過帯域幅を共有するためにインターフェイスに割り当てられる重み値です。インターフェイスに割り当てられる超過帯域幅は相対的で、他のインターフェイスに割り当てられた空き帯域幅と使用可能な空き帯域幅に依存します。有効な範囲は 40 ～ 10000 です。

コマンド デフォルト

たとえば、SIP0 はテンプレート 1 ～ 62 を使用し、SIP1 はテンプレート 63 ～ 124 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	変更箇所
3.1.0S	分類テンプレートをインターフェイスにアタッチし、インターフェイスに重みを割り当てて、超過帯域幅を分配できるようにするために、このコマンドが導入されました。

使用上のガイドライン

分類テンプレート固有の詳細はテンプレートで定義され、テンプレートは **plim qos input class-map***class-map index* コマンドを使用してインターフェイスにアタッチされます。このコマンドの **no** 形式を使用することで、分類テンプレートを削除できます。**plim qos input**

class-map*class-mapindex* コマンドは、POS SPA、チャネライズド SPA、およびクリアチャネル SPA に適用できます。

plim qos input weight*weight-value* コマンドは、低プライオリティ パケットの超過帯域幅の共有を割り当てるために使用されます。**plim qos input weight***weight-value* コマンドは、インターフェイスに重みを割り当てるために使用され、他のインターフェイスに割り当てられた相対的な重みに応じて、インターフェイス間で帯域幅が共有されます。超過帯域幅は、高プライオリティ パケットが処理された後に割り当てられます。

（注） **plim qos input weight***weight-value* コマンドは、クリアチャネル SPA にのみ適用できます。

（注） ポートレベル（インターフェイス レベル）で「絶対優先」キューの最小帯域幅を設定するためのこのオプションは、現在の操作モードに適用できないため廃止されました。既存の設定は、エラーが発生して拒否されます。

（注） **plim qos input** コマンドは、Cisco ASR 1000 シリーズ ルータ上の Circuit Emulation over Packet（CEoP）OC-3 SPA の CEM インターフェイスからはサポートされていません。

（注） **plim qos input** は、Cisco ASR 1000 シリーズ ルータ上のチャネライズド T1/E1（CTE1）CEoP SPA の CEM インターフェイスからはサポートされていません。

コマンドライン インターフェイスには次のコマンドがありますが、Cisco ASR 1000 シリーズ ルータ上の CEoP OC3 SPA および CTE1 CEoP SPA には効果がありません。これらのコマンドのいずれかを設定した場合、そのコマンドが CEoP OC3 SPA でサポートされていないことを示すメッセージが表示されます。これらのコマンドのいずれかを設定すると、Cisco ASR 1000 シリーズ ルータでも同じ内容のメッセージが表示されます。

hw-module subslot {*slot*/*subslot*} **qos input** {{**policer bandwidth** *bandwidth***strict-policy**} | **weight** *weight*}}

例

次に、**plim qos input class-map***class-map index* コマンドを使用して分類テンプレートをインターフェイスにアタッチする例を示します。

```
Router# config
Router(config)# interface POS 0/2/0
Router(config-if)# plim qos input class-map
2
```

次に、**plim qos input weight***50* コマンドを使用してインターフェイスに 50 の重みを割り当てて、低プライオリティ パケット間で超過帯域幅を共有できるようにする例を示します。

```
Router# config
Router(config)# interface POS 0/2/0
Router(config-if)# plim qos input weight
50
```

関連コマンド

Command	Description
plimqosclass-map	分類テンプレートをインターフェイスにアタッチします。

plim qos input map

ギガビット イーサネット共有ポート アダプタ（SPA）でのプライオリティ キューを設定するには、インターフェイス コンフィギュレーション モードまたはサブインターフェイス コンフィギュレーション モードで **plim qos input map** コマンドを使用します。プライオリティ キューを削除するには、このコマンドの **no** 形式を使用します。

plim qos input map { **cos** {**enable** | *cos-value***queue low-latency**} | **ip** {**precedence-based** | **precedence** *precedence-value***queue low-latency**} | **ipv6 tc** *tc-value* **queue low-latency** | **mpls exp** *exp-value***queue low-latency**

no plim qos input map { **cos** {**enable** | *cos-value***queue low-latency**} | **ip** {**precedence-based** | **precedence** *precedence-value***queue low-latency**} | **ipv6 tc** *tc-value* **queue low-latency** | **mpls exp** *exp-value***queue low-latency**

構文の説明

cos enable	IEEE 802.1Q ネットワーキング標準 TCI プライオリティ ビットに応じた入力 VLAN トラフィックの分類を有効にします。 （注） このコマンドは、VLANインターフェイスだけに適用できます。
cos *cos-value* **queue low-latency**	サブインターフェイス上の着信 VLAN トラフィックを 802.1Q プライオリティ ビットに応じて分類し、トラフィックを適切なキューに配置します。デフォルトでは、802.1Q プライオリティ ビットが 6 または 7 に設定されたトラフィックは高プライオリティ キューに配置され、他のすべてのトラフィックは低プライオリティ キューに配置されます。 *cos-value* は、0 ～ 7 の IEEE 802.1Q または ISL サービス クラス（CoS）値を指定します。 （注） QinQ サブインターフェイスで CoS 値を設定すると、同じ外部 VLAN ID を持つすべての QinQ サブインターフェイスに、その CoS 値が適用されます。 **low-latency** は、高プライオリティ キューを指定します。
ip dscp-based	DSCP ビットの値に応じた着信 IP トラフィックの分類を有効にします。 （注） このコマンドは物理インターフェイスにのみ適用されます。

ip dscp *dscp-value* **queue low-latency**	DiffServ コード ポイント（DSCP）ビットの値に応じて着信 IP トラフィックを分類し、トラフィックを適切なキューに配置します。デフォルトでは、Expedited Forwarding（EF）と等しい DSCP ビットを持つ IP トラフィックは低遅延キューを使用し、その他の DSCP 値を持つトラフィックは低プライオリティ キューを使用します。 **dscp-value** は、DSCP ビットの値です。ハイフンで区切られた値の範囲または値のリストを指定できます。有効な値のリストについては、「使用上のガイドライン」セクションを参照してください。 *low-latency* は、高プライオリティ キューを指定します。
ip precedence-based	IP プレシデンス値に応じた着信 IP トラフィックの分類を有効にします。 （注）　このコマンドは物理インターフェイスにのみ適用されます。
ip precedence *precedence-value* **queue low-latency**	IP プレシデンス ビットの値に応じて着信 IP トラフィックを分類し、トラフィックを適切なキューに配置します。IP プレシデンス ビットが 6 または 7 に設定されている IP トラフィックは低遅延キューを使用し、その他のすべてのトラフィックは低プライオリティ キューを使用します。 *precedence-value* は、IP プレシデンス ビットの値（0 ～ 7）です。ハイフンで区切られた値の範囲または値のリストを指定できます。「使用上のガイドライン」セクションを参照してください。 **low-latency** は、高プライオリティ キューを指定します。
ipv6 tc *tc-value***queue low-latency**	トラフィック クラス ビットの値に応じて入力 IPv6 トラフィックを分類し、トラフィックを適切なキューに配置します。デフォルトでは、**ef** と等しいトラフィック クラス値を持つ IPv6 トラフィックは高プライオリティ キューを使用し、その他のすべてのトラフィックは低プライオリティ キューを使用します。トラフィック クラス オクテットの最上位 6 ビットのみが分類に使用されます。 （注）　このコマンドは物理インターフェイスに適用されます。 *tc-value* は、トラフィック クラス ビットの値です。ハイフンで区切られた値の範囲または値のリストを指定できます。有効な値のリストについては、「使用上のガイドライン」セクションを参照してください。 **low-latency** は、高プライオリティ キューを指定します。

mpls exp *exp-value* **queue low-latency**	EXP ビットの値に応じて着信 MPLS トラフィックを分類し、トラフィックを適切なキューに配置します。デフォルトでは、EXP ビットが 6 または 7 に設定されているトラフィックは高プライオリティ キューを使用し、その他のすべてのトラフィックは低プライオリティ キューを使用します。 （注）　このコマンドは物理インターフェイスに適用されます。 *exp-value* は、EXP ビットの値（0 ～ 7）です。ハイフンで区切られた値の範囲または値のリストを指定できます。 **low-latency** は、高プライオリティ キューを指定します。

コマンド デフォルト

無効

コマンド モード

インターフェイス コンフィギュレーション（config-if）
サブインターフェイス コンフィギュレーション（config-subif）

コマンド履歴

リリース	変更箇所
12.2(33)SB	このコマンドが、PRE3 用と PRE4 用の Cisco 10000 シリーズ ルータに導入されました。
12.2(33)SCB	このコマンドが Cisco IOS リリース 12.2(33)SCB に統合されました。
3.1.0S	このコマンドが、Cisco ASR 1000 シリーズ ルータの ATM インターフェイスでサポートされました。

使用上のガイドライン

plim qos input map コマンドは、高プライオリティ トラフィックと低プライオリティ トラフィックを分離し、トラフィックを適切なインターフェイス キューに配置します。このコマンドは、SPA インターフェイス プロセッサ（SIP）でプライオリティ トラフィックと非プライオリティ トラフィックを分離し、オーバーサブスクリプション シナリオでの高プライオリティ トラフィックのドロップを防止します。各 SPA は、1 つのプライオリティ キューをサポートします。

ルータは、ギガビット イーサネット SPA での入力トラフィックの優先順位付けのために、次の分類タイプをサポートしています。

- VLAN 802.1Q プライオリティ ビット
- IP DSCP ビット
- IP プレシデンス ビット
- IPv6 トラフィック クラス ビット

plim qos input map ip dscp *dscp-value***queue low-latency** コマンドで、*dscp-value* に有効な値は次のいずれかです。

- 0 to 63：DiffServ コード ポイント値

- af11：001010
- af12：001100
- af13：001110
- af21：010010
- af22：010100
- af23：010110
- af31：011010
- af32：011100
- af33：011110
- af41：100010
- af42：100100
- af43：100110
- cs1：優先順位 1（001000）
- cs2：優先順位 2（010000）
- cs3：優先順位 3（011000）
- cs4：優先順位 4（100000）
- cs5：優先順位 5（101000）
- cs6：優先順位 6（110000）
- cs7：優先順位 7（111000）
- default：000000
- ef：101110

plim qos input map ipv6 tc *tc-value***queue low-latency** コマンドで、*tc-value* に有効な値は次のいずれかです。

- 0 to 63：DiffServ コード ポイント値
- af11：001010
- af12：001100
- af13：001110
- af21：010010
- af22：010100

- af23：010110
- af31：011010
- af32：011100
- af33：011110
- af41：100010
- af42：100100
- af43：100110
- cs1：優先順位 1（001000）
- cs2：優先順位 2（010000）
- cs3：優先順位 3（011000）
- cs4：優先順位 4（100000）
- cs5：優先順位 5（101000）
- cs6：優先順位 6（110000）
- cs7：優先順位 7（111000）
- default：000000
- ef：101110

例

次に、**plim qos input map ip dscp-based** コマンドを使用して、Cisco 10000 シリーズ ルータのスロット 1 の SIP のサブスロット 0 にある SPA で DSCP ベースの分類を有効にする例を示します。

```
Router(config)# interface gigabitethernet 3/0/1
Router(config-if)# plim qos input map ip dscp-based
```

次に、**plim qos input map** コマンドを使用して DSCP ビットの値に応じて着信 IP トラフィックを分類し、Cisco ASR 1000 シリーズ ルータ上の ATM インターフェイスの適切なキューにトラフィックを配置する例を示します。

```
Router# configure terminal
Router(config)# interface ATM0/1/0
Router(config-if)# plim qos input map ip dscp af11 - af12 queue strict-priority
Router(config-if)# plim qos input map ipv6 tc af11 - af12 queue strict-priority
Router(config-if)# plim qos input map mpls exp 7 queue 0
```

関連コマンド

コマンド	説明
card	SIP-600 および SPA を事前にプロビジョニングします。

コマンド	説明
mtu	インターフェイスの最大パケットサイズを設定します。デフォルト値は1500バイトです。設定できる最大の MTU は 9129 バイトです。
negotiation auto	Cisco 10000 SIP-600 上のギガビット イーサネット SPA インターフェイスで、自動ネゴシエーションを有効にします。

plim qos input map cos（VLAN の CoS 値を分類）

QinQ サブインターフェイスの内部または外部 VLAN タグのサービス クラス（CoS）値または CoS 範囲に基づいて、イーサネット共有ポート アダプタ（SPA）で入力トラフィックを高プライオリティ（低遅延）または低プライオリティ（キュー0）に分類するには、サブインターフェイス コンフィギュレーション モードで **plim qos input map cos** コマンドを使用します。CoS ベー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。

内部 VLAN の CoS 値を高プライオリティまたは低プライオリティに分類するための構文
plim qos input map cos {**enable**|**inner-based**|**inner** {*cos-valuecos-range*} **queue** {**strict-priority**|**0**}}
no plim qos input map cos enable

外部 VLAN の CoS 値を高プライオリティまたは低プライオリティに分類するための構文
plim qos input map cos {**enable**|**outer-based**|**outer** {*cos-valuecos-range*} **queue** {**strict-priority**|**0**}}
no plim qos input map cos enable

構文の説明

enable	IEEE 802.1Q CoS ベースの分類を有効にします。
inner-based	内部 VLAN ベースの分類を有効にします。内部 VLAN の CoS 値を設定する前に、まず内部 VLAN ベースの分類を有効にする必要があります。
outer-based	外部 VLAN ベースの分類を有効にします。外部 VLAN の CoS 値を設定する前に、まず外部 VLAN ベースの分類を有効にする必要があります。
inner	内部 VLAN の絶対優先を必要とする CoS の値または範囲を設定できます。
outer	外部 VLAN の絶対優先を必要とする CoS の値または範囲を設定できます。
cos-value	CoS 値を高プライオリティまたは低プライオリティにマッピングしてパケットを分類する内部または外部 VLAN の CoS 値です。
cos-range	CoS 範囲を高プライオリティまたは低プライオリティにマッピングしてパケットを分類する内部または外部 VLAN の CoS 範囲です。
queue	内部または外部 VLAN の CoS 値または CoS 範囲の、高プライオリティまたは低プライオリティへの分類を有効にします。
strict-priority	指定された CoS の値または範囲を高プライオリティ（低遅延）に分類します。
0	指定された CoS の値または範囲を低プライオリティ（キュー0）に分類します。

コマンド デフォルト

外部 VLAN の 6 または 7 の CoS 値は、高プライオリティに分類されます。

コマンド モード

サブインターフェイス コンフィギュレーション モード（config-subif）

コマンド履歴

リリース	変更箇所
Cisco IOS XE Release 3.1S	このコマンドがイーサネット SPA に導入され、Cisco ASR 1000 シリーズ ルータ上の ATM インターフェイスでサポートされました。

内部 VLAN の CoS ベースの分類の設定

内部 VLAN の CoS 値に基づいて入力トラフィックを分類する前に、まず **plimqosinputmapcosinner-based** コマンドを使用して内部 VLAN の CoS ベースの分類を有効にする必要があります。

外部 VLAN の CoS ベースの分類の設定

外部 VLAN の CoS 値に基づいて入力トラフィックを分類する前に、まず **plimqosinputmapcosouter-based** コマンドを使用して外部 VLAN の CoS ベースの分類を有効にする必要があります。

サブインターフェイス レベルでの CoS ベースの分類を無効にし、メイン インターフェイス レベルでのレイヤ 3 情報ベースの分類を有効にするには、サブインターフェイス コンフィギュレーション モードで **noplimqosinputmapcosenable** コマンドを使用します。**noplimqosinputmapcosenable** コマンドを設定すると、メイン インターフェイス レベルの分類設定が適用可能になることを示すメッセージが表示されます。

（注） CSCtd91658 では、外部 VLAN に基づく分類がすでにあるサブインターフェイスで内部 VLAN に CoS ベースの分類を設定しようとした場合（またはその逆を設定しようとした場合）や、存在しない CoS ベースの分類を削除しようとした場合は、警告メッセージが表示されます。

（注） **plimqosinputmapcos** コマンドは、イーサネット SPA でのみサポートされています。**plimqosinputmapcos** コマンドは、QinQ サブインターフェイスの VLAN サブインターフェイス コンフィギュレーション モードから実行されます。

例

次に、内部 VLAN の CoS 値 3 を高プライオリティに分類する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# plim qos input map cos inner-based
Router(config-subif)# plim qos input map cos inner 3 queue strict-priority
```

次に、外部 VLAN の CoS 値 3 を高プライオリティに分類する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# plim qos input map cos outer-based
Router(config-subif)# plim qos input map cos outer 3 queue strict-priority
```

次に、QinQ サブインターフェイス コンフィギュレーション モードで IEEE 802.1Q CoS ベースの分類を有効にする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.2
Router(config-subif)# encapsulation dot1q 2 second-dot1q 100
Router(config-subif)# plim qos input map cos enable
```

次に、QinQ サブインターフェイス コンフィギュレーション モードで IEEE 802.1Q CoS ベースの分類を無効にする例を示します。メイン インターフェイス レベルの分類設定が適用可能になることを示すメッセージが表示されます。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.2
Router(config-subif)# encapsulation dot1q 2 second-dot1q 100
Router(config-subif)# no plim qos input map cos enable
%Classification will now be based on Main interface configuration.
```

次に、Dot1Q サブインターフェイス コンフィギュレーション モードで IEEE 802.1Q CoS ベースの分類を有効にする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# encapsulation dot1Q 1 native
Router(config-subif)# plim qos input map cos enable
```

次に、Dot1Q サブインターフェイス コンフィギュレーション モードで IEEE 802.1Q CoS ベースの分類を無効にする例を示します。メイン インターフェイス レベルの分類設定が適用可能になることを示すメッセージが表示されます。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# encapsulation dot1Q 1 native
Router(config-subif)# no plim qos input map cos enable
%Classification will now be based on Main interface configuration.
```

次に、**plim qos input map** コマンドを使用して DSCP ビットの値に応じて着信 IP トラフィックを分類し、Cisco ASR 1000 シリーズ ルータ上の ATM インターフェイスの適切なキューにトラフィックを配置する例を示します。

```
Router# configure terminal
Router(config)# interface ATM0/1/0
Router(config-if)# plim qos input map ip dscp af11 - af12 queue strict-priority
Router(config-if)# plim qos input map ipv6 tc af11 - af12 queue strict-priority
Router(config-if)# plim qos input map mpls exp 7 queue 0
```

関連コマンド

コマンド	説明
encapsulation	インターフェイスで使用するカプセル化方式を設定します。

police

トラフィック ポリシングを設定するには、ポリシー マップ クラス コンフィギュレーション モードまたはポリシー マップ クラス ポリス コンフィギュレーション モードで **police** コマンドを使用します。トラフィック ポリシングを設定から削除するには、このコマンドの **no** 形式を使用します。

police *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
no police *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

構文の説明

bps	平均レート（ビット/秒）です。有効な値は 8000 ～ 128000000000（128 Gb/s）です。
burst-normal	（任意）バイト単位の通常バースト サイズです。有効な値は 1000 ～ 2000000000（2 Gb）です。デフォルトの通常バースト サイズは 1500 です。
burst-max	（任意）バイト単位の最大バースト サイズです。有効な値は 1000 ～ 2000000000（2 Gb）です。デフォルトはプラットフォームによって異なります。
conform-action	レート制限に適合したパケットに対して実行するアクションを指定します。
exceed-action	レート制限を超過したパケットに対して実行するアクションを指定します。
violate-action	通常および超過バースト サイズに違反するパケットに対して実行するアクションを指定します。

action	

パケットに対して実行するアクションです。次のいずれかのキーワードを指定します。

- **drop**：パケットをドロップします。
- **set-clp-transmit** *value*：ATM セルの 0 から 1 の ATM セル損失率優先度（CLP）を設定し、ATM CLP ビットを 1 に設定してパケットを送信します。
- **set-cos-inner-transmit** *value*：拡張 FlexWAN モジュール、および、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA でブリッジ処理機能の使用時に、ブリッジ処理されたフレームに対するポリシング アクションとして、サービス フィールドの内部クラスを設定します。
- **set-cos-transmit** *value*：サービス クラス（CoS）パケット値を設定し、送信します。
- **set-discard-class-transmit**：パケットの廃棄クラス属性を設定し、設定した新しい廃棄クラスでパケットを送信します。
- **set-dscp-transmit** *value*：IP DiffServ コード ポイント（DSCP）値を設定して、新しい IP DSCP 値でパケットを送信します。
- **set-dscp-tunnel-transmit** *value*：トンネル マーキングのため、レイヤ 2 Tunnel Protocol Version 3（L2TPv3）または Generic Routing Encapsulation（GRE）のトンネル ヘッダーで DSCP の値（0 ～ 63）を設定し、新しい値でパケットを送信します。
- **set-frde-transmit** *value*：フレーム リレー フレーム上のフレーム リレー廃棄適格（DE）ビットを 0 から 1 に設定し、1 に設定した DE ビットが含まれるパケットを送信します。
- **set-mpls-experimental-imposition-transmit** *value*：強制ラベルのヘッダーでマルチプロトコル ラベル スイッチング（MPLS）の EXP ビット（0 ～ 7）を設定し、新しい MPLS EXP ビット値でパケットを送信します。
- **set-mpls-experimental-topmost** *value*：EXP 値を再書き込みします。
- **set-mpls-experimental-topmost-transmit** *value*：入力インターフェイスや出力インターフェイスでの最上位 MPLS ラベル ヘッダーに MPLS EXP フィールド値を設定します。
- **set-prec-transmit** *value*：IP プレシデンスを設定して、新しい IP プレシデンス値でパケットを送信します。
- **set-prec-tunnel-transmit** *value*：トンネル マーキングのため、L2TPv3 または GRE のトンネル ヘッダーで優先順位の値（0 ～ 7）を設定し、新しい値でパケットを送信します。
- **set-qos-transmit** *value*：QoS グループ値を設定し、設定した新しい QoS グ

	ループ値でパケットを送信します。 • **transmit**：パケットを送信します。パケットは変更されません。

コマンド デフォルト

トラフィック ポリシングは設定されません。

コマンド モード

マークされたパケットに適用される単一のアクションを指定する場合は、ポリシー マップ クラス コンフィギュレーション（config-pmap-c）

マークされたパケットに適用される複数のアクションを指定する場合は、ポリシー マップ クラス ポリシング コンフィギュレーション（config-pmap-c-police）

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが Cisco IOS リリース 12.1(5)T に統合されました。 **violate-action** キーワードが追加されました。
12.2(2)T	このコマンドが変更されました。 • *action* 引数の **set-clp-transmit** キーワードが追加されました。 • *action* 引数の **set-frde-transmit** キーワードが追加されました。 （注） ただし、このリリースでは **set-frde-transmit** キーワードは AToM トラフィックではサポートされていません。また、**set-frde-transmit** キーワードは、カプセル化されていない物理インターフェイス上にフレーム リレーが実装されている場合にのみサポートされます。 • action 引数の **set-mpls-experimental-transmit** キーワードが追加されました。
12.2(8)T	このコマンドが、Policer Enhancement（Multiple Actions 機能）のために変更されました。このコマンドが、特定のレートについて適合、超過、または違反しているとマークされたパケットに対して、複数のアクションを適用できるようになりました。
12.2(13)T	このコマンドが変更されました。*action* 引数で、**set-mpls-experimental-transmit** キーワードの名前が **set-mpls-experimental-imposition-transmit** に変更されました。

リリース	変更箇所
12.2(28)SB	このコマンドが変更されました。*action* 引数の **set-dscp-tunnel-transmit** および **set-prec-tunnel-transmit** キーワードが追加されました。これらのキーワードは、Layer 2 Tunnel Protocol Version 3（L2TPv3）トンネル型パケット用です。
12.2(33)SRA	このコマンドが変更されました。拡張 FlexWAN モジュールでマルチポイント ブリッジング（MPB）機能を使用する場合のために、また、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB を使用する場合のために、action 引数に **set-cos-inner-transmit** キーワードが追加されました。
12.2(31)SB2	このコマンドが変更されました。**set-frde-transmit** *action* 引数のサポートが Cisco 10000 シリーズ ルータに追加されました。
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。
12.2(33)SRC	このコマンドが変更されました。Cisco 7600 シリーズ ルータのサポートが追加されました。
12.4(15)T2	Generic Routing Encapsulation（GRE）トンネル型パケットのマーキングのサポートが含まれるように、このコマンドが変更されました。 （注） このリリースでは、GRE トンネル型パケットのマーキングは、Cisco MGX ルート プロセッサ モジュール（RPM-XF）に搭載されているプラットフォームでのみ、サポートされます。
12.2(33)SB	GRE トンネル型パケットのマーキングのサポートと、Cisco 7300 シリーズ ルータのサポートが含まれるように、このコマンドが変更されました。
15.1(1)T	このコマンドが、Cisco ISR 1800、2800、および 3800 シリーズ ルータの SVI インターフェイスでのポリシングをサポートするように変更されました。
12.2(50)SY	このコマンドが変更されました。**set-mpls-experimental-topmost** *value* 引数のサポートが追加されました。
15.0(1)SY	このコマンドが変更されました。*bps*、*burst-normal*、および *burst-max* 引数の最大値が増えました。
Cisco IOS XE リリース 3.5S	このコマンドが変更されました。Cisco ASR 903 ルータのサポートが追加されました。

使用上のガイドライン

police コマンドは、サービス レベル契約への準拠に基づいて、異なる Quality of Service（QoS）値を持つパケットをマークするために使用します。

Cisco IOS リリース 12.2(50)SY では、出力方向で **set-mpls-experimental-topmost** *value* を適用すると、**set-mpls-experimental-imposition** *value* がブロックされます。

（注） Cisco IOS リリース 15.0(1)SY 以降では、バースト サイズを指定せずにポリシー マップを設定すると、デフォルト バースト サイズが 2 Gb/s に達することがあります。

高いレートまたは大きいバーストサイズを設定してから、その設定をサポートしていないCisco IOS ソフトウェア リリースに変更すると、起動時に設定が拒否され、ポリシー マップから **police** コマンドが削除されます。

複数のアクションの指定

police コマンドでは、複数のポリシング アクションを指定できます。**police** コマンドの設定時に複数のポリシング アクションを指定する場合は、次の点に注意してください。

- 同時に最大 4 つのアクションを指定できます。
- **conform-action transmit** と **conform-action drop** などの、矛盾するアクションを指定することはできません。

police コマンドとトラフィック ポリシング機能の使用

police コマンドは、トラフィック ポリシング機能とともに使用することができます。トラフィック ポリシング機能は、トークン バケット アルゴリズムで動作します。Cisco IOS リリース 12.1(5)T には、シングル トークン バケット アルゴリズムと 2 トークン バケット アルゴリズムの 2 種類のトークン バケット アルゴリズムがあります。シングル トークン バケット システムは、**violate-action** オプションを指定しなかった場合に使用され、2 トークン バケット システムは、**violate-action** オプションを指定した場合に使用されます。

Cisco IOS リリース 12.0(5)XE で導入された **police** コマンドのトークン バケット アルゴリズムは、Cisco IOS リリース 12.1(5)T で導入された **police** コマンドのトークン バケット アルゴリズムとは異なります。リリース 12.0(5)XE で導入されたトークン バケット アルゴリズムの詳細については、リリース 12.0(5)XE の『*Traffic Policing*』ドキュメントを参照してください。このドキュメントは、www.cisco.com の（Modular QoS CLI 関連の機能モジュールの下にある）「New Features for 12.0(5)XE」ドキュメント インデックスで利用できます。

次に、Cisco IOS リリース 12.1(5)T で導入されたトークン バケット アルゴリズムの仕組みを説明します。

シングル トークン バケットを使用するトークン バケット アルゴリズム

シングル トークン バケット アルゴリズムは、**police** コマンド CLI で **violate-action** オプションが指定されていない場合に使用されます。

適合バケットは、最初はフル サイズに設定されています（フル サイズは、通常バースト サイズとして指定されているバイト数です）。

指定サイズのパケット（たとえば、「B」バイト）が特定の時間（時間「T」）に到着する場合、次のようなアクションが実行されます。

- 適合バケットでトークンが更新されます。前にパケットが到着したのが T1 で、現在の時間が T の場合、バケットはトークン到着レートに基づいて（T - T1）相当のビット数で更新されます。トークンの到達レートは次のように計算されます。

（パケット間の時間（つまり T - T1）x ポリシング レート）/8 バイト

- 適合バケット B のバイト数がパケット サイズ以上の場合、パケットは適合し、パケットで適合アクションが実行されます。パケットが適合した場合、B バイトが適合バケットから削除されて、そのパケットに対する適合アクションが完了します。
- 適合バケット B のバイト数（制限されているパケット サイズを引いたもの）が 0 未満の場合、超過アクションが実行されます。

2 トークン バケットを使用するトークン バケット アルゴリズム

2 トークン バケット アルゴリズムは、**police** コマンドで **violate-action** オプションが指定されている場合に使用されます。

適合バケットは、最初はフル サイズになっています（フル サイズは、通常バースト サイズとして指定されているバイト数です）。

超過バケットは、最初はフル サイズになっています（フル超過サイズは、最大バースト サイズとして指定されているバイト数です）。

適合および超過トークン バケットのいずれのトークンも、トークン到着レートまたは認定情報レート（CIR）に基づいて更新されます。

指定サイズのパケット（たとえば、「B」バイト）が特定の時間（時間「T」）に到着する場合、次のようなアクションが実行されます。

- 適合バケットでトークンが更新されます。前のパケットが T1 に到達し、現在のパケットが T に到達した場合、バケットはトークン到達レートに基づいて T - T1 に相当するビット数で更新されます。リフィル トークンは、準拠バケットに置かれます。トークンが準拠バケットでオーバーフローになると、超過バケットにオーバーフロー トークンが置かれます。

トークンの到達レートは次のように計算されます。

（パケット間の時間（つまり T-T1）x ポリシング レート）/8 バイト

- 適合バケット B のバイト数がパケット サイズ以上の場合、パケットは適合し、パケットで適合アクションが実行されます。パケットが準拠している場合、B バイトが準拠バケットから削除され、準拠処理が実行されます。このシナリオでは、超過バケットには影響ありません。
- 適合バケット B のバイト数がパケット サイズ未満の場合、超過トークン バケットでパケットによるバイトがチェックされます。適合バケット B のバイト数が 0 以上の場合、超過アクションが実行され、超過トークン バケットから B バイトが削除されます。適合バケットから削除されるバイトはありません。

- 超過バケット B のバイト数がパケット サイズ未満の場合、パケットはレートに違反しているため、違反アクションが実行されます。パケットに対する処理が完了します。

Cisco 7600 シリーズ ルータ上の SIP および SPA の set-cos-inner-transmit アクションの使用

拡張 FlexWAN モジュールで MPB 機能を使用する場合や、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB 機能を使用する場合に、内部 CoS 値をポリシング アクションとしてマーキングすることをサポートするために、Cisco IOS リリース 12.2(33)SRA で **set-cos-inner-transmit** キーワード アクションが導入されました。

このコマンドは、Cisco 7600 SIP-600 ではサポートされていません。

Cisco 7600 シリーズ ルータで、SIP によってサポートされる QoS と **police** コマンドの形式については、『*Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide*』を参照してください。

Cisco ASR 903 ルータでの police コマンドの使用

Cisco ASR 903 ルータで **police** コマンドを使用する場合は、次の制限が適用されます。

- サブインターフェイスでのクラスベース ポリシングはサポートされていません。
- ポリシングは、入力ポリシー マップでのみサポートされています。
- 階層型ポリシング（親レベルと子レベルの両方でのポリシング）はサポートされていません。
- Cisco ASR 903 ルータは、次のアクション キーワードのみをサポートしています。
  - **drop**
  - **set-cos-transmit**
  - **set-discard-class-transmit**
  - **set-dscp-transmit**
  - **set-mpls-exp-imposition-transmit**
  - **set-mpls-exp-topmost-transmit**
  - **set-precp-transmit**
  - **set-qos-transmit**
  - **transmit**

例

シングル トークン バケットを使用するトークン バケット アルゴリズム：例

次の例では、（**class-map** コマンドを使用して）トラフィック クラスを定義し、（**policy-map** コマンドを使用して）トラフィック クラスからの一致基準をサービス ポリシーに設定されているトラフィック ポリシング設定に関連付ける方法を示します。ここで、**service-policy** コマンドはこのサービス ポリシーをインターフェイスに対応付けるために使用されます。

この特定の例では、トラフィック ポリシングは平均レート 8000 ビット/秒で設定され、ファスト イーサネット インターフェイス 0/0 から発信される全パケットに対して通常バースト サイズが 1000 バイトとなります。

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

この例では、初期トークン バケットはフルの 1000 バイトで開始します。450 バイトのパケットを受信すると、準拠トークン バケットに使用可能なバイトが十分あるため、パケットは準拠しています。パケットにより準拠処理（送信）が実行され、450 バイトが準拠トークン バケットから削除されます（残り 550 バイト）。

次のパケットが 0.25 秒後に到着すると、250 バイトがトークン バケットに追加され（（0.25 × 8000）/8）、トークン バケットには 800 バイトが残ります。次のパケットが 900 バイトの場合、パケットが超過して超過アクション（ドロップ）が実行されます。トークン バケットから取り出されるバイトはありません。

2 トークン バケットを使用するトークン バケット アルゴリズム：例

この例では、トラフィック ポリシングは平均レート 8000 ビット/秒で設定され、ファスト イーサネット インターフェイス 0/0 から発信される全パケットに対して通常バースト サイズが 1000 バイト、超過バースト サイズが 1000 バイトとなります。

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action
set-qos-transmit 1 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

この例では、初期トークン バケットはフルの 1000 バイトで開始します。450 バイトのパケットを受信すると、準拠トークン バケットに使用可能なバイトが十分あるため、パケットは準拠しています。パケットにより準拠処理（送信）が実行され、450 バイトが準拠トークン バケットから削除されます（残り 550 バイト）。

次のパケットが 0.25 秒後に到着すると、250 バイトが準拠トークン バケットに追加され（（0.25 × 8000）/8）、準拠トークン バケットには 800 バイトが残ります。次のパケットが 900 バイトの場合、準拠トークン バケットでは 800 バイトしか使用できないため、パケットは準拠していません。

（超過バースト サイズで指定された）フルの 1000 バイトで始まる超過トークン バケットに、使用可能なバイトがあるかどうかがチェックされます。超過トークン バケットには使用可能なバイトが十分あるため、超過アクション（QoS 送信値を 1 に設定）が

実行され、超過バケットから 900 バイトが取られ、超過トークン バケットの残りは 100 バイトになります。

次のパケットが 0.40 秒後に到達し、トークン バケットに 400 バイトが追加されます（(.40 X 8000)/8）。これで、適合トークン バケットは 1000 バイト（適合バケットで使用可能な最大トークン数）になり、200 バイトが適合トークン バケットをオーバーフローします（適合トークン バケットの容量を満たすのに 200 バイトだけが必要であったため）。これらのオーバーフローバイトは、超過トークン バケットに置かれ、超過トークン バケットに 300 バイト与えられます。

着信パケットが 1000 バイトの場合、準拠トークン バケットで使用可能なバイト数が十分あるため、パケットは準拠します。パケットにより準拠処理（送信）が実行され、1000 バイトが準拠トークン バケットから削除されます（残り 0 バイト）。

次のパケットが 0.20 秒後に到達し、トークン バケットに 200 バイトが追加されます（(.20 X 8000)/8）。これで、準拠バケットの中身は 200 バイトになります。着信パケットが 400 バイトの場合、準拠トークン バケットでは 200 バイトしか使用できないため、パケットは準拠していません。同様に、超過バケットで使用可能なバイト数は 300 バイトだけなので、パケットは超過しません。したがって、パケットは違反となり、違反処理（ドロップ）が実行されます。

MPLS EXP 値への適合：例

次の例は、パケットがレート制限に適合する場合に、MPLS EXP フィールドが 5 に設定されることを示しています。パケットがレート制限を超える場合は、MPLS EXP フィールドが 3 に設定されます。

```
Router(config)# policy-map input-IP-dscp
Router(config-pmap)# class dscp24
Router(config-pmap-c)# police 8000 1500 1000 conform-action
set-mpls-experimental-imposition-transmit 5 exceed-action
set-mpls-experimental-imposition-transmit 3
Router(config-pmap-c)# violate-action drop
```

Cisco 7600 シリーズ ルータ上の SIP および SPA のアクションとしての内部 CoS 値の設定：例

次に、仮想 LAN（VLAN）100 のすべてのトラフィックをクラス「vlan-inner-100」にフィルタリングし、vlan-inner-100 クラスのトラフィック シェーピング ポリシーを確立する QoS クラスの設定例を示します。このサービス ポリシーは、トラフィックの平均レートを 500 kb/s に制限して、1000 バイトの通常バーストと 1500 バイトの最大バーストを使用し、内部 CoS 値を 3 に設定します。内部 CoS 値の設定はブリッジング機能を使用する場合に限ってサポートされるので、**bridge-domain** コマンドを使用して VLAN 100 にトラフィックをブリッジングする ATM SPA インターフェイスの相手先固定接続（PVC）に出力ポリシーとして適用されるサービス ポリシーも示します。

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
```

```
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap)# class vlan-inner-100
Router(config-pmap-c)# police 500000 1000 1500 conform-action set-cos-inner-transmit 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm3/0/0
Router(config-if)# pvc 100/100
Router(config-if-atm-vc)# bridge-domain 100 dot1q
Router(config-if-atm-vc)# service-policy output vlan-inner-100
Router(config-if-atm-vc)# end
```

関連コマンド

コマンド	説明
bridge-domain	RFC 1483 ATM ブリッジングまたは RFC 1490 フレーム リレー ブリッジングで、ブリッジ処理された VLAN の ATM PVC またはフレーム リレー データリンク接続識別子（DLCI）へのマップを有効にします。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
service-policy	インターフェイスに付加するサービスポリシーの名前を指定します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

police (EtherSwitch)

分類したトラフィックにポリサーを定義するには、ポリシーマップ クラス コンフィギュレーション モードで **police** コマンドを使用します。既存のポリサーを削除するには、このコマンドの **no** 形式を使用します。

police {*bps*|**cir** *bps*} [{*burst-byte*|**bc** *burst-byte*}] **conform-action transmit** [**exceed-action** {**drop**|**dscp** *dscp-value*}]
no police {*bps*|**cir** *bps*} [{*burst-byte*|**bc** *burst-byte*}] **conform-action transmit** [**exceed-action** {**drop**|**dscp** *dscp-value*}]

構文の説明

bps | **cir** *bps*	1 秒あたりのビット数（bps）単位の平均トラフィック レートまたは認定情報レート（CIR）です。 10/100 ポートの場合、範囲は 1000000 ～ 100000000 で、粒度は 1 Mbps です。 ギガビット対応イーサネット ポートの場合、範囲は 8000000 ～ 128000000000（128 Gbps）です。16 Mbps を超えるポリサーの粒度はレートの 0.1% で、16 Mbps を下回るポリサーの粒度は 8 Mbps です。
burst-byte | **bc** *burst-byte*	（任意）バイト単位の通常バースト サイズまたはバースト カウントです。有効な値は 1000 ～ 2000000000（2 Gb）です。
conform-actiontransmit	レート制限に適合するパケットを送信します。
exceed-actiondrop	（任意）指定されたレートを超えた場合は、スイッチがパケットをドロップするように指定します。
exceed-actiondscp *dscp-value*	（任意）指定されたレートを超えた場合は、スイッチがパケットの DiffServ コード ポイント（DSCP）を指定された *dscp-value* に変更し、パケットを送信するよう指定します。

コマンド デフォルト

ポリサーは定義されません。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが変更されました。このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに実装されました。

リリース	変更箇所
12.3(4)T	このコマンドが変更されました。このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに実装されました。
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。
15.0(1)SY	このコマンドが変更されました。*burst-byte* 引数の最大値が増えました。

使用上のガイドライン

入力側ファスト イーサネット ポートでは、最大 6 個のポリサーを設定できます。

入力ギガビット対応イーサネット ポートでは、最大 60 個のポリサーを設定できます。

出力側ファスト イーサネットおよびギガビット対応イーサネット ポートでは、ポリサーを設定することはできません。

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

設定を確認するには、**showpolicy-map** 特権 EXEC コマンドを使用します。

例

次の例では、トラフィックが平均レート 1 Mbps、バースト サイズ 65536 バイトを超えないときに DSCP 値を 46 に設定し、トラフィックがこれらの条件を超えるとパケットを廃棄するポリサーを設定する方法を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip dscp 46
Router(config-pmap-c)# police 1000000 65536 conform-action transmit exceed-action drop
Router(config-pmap-c)# end
```

関連コマンド

コマンド	説明
policy-map	複数のインターフェイスに適用できるポリシー マップを作成または変更し、ポリシーマップ コンフィギュレーション モードを開始します。
showpolicy-map	QoS ポリシー マップを表示します。

police（percent）

インターフェイスで利用可能な帯域幅のパーセンテージに基づいてトラフィック ポリシングを設定するには、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 **police** コマンドを使用します。トラフィック ポリシングを設定から削除するには、このコマンドの **no** 形式を使用します。

police cir percent *percentage* [*burst-in-msec*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percentage*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
no police cir percent *percentage* [*burst-in-msec*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percentage*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
police cir percent *percent* [*burst-in-msec*] [**bc** *conform-burst-in-msec* **ms**] [**pir** *percent*] [**be** *peak-burst-in-msec* **ms**] [**conform-action action**] [**exceed-action action**] [**violate-action action**]
no police cir percent *percent* [*burst-in-msec*] [**bc** *conform-burst-in-msec* **ms**] [**pir** *percent*] [**be** *peak-burst-in-msec* **ms**] [**conform-action action**] [**exceed-action action**] [**violate-action action**]

構文の説明

cir	情報レートを指定します。CIR がトラフィック ポリシングに使用されることを示します。
percent	帯域幅の割合を使用して CIR を計算するように指定します。
percentage	帯域幅のパーセンテージです。有効値の範囲は 1 ～ 100 です。
burst-in-msec	（任意）ミリ秒単位でのバースト。有効な範囲は1～2000の数字です。
bc	（任意）最初のトークン バケットでトラフィック ポリシングに使用される適合バースト（bc）サイズを指定します。
conform-burst-in-msec	（任意）ミリ秒単位の bc 値です。有効な範囲は 1 ～ 2000 の数字です。
ms	（任意）バーストの値がミリ秒単位で指定されていることを示します。
be	（任意）2番目のトークン バケットでトラフィック ポリシングに使用されるピーク バースト（be）サイズを指定します。
peak-burst-in-msec	（任意）ミリ秒単位の be サイズです。有効な範囲は 1 ～ 2000 の数字です。
pir	（任意）最大情報レート（PIR）がトラフィック ポリシングに使用されることを示します。
percent	（任意）PIR の計算に使用される帯域幅のパーセンテージです。
conform-action	（任意）適合バーストよりレートが小さいパケットで実行されるアクション。**conform-action** を指定する前に、peak-burst-in-msec の値を指定する必要があります。

exceed-action	（任意）適合バースト内および適合バーストに超過バーストを加えたレートのパケットで実行されるアクションを指定します。
violate-action	（任意）適合バーストに超過バーストを加えたレートよりレートが超過しているパケットで実行されるアクションを指定します。violate-action を指定する前に、exceed-action を指定する必要があります。
action	（任意）パケットに対して実行するアクションです。次のいずれかのキーワードを指定します。 **サポートされているすべてのプラットフォーム** • **drop**：パケットをドロップします。 • **set-clp-transmit**：ATM セルの 0 から 1 の ATM セル損失率優先度（CLP）を設定して、ATM CLP ビットを 1 に設定してパケットを送信します。 • **set-dscp-transmit** *new-dscp*：IP DiffServ コード ポイント（DSCP）の値を設定して、新しい IP DSCP 値設定でパケットを送信します。 • **set-frde-transmit**：フレーム リレー フレーム上のフレーム リレー廃棄適正（DE）ビットを 0 から 1 に設定して、1 に設定した DE ビットが含まれるパケットを送信します。 • **set-prec-transmit** *new-prec*：IP プレシデンスを設定して、その新しい IP プレシデンス値設定でパケットを送信します。 • **transmit**：パケットをそのまま無変更で送信します。 **Cisco 10000 シリーズ ルータ以外でサポートされるプラットフォーム** • **policed-dscp-transmit**：（超過アクションと違反アクションのみ）ポリシングされる DSCP マップごとに DSCP の値を変更し、パケットを送信します。 • **set-cos-inner-transmit** *value*：拡張 FlexWAN モジュール、および Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 と Cisco 7600 SIP-400 の SPA でブリッジング機能の使用時に、ブリッジ処理されたフレームに対するポリシング アクションとして、サービス フィールドの内部クラスを設定します。 • **set-cos-transmit** *value*：パケットのサービス クラス（CoS）の値を設定して、パケットを送信します。 • **set-mpls-exposition-transmit**：マルチプロトコル ラベル スイッチング（MPLS）の EXP ビットを 0 から 7 に設定して、新しい MPLS EXP ビット値設定でパケットを送信します。 • **set-mpls-topmost-transmit**：最上位ラベルにある MPLS EXP ビットを設定して、パケットを送信します。

action (continued)	**Cisco 10000 シリーズ ルータ** • **drop**：パケットをドロップします。 • **set-clp-transmit** *value*：ATM セルの 0 から 1 の ATM セル損失率優先度（CLP）を設定し、ATM CLP ビットを 1 に設定してパケットを送信します。 • **set-cos-inner-transmit** *value*：拡張 FlexWAN モジュール、および Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 と Cisco 7600 SIP-400 の SPA でブリッジング機能の使用時に、ブリッジ処理されたフレームに対するポリシング アクションとして、サービス フィールドの内部クラスを設定します。 • **set-cos-transmit** *value*：パケットの COS 値を設定して、送信します。 • **set-discard-class-transmit**：パケットの廃棄クラス属性を設定して、新しい廃棄クラス設定でパケットを送信します。 • **set-dscp-transmit** *value*：IP DiffServ コードポイント（DSCP）値を設定して、新しい IP DSCP 値設定でパケットを送信します。 • **set-frde-transmit** *value*：フレーム リレー フレーム上のフレーム リレー廃棄適格（DE）ビットを 0 から 1 に設定して、1 に設定した DE ビットが含まれるパケットを送信します。 • **set-mpls-experimental-imposition-transmit** *value*：強制ラベルのヘッダーでマルチプロトコル ラベル スイッチング（MPLS）の Experimental（EXP）ビット（0 ～ 7）を設定して、新しい MPLS EXP ビット値設定でパケットを送信します。 • **set-mpls-experimental-topmost-transmit** *value*：入力インターフェイスや出力インターフェイスでの最上位 MPLS ラベル ヘッダーに、MPLS EXP フィールド値を設定します。 • **set-prec-transmit** *value*：IP プレシデンスを設定して、新しい IP プレシデンス値設定でパケットを送信します。 • **set-qos-transmit** *value*：Quality of Service（QoS）グループの値を設定して、新しい QoS グループ値設定でパケットを送信します。有効な値は 0 ～ 99 です。 • **transmit**：パケットを送信します。パケットは変更されません。

コマンド デフォルト

デフォルトの **bc** および **be** の値は 4 ms です。

conform-action のデフォルト アクションは transmit です。

exceed-action および **violate-action** のデフォルト アクションは drop です。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.0(25)SX	このコマンドが変更されました。パーセントベース ポリシング機能が、Cisco 10000 シリーズ ルータに追加されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.2(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.2(13)T	このコマンドは、パーセントベース ポリシング機能とシェーピング機能のために、変更されました。
12.0(28)S	このコマンドが Cisco IOS Release 12.0(28)S に統合されました。
12.2(18)SXE	このコマンドが Cisco IOS Release 12.2(18)SXE に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが変更されました。拡張 FlexWAN モジュールでマルチポイントブリッジング（MPB）機能を使用する場合のために、また、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB を使用する場合のために、action 引数に **set-cos-inner-transmit** キーワードが追加されました。
12.2(31)SB2	このコマンドが変更されました。PRE3 で、Cisco 10000 シリーズ ルータの **set-frde-transmit** action 引数が追加されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。
15.0(1)SY	このコマンドが変更されました。CIR および PIR の最大値が増えました。

使用上のガイドライン

このコマンドでは、インターフェイスで利用可能な最大帯域幅の割合に基づいて CIR および PIR を計算します。ポリシー マップがインターフェイスに対応付けられている場合、ビット/秒（bps）単位の等価 CIR および PIR 値が、インターフェイス帯域幅とこのコマンドで入力したパーセント値に基づいて計算されます。その後、**showpolicy-mapinterface** コマンドを使用して、計算された bps レートを確認できます。

計算された CIR および PIR の bps レートは、8000 ～ 128000000000 bps（128 Gbps）の範囲内でなければなりません。レートがこの範囲外の場合、関連ポリシーマップをインターフェイスに対応付けることができません。インターフェイス帯域幅が変更された場合（帯域幅が追加された場合など）、改訂された帯域幅に基づいて CIR および PIR の bps 値が再計算されます。ポリ

シーマップをインターフェイスに対応付けたあとにCIRおよびPIRの割合が変更された場合、CIR および PIR の bps 値が再計算されます。

また、このコマンドでは、適合バースト サイズとピーク バースト サイズの値をミリ秒単位で指定することもできます。帯域幅を割合として計算する場合は、適合バーストサイズとピークバースト サイズをミリ秒単位で指定する必要があります。

ポリシーマップは、トップ（または「親」）レベルおよびセカンダリ（または「子」）レベルの、2 つのレベルの（ネストされた）階層で設定できます。**police** (percent) コマンドは、親ポリシー マップまたは子ポリシー マップのいずれかで使用するために設定できます。

police (percent) コマンドにより、帯域幅のパーセンテージを計算する参照ポイントとして、使用可能な帯域幅の最大レートが使用されます。子ポリシーマップで **police** (percent) コマンドが設定されている場合、**police** (percent) コマンドにより、次に上位のレベルにあるポリシー（この場合は、親ポリシー マップ）で指定されている帯域幅量が使用されます。親ポリシー マップで使用可能な最大帯域幅レートが指定されていない場合、**police** (percent) コマンドにより、次に上位のレベルにあるポリシー（この場合は、物理インターフェイスで、階層の最高ポイント）で使用可能な最大帯域幅レートが、参照ポイントとして使用されます。**police** (percent) コマンドでは、帯域幅の参照ポイントとして、次に上位のレベルが常に参照されます。次に、このポイントについての設定例を示します。

```
Policymap parent_policy
 class parent
  shape average 512000
  service-policy child_policy
Policymap child_policy
 class normal_type
  police cir percent 30
```

この設定例では、parent_policy と child_policy の 2 つの階層ポリシーがあります。child_policy と呼ばれるポリシー マップでは、normal_type と呼ばれるクラスで police コマンドが設定されました。このクラスでは、**police** (percent) コマンドによって指定されたパーセンテージは 30% です。コマンドにより、parent_policy にある親クラスの帯域幅参照ポイントとして、512 kbps というピーク レートが使用されます。**police** (percent) コマンドでは、cir レート（512 kbps * 30%）の計算の根拠として、512 kbps が使用されます。

```
interface serial 4/0
 service-policy output parent_policy
Policymap parent_policy
 class parent
  bandwidth 512
  service-policy child_policy
```

前述の例では、parent_policy と呼ばれる 1 つのポリシーマップがあります。このポリシーマップでは、ピーク レートが指定されていません。**bandwidth** コマンドが使用されましたが、このコマンドは使用可能な帯域幅の最大レートを表しません。したがって、**police** (percent) コマンドでは、帯域幅の参照ポイントを取得する目的で、次に上位のレベル（この場合は、シリアル インターフェイス 4/0）が参照されます。シリアル インターフェイス 4/0 の帯域幅が 1.5 Mbps とすると、**police** (percent) コマンドでは、cir レート（1500000 * 30%）の計算の根拠として、1.5 Mbps が使用されます。

police (percent) コマンドは、しばしば **bandwidth** コマンドと **priority** コマンドとの組み合わせで使用されます。**bandwidth** コマンドと **priority** コマンドを使用すると、エンティティ（たとえば、物理インターフェイスなど）で使用可能な帯域幅の合計量を計算できます。**bandwidth** コマンドと **priority** コマンドを使用して、エンティティで使用可能な帯域幅の合計量を計算する場合は、次の注意事項に従ってください。

- エンティティが物理インターフェイスの場合、合計帯域幅は、物理インターフェイス上の帯域幅です。
- エンティティが整形 ATM 相手先固定接続（PVC）の場合、合計帯域幅は、次のように計算されます。
  - 可変ビット レート（VBR）の仮想回線（VC）の場合、計算には、平均セル レート（SCR）が使用されます。
  - 使用可能ビット レート（ABR）の VC の場合、計算には、最小セル レート（MCR）が使用されます。

帯域幅割り当ての詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Congestion Management Overview」の章を参照してください。

Cisco 7600 シリーズ ルータ上の SIP および SPA の set-cos-inner-transmit アクションの使用

拡張 FlexWAN モジュールで MPB 機能を使用する場合や、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB 機能を使用する場合に、内部 CoS 値をポリシング アクションとしてマーキングすることをサポートするために、Cisco IOS Release 12.2(33)SRA で **set-cos-inner-transmit** キーワード アクションが導入されました。

このコマンドは、Cisco 7600 SIP-600 ではサポートされていません。

Cisco 7600 シリーズ ルータで、SIP によってサポートされる QoS と **police** コマンドの形式の詳細については、『*Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide*』を参照してください。

例

次に、帯域幅の割合（%）に基づいた CIR と PIR を使用してトラフィック ポリシングを設定する例を示します。この例では、CIR に 20 %、PIR に 40 % が指定されています。オプションの bc 値と be 値（それぞれ、300 ms、400 ms）も指定されています。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40

Router(config-pmap-c-police)# exit
```

次の例に示したように、ポリシー マップとクラス マップの設定後、ポリシー マップがインターフェイスに付加されます。

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/0
```

```
Router(config-if)# service-policy input policy1
Router(config-if)# exit
```

Cisco 7600 シリーズ ルータ上の SIP および SPA のアクションとしての内部 CoS 値の設定

次に、仮想 LAN（VLAN）100 のすべてのトラフィックをクラス vlan-inner-100 にフィルタリングし、vlan-inner-100 クラスのトラフィック シェーピング ポリシーを確立する QoS クラスの設定例を示します。サービス ポリシーで CIR は 20%、PIR は 40% にトラフィックを制限し、適合バースト（bc）を 300 ms、ピーク バースト（be）を 400 ms とし、インナー CoS 値を 3 に設定します。内部 CoS 値の設定はブリッジング機能を使用する場合に限ってサポートされるので、**bridge-domain** コマンドを使用して VLAN 100 にトラフィックをブリッジングする ATM 共有ポート アダプタ（SPA）インターフェイスの相手先固定接続（PVC）に、出力ポリシーとして適用されるサービス ポリシーも示します。

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40
conform-action set-cos-inner-transmit 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm3/0/0
Router(config-if)# pvc 100/100
Router(config-if-atm-vc)# bridge-domain 100 dot1q
Router(config-if-atm-vc)# service-policy output vlan-inner-100
Router(config-if)# end
```

次に、プライオリティ サービスに police (percent) コマンドを設定する例を示します。この例では、New-Traffic という名前のポリシー マップで、Voice という名前のプライオリティ クラスが設定されています。このルータは、音声トラフィックに認定レートの 25% を割り当て、4 ms の認定バーストと 1 ms の超過バーストを許可します。このルータは、認定レートに適合する音声トラフィックを送信して、バースト サイズを超える音声トラフィックの QoS 送信値を 4 に設定し、認定レートに違反する音声トラフィックをドロップします。

```
Router(config)# policy-map New-Traffic
Router(config-pmap)# class Voice
Router(config-pmap-c)# priority
Router(config-pmap-c)# queue-limit 32
Router(config-pmap-c)# police percent 25 4 ms 1 ms conform-action transmit exceed-action
 set-qos-transmit 4 violate-action drop
```

関連コマンド

コマンド	説明
bandwidth(policy-mapclass)	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。

コマンド	説明
bridge-domain	RFC 1483 ATM ブリッジングまたは RFC 1490 フレーム リレー ブリッジングで、ブリッジ処理された VLAN の ATM PVC またはフレーム リレー DLCI へのマップをイネーブルにします。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
priority	ポリシーマップのトラフィック クラスに、プライオリティを付与します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
shape(percent)	インターフェイスで使用可能な帯域幅の割合（%）に基づいて、平均レート トラフィック シェーピングとピーク レート トラフィック シェーピングを指定します。
showpolicy-map	指定されたサービス ポリシーマップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

police（ポリシー マップ）

インターフェイスごとにポリサーを作成し、ポリシーマップ クラスを設定して使用するには、ポリシーマップ クラス コンフィギュレーション モードで **police** コマンドを使用します。ポリシーマップ クラスからインターフェイスごとのポリサーを削除するには、このコマンドの **no** 形式を使用します。

police *bps* [**[bc]** *normal-burst-bytes* [{*maximum-burst-bytes*|**[be]** [*burst-bytes*]}]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
no police *bps*
police aggregate *name*
no police aggregate *name*
police cir *bps* [[*bc*] *normal-burst-bytes* [{*maximum-burst-bytes*|**[be]** [*burst-bytes*]}]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
no police cir *bps*
police cir percent *percent* [*burst* **ms [be]** [*burst* **ms**]] [**pir percent** *percent* [**be** *burst* **ms**]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
no police cir *percent*
police flow *bps* [*normal-burst-bytes*] [**conform-action** *action* [**exceed-action** *action*]]
police flow mask {**dest-only**|**full-flow**|**src-only**} *bps* [*normal-burst-bytes*] [**conform-action** *action* [**exceed-action** *action*]]
no police flow

構文の説明

bps	ビット/秒（bps）単位でのターゲット ビット レート。ポストフィックスの値は、小数点として、**k**、**m** および **g** を使用できます。有効な範囲は 8000（または 8k）～ 128000000000（または 128 Gbps）です。
normal-burst-bytes	（任意）バーストを処理するための、バイト単位での CIR トークン バケット サイズ。有効な値は 1000 ～ 2000000000（2 Gb）です。
maximum-burst-bytes	（任意）バーストを処理するための、バイト単位での PIR トークン バケット サイズ。有効な値は 1000 ～ 2000000000（2 Gb）です。
burst-bytes	（任意）バーストを処理するための、バイト単位でのトークン バケット サイズ。有効な値は 1000 ～ 2000000000（2 Gb）です。
bc	（任意）使用可能な（適合）バースト サイズをバイト単位でサイズを指定します。
be	（任意）使用可能な超過バースト サイズをバイト単位でサイズを指定します。
pir	（任意）最大情報レート（PIR）を指定します。
cir	認定情報レート（CIR）を指定します。

conform-action アクション	（任意）レート リミットに適合するパケットで実行されるアクションを指定します。*action* 引数で有効な値については、「使用上のガイドライン」セクションを参照してください。
exceed-action アクション	（任意）*maximum-burst-bytes* 引数での指定レートよりもパケット レートが大きい場合に、パケットで実行されるアクションを指定します。*action* 引数で有効な値については、「使用上のガイドライン」セクションを参照してください。
violate-action アクション	（任意）*maximum-burst-bytes* 引数での指定レートよりもパケット レートが大きい場合に実行されるアクションを指定します。*action* 引数で有効な値については、「使用上のガイドライン」セクションを参照してください。
aggregate 名前	前に定義した集約ポリサーの名前を指定し、指定された集約ポリサーで使用するポリシー マップ クラスを設定します。
percent パーセント	使用可能なインターフェイス帯域幅の割合（%）を指定します。有効な範囲は 1 ～ 100 です。
バースト	（任意）バーストを処理するための、ミリ秒（ms）単位でのトークン バケット サイズです。有効な範囲は 1 ～ 2000 です。
ms	ミリ秒を示します。帯域幅をパーセンテージで指定する場合、*burst* 引数の次に、このキーワードを指定する必要があります。
flow	各フローをポリシングするマイクロフロー ポリサーを指定します。
mask	ポリシングに使用するフロー マスクを指定します。
dest-only	宛先だけのフロー マスクを指定します。
full-flow	フルフロー マスクを指定します。
src-only	発信元だけのフロー マスクを指定します。

コマンド デフォルト

ポリシングは実行されません。

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドが Supervisor Engine 720 に導入されました。
12.2(17d)SXB	このコマンドが、Cisco IOS Release 12.2(17d)SXB に統合され、Supervisor Engine 2 に実装されました。

リリース	変更箇所
12.2(17d)SXB3	このコマンドが変更されました。FlexWAN インターフェイスでのみ、**police** *bps* の最小レートが 32,000 から 8,000 に下げられました。
12.2(18)SXD	このコマンドが次のように変更されました。 • **conform-action** キーワードの有効な値に **set-mpls-exp-topmost-transmit** が追加されました。 • **set-mpls-exp-transmit** キーワードが **set-mpls-exp-imposition-transmit** に変更されました。
12.2(18)SXE	このコマンドが変更されました。10 ギガビット イーサネットをサポートするため、bps の最大レートが、4,000,000,000 bps から 10,000,000,000 bps に増加されました。
12.2(18)SXF	このコマンドが変更されました。CIR の最大レートが、10,000,000,000 bps に増加されました。
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。
12.2(31)SB	このコマンドが変更されました。コマンドの動作が変更され、ポリシング アクションは変更せずにポリシング レート パラメータだけを変更する場合、ポリシング アクションのデフォルト アクションは、conform-action transmit、exceed-action drop、および violate-action drop になりました。これは、PRE3 用の Cisco 10000 シリーズ ルータに実装されました。
12.2(33)SB	このコマンドが変更されました。コマンドの動作が変更され、ポリシング アクションは変更せずにポリシング レート パラメータだけを変更する場合、ポリシング アクションが保存されます。これは、PRE3 用と PRE4 用の Cisco 10000 シリーズ ルータに実装されました。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(33)SXH2	このコマンドが変更されました。CIR の最大レートが、64,000,000,000 bps に増加されました。
12.2(33)SXI	このコマンドが変更されました。CIR の最小トークン バケット サイズが、1 バイトに削減されました。
15.0(1)SY	このコマンドが変更されました。*normal-burst-bytes*、*maximum-burst-bytes*、および *burst-bytes* 引数の最大値が 2 Gb に増えました。bps 引数の最大値が 128 Gb に増えました。

使用上のガイドライン

Cisco IOS Release 12.2(17d)SXB3 では、FlexWAN インターフェイスのみ *bps* 引数の範囲は、8,000 ～ 4,000,000,000 bps です。

名前付き集約ポリサーを作成するには、**mlsqosaggregate-policer** *name* コマンドを使用します。

名前付きとインターフェイスごとの、2 つのタイプの集約ポリサーを作成できます。両方のタイプとも、次のように、複数のポートに付加できます。

- **mlsqosaggregate-policer** コマンドを使用して、名前付き集約ポリサーを作成します。名前付き集約ポリサーを複数の入力ポートに対応付けると、そのポリサーが付加された全入力ポートからの一致するトラフィックがポリシングされます。
- ポリシーマップ クラスにあるインターフェイスごとの集約ポリサーは、**police** コマンドを使用して定義します。インターフェイス別集約ポリサーを複数の入力ポートに対応付けると、各入力ポート上の一致するトラフィックが個別にポリシングされます。

名前付き集約ポリサーの使用をクリアするには、**nopoliceaggregate** *name* コマンドを使用します。

マイクロフロー ポリサーを定義するには、**policeflow** コマンドを入力します（ARP トラフィックには、マイクロフロー ポリシングは適用できません）。

インターフェイスごとの（名前付きではない）集約ポリサーを定義するには、**police** コマンドを入力します。

トラフィックが集約とマイクロフローの両方でポリシングされている場合、集約とマイクロフローの両方のポリサーは同じポリシーマップ クラスにあり、それぞれで **conform-action** キーワードおよび **exceed-action** キーワードを使用する必要があります。

アクション引数の値

action 引数の有効値は、次のとおりです。

- **drop**：*bps* 引数に設定されているレートを超えないパケットをドロップします。
- **set-clp-transmit**：ATM セル損失率優先度（CLP）を設定し、送信します。
- **set-cos-inner-transmit{** *new- cos*}：*new-cos* 引数の新しい内部サービス クラス（CoS）の値に一致するトラフィックにマーク付けします。*new-cos* 引数の有効値の範囲は 0 ～ 7 です。
- **set-cos-transmit{** *new- cos*}：*new-cos* 引数の新しい CoS の値に一致するトラフィックにマーク付けします。*new-cos* 引数の有効値の範囲は 0 ～ 7 です。
- **set-cos-transmit**：ATM セル損失率優先度（CLP）を設定し、送信します。
- **set-dscp-transmit{** *dscp-bit-pattern* **|** *dscp-value* **|default|ef}**：新しい DSCP の値に一致するトラフィックにマーク付けします。
  - *dscp-bit-pattern*：DSCP ビット パターンを指定します。表 1 に、有効な値のリストを示します。
  - *dscp-value*：DSCP の値を指定します。有効な値は 0 ～ 63 です。
  - **default**：パケットをデフォルト DSCP 値（000000）と一致させます。
  - **ef**：Expedited Forwarding（EF）Per-Hop Behavior（PHB）DSCP の値（101110）とパケットが一致します。

表 *29 :* 有効な *DSCP* ビット パターンの値

キーワード	定義
af11	パケットが AF11 DSCP（001010）と一致します。
af12	パケットが AF12 DSCP（001100）と一致します。
af13	パケットが AF13 DSCP（001110）と一致します。
af21	パケットが AF21 DSCP（010010）と一致します。
af22	パケットが AF22 DSCP（010100）と一致します。
af23	パケットが AF23 DSCP（010110）と一致します。
af31	パケットが AF31 DSCP（011010）と一致します。
af32	パケットが AF32 DSCP（011100）と一致します。
af33	パケットが AF33 DSCP（011110）と一致します。
af41	パケットが AF41 DSCP（100010）と一致します。
af42	パケットが AF42 DSCP（100100）と一致します。
af43	パケットが AF43 DSCP（100110）と一致します。
cs1	パケットが CS1（Precedence 1）DSCP（001000）と一致します。
cs2	パケットが CS2（Precedence 2）DSCP（010000）と一致します。
cs3	パケットが CS3（Precedence 3）DSCP（011000）と一致します。
cs4	パケットが CS4（Precedence 4）DSCP（100000）と一致します。
cs5	パケットが CS5（Precedence 5）DSCP（101000）と一致します。
cs6	パケットが CS6（Precedence 6）DSCP（110000）と一致します。
cs7	パケットが CS7（Precedence 7）DSCP（111000）と一致します。

- **set-frde-transmit**：フレーム リレー廃棄適性（FR DE）ビットを設定し、送信します。これは、**exceed-action** *action* キーワードと引数との組み合わせで有効です。
- **set-mpls-exp-imposition-transmit** *new-mpls-exp*：強制ラベル エントリのマルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）ビットを再書き込みして、ビットを送信します。*new-mpls-exp* 引数により、ポリシーマップによって定義される MPLS EXP ビットの設定に使用される値が指定されます。*new-mpls-exp* 引数の有効値の範囲は 0 ～ 7 です。

- **set-mpls-exp-topmost-transmit**：最上位ラベルにある EXP ビットを設定し、パケットを送信します。

（注） **set-mpls-exp-topmost-transmit** キーワードは、Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの一部のリリースではサポートされていません。

- **set-prec-transmit** *new-precedence* [**exceed-action**]：新しい IP プレシデンスの値に一致するトラフィックにマーク付けし、送信します。*new-precedence* 引数の有効値の範囲は 0 ～ 7 です。このアクションには、**exceed-action** キーワードを付けることもできます。
- **set-qos-transmit**：qos-group を再書き込みし、パケットを送信します。
- **transmit**：*bps* 引数に設定されているレートを超えないパケットを送信します。**transmit** キーワードのオプションのキーワードと引数の組み合わせは、**exceed-action** *action* です。

続くキーワードが指定されない場合、デフォルト アクションは、次のとおりです。

- **conform-action** は **transmit**
- **exceed-action** は **drop**
- **violate-action** は **drop**

Cisco 10000 シリーズ ルータ

Cisco IOS Release 12.2(31)SB よりも前のリリースでは、ポリシング レート パラメータを変更してアクション パラメータを変更しない場合、アクション パラメータはデフォルトのアクションに戻ります。

たとえば、次の設定例は、test という名前のポリシー マップで設定された **police** コマンドを示しています。適合するトラフィック、超過するトラフィック、および違反するトラフィックのポリシング アクションが、set-clp-transmit に設定されます。その後、ポリシング レート パラメータがそれぞれ 500000、250、および 200 に変更されますが、アクションは変更されません。test ポリシーマップを再度表示すると、ポリシングアクションはそれぞれデフォルトの transmit、drop、および drop になっています。

```
Router# show policy-map test
Policy Map test
Class prec1
police 248000 100 10 conform-action set-clp-transmit exceed-action set-clp-transmit
violate-action set-clp-transmit
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map test
Router(config-pmap)# class prec1
Router(config-pmap-c)# police 500000 250 200
Router(config-pmap-c)# end
Router# show policy-map test
Policy Map test
Class prec1
police 500000 250 200 conform-action transmit exceed-action drop violate-action drop
```

Cisco IOS Release 12.2(33)SB 以降のリリースは、デュアル ポリシング アクションとポリシング サブモードをサポートしています。そのため、レート パラメータのみを変更するために **police** コマンドを使用した場合、ポリシング アクションはデフォルトのアクションにならず、以前のアクションが保持されます。

たとえば、次の設定例は、test という名前のポリシー マップの prec1 という名前のトラフィック クラスで設定された **police** コマンドを示しています。ポリシング レートが指定され、ポリシング サブモードでポリシング アクションが指定されます。ポリシング レート パラメータのみを変更した後は、ポリシング アクションはデフォルトにならず、元の設定が保持されます。

```
Router# show policy-map test
Policy Map test
Class prec1
police 248000 1000 100
conform-action set-clp-transmit
exceed-action set-clp-transmit
violate-action set-clp-transmit
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map test
Router(config-pmap)# class prec1
Router(config-pmap-c)# police 500000 100 200
Router(config-pmap-c)# end
Router# show policy-map test
Policy Map test
Class prec1
police 500000 100 200
conform-action set-clp-transmit
exceed-action set-clp-transmit
violate-action set-clp-transmit
```

例

次に、前に定義した集約ポリサーの名前を指定し、指定された集約ポリサーで使用するポリシー マップ クラスを設定します。

```
Router(config-pmap-c)# police aggregate agg1
```

次に、クラスマップ access-match を使用する、police-setting という名前のポリシーマップを作成する例を示します。これは、受信する IP precedence の値を信頼するよう設定され、証明書信頼リストの集約ポリサーおよびマイクロフロー ポリサーで設定されます。

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 1000000000 200000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
class-map	QoS クラス マップ コンフィギュレーション モードにアクセスし、QoS クラス マップを設定します。
mlsqosaggregate-policer	ポリシー マップで使用するために、名前付き集約ポリサーを定義します。
police	トラフィック ポリシングを、QoS ポリシー マップ クラス コンフィギュレーション モードまたは QoS ポリシー マップ クラス ポリシング コンフィギュレーション モードで設定します。
service-policy	ポリシー マップをインターフェイスに付加します。
showclass-map	クラス マップ情報を表示します。
showpolicy-map	ポリシー マップ情報を表示します。
showpolicy-mapinterface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

police（2 つのレート）

認定情報レート（CIR）と最大情報レート（PIR）の 2 つのレートを使用してトラフィック ポリシングを設定するには、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 **police** コマンドを使用します。2 レート トラフィック ポリシングを設定から削除するには、このコマンドの **no** 形式を使用します。

police cir *cir* [**bc** *conform-burst*] [**pir** *pir*] [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
no police cir

構文の説明

cir	最初のトークン バケットが更新される認定情報レート（CIR）を指定します。
cir	ビット/秒単位の CIR 値です。値は 8000 ～ 128000000000（128 Gbps）までの数字です。
bc	（任意）最初のトークン バケットでポリシングに使用される適合バースト（bc）サイズを指定します。
conform-burst	（任意）バイト単位の bc 値です。値は 1000 ～ 2000000000（2 Gb）までの数字です。
pir	（任意）2 番目のトークン バケットが更新される最大情報レート（PIR）を指定します。
pir	（任意）ビット/秒単位の PIR 値です。値は 8000 ～ 128000000000（128 Gbps）までの数字です。
be	（任意）2 番目のトークン バケットでポリシングに使用されるピーク バースト（be）サイズを指定します。
peak-burst	（任意）バイト単位のピーク バースト（be）サイズです。サイズは、使用する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。
conform-action	（任意）CIR および PIR に適合するパケットに対して実行するアクションを指定します。
exceed-action	（任意）PIR に適合するものの CIR には適合しないパケットに対して実行するアクションを指定します。
violate-action	（任意）PIR を超過するパケットに対して実行するアクションを指定します。

action	（任意）パケットに対して実行するアクションを指定します。次のいずれかのキーワードを指定します。 • **drop**：パケットをドロップします。 • **set-clp-transmit**：ATM セルの 0 から 1 の ATM セル損失率優先度（CLP）を設定して、ATM CLP ビットを 1 に設定してパケットを送信します。 • **set-cos-inner-transmit** *value*：拡張 FlexWAN モジュール、および Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 と Cisco 7600 SIP-400 の SPA でブリッジング機能の使用時に、ブリッジ処理されたフレームに対するポリシングアクションとして、サービス フィールドの内部クラスを設定します。 • **set-dscp-transmit** *new-dscp*：IP DiffServ コードポイント（DSCP）の値を設定して、新しい IP DSCP 値設定でパケットを送信します。 • **set-dscp-tunnel-transmit** *value*：トンネル マーキングのため、レイヤ 2 Tunnel Protocol Version 3（L2TPv3）または Generic Routing Encapsulation（GRE）トンネル型パケットのトンネル ヘッダーで DSCP の値（0 ～ 63）を設定して、新しい値でパケットを送信します。 • **set-frde-transmit**：フレーム リレー フレーム上のフレーム リレー廃棄適正（DE）ビットを 0 から 1 に設定して、1 に設定した DE ビットが含まれるパケットを送信します。 • **set-mpls-exp-transmit** ：マルチプロトコル ラベル スイッチング（MPLS）の EXP ビットを 0 から 7 に設定して、新しい MPLS EXP ビット値設定でパケットを送信します。 • **set-prec-transmit** *new-prec*：IP プレシデンスを設定して、その新しい IP プレシデンス値設定でパケットを送信します。 • **set-prec-tunnel-transmit** *value*：トンネル マーキングのため、L2TPv3 または GRE トンネル型パケットのトンネル ヘッダーで優先順位の値（0 ～ 7）を設定して、新しい値でパケットを送信します。 • **set-qos-transmit** *new-qos*：Quality of Service（QoS）グループの値を設定して、新しい QoS グループ値設定でパケットを送信します。 • **transmit**：パケットをそのまま無変更で送信します。

コマンド デフォルト

2 つのレートを使用するトラフィック ポリシングがディセーブルにされます。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。

リリース	変更箇所
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが変更されました。**violate-action** キーワードが追加されました。
12.2(2)T	このコマンドが変更されました。*action* 引数に次のキーワードが追加されました。 • **set-clp-transmit** • **set-frde-transmit** • **set-mpls-exp-transmit**
12.2(4)T	このコマンドが変更されました。2 レート トラフィック ポリシングに対応するために、**cir** および **pir** キーワードが追加されました。
12.2(28)SB	このコマンドが変更されました。*action* 引数の **set-dscp-tunnel-transmit** および **set-prec-tunnel-transmit** キーワードが追加されました。これらのキーワードは、Layer 2 Tunnel Protocol Version 3（L2TPv3）トンネル型パケット用です。
12.2(33)SRA	このコマンドが変更されました。拡張 FlexWAN モジュールでマルチポイント ブリッジング（MPB）機能を使用する場合のために、また、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB を使用する場合のために、action 引数に **set-cos-inner-transmit** キーワードが追加されました。
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。
12.2(33)SRC	このコマンドが、Cisco マルチレイヤ スイッチ フィーチャ カード 3（MSFC3）に搭載されている Cisco 7600 シリーズ ルータをサポートするために変更されました。
12.4(15)T2	Generic Routing Encapsulation（GRE）トンネル型パケットのマーキングのサポートが含まれるように、このコマンドが変更されました。 （注） このリリースでは、GRE トンネル型パケットのマーキングは、Cisco MGX ルート プロセッサ モジュール（RPM-XF）に搭載されているプラットフォームでのみ、サポートされます。
12.2(33)SB	GRE トンネル型パケットのマーキングのサポートと、Cisco 7300 シリーズ ルータのサポートが含まれるように、このコマンドが変更されました。
12.4(20)T	このコマンドが変更されました。モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）を使用した階層型キューイング フレームワーク（HQF）のサポートが追加されました。
15.0(1)SY	このコマンドが変更されました。*cir*、*conform-burst*、および *pir* 引数の最大値が増えました。

使用上のガイドライン

明示的なポリシング レートでのプライオリティの設定

明示的なポリシング レートでプライオリティ クラスを設定する場合、輻輳条件に関係なく、トラフィックはポリシング レートに限定されます。つまり、帯域幅が使用可能な場合、プライオリティ トラフィックは、明示的なポリサーで指定されたレートを超えることはできません。

トークン バケット

2 レート トラフィック ポリシングでは、2 つの独立したレートでのトラフィックのポリシングに、2 つのトークン バケット（Tc と Tp）を使用します。2 つのトークン バケットに関して次の点に注意してください。

- Tc トークン バケットは、パケットが 2 レート ポリサーで到着するたびに CIR 値で更新されます。Tc トークン バケットには、適合バースト（Bc）値まで含めることができます。
- Tp トークン バケットは、パケットが 2 レート ポリサーで到着するたびに PIR 値で更新されます。Tp トークン バケットには、ピーク バースト（Be）値まで含めることができます。

トークン バケットの更新

次のシナリオは、トークン バケットの更新方法について説明したものです。

B バイトのパケットは時間 t に着信します。最後のパケットは時間 t1 に着信しました。時間 t での CIR と PIR トークン バケットは、それぞれ Tc(t) および Tp(t) で表されます。これらの値をこのシナリオで使用する場合、トークン バケットは次のように更新されます。

$Tc(t) = \min(CIR \times (t-t1) + Tc(t1), Bc)$

$Tp(t) = \min(PIR \times (t-t1) + Tp(t1), Be)$

トラフィックのマーキング

2 レート ポリサーは、指定レートに適合しているか、超過しているか、または違反しているとしてパケットをマークします。次のポイント（B バイトのパケットを使用）は、パケットがどのようにマークされるかを示しています。

- B > Tp(t) の場合、パケットは指定レートに違反しているとマークされます。
- B > Tc(t) の場合、パケットは指定レートを超過しているとマークされ、Tp(t) トークン バケットは Tp(t) = Tp(t) - B として更新されます。

これ以外の場合、パケットは指定レートに適合しているとマークされ、Tc(t) および Tp(t) のトークン バケットが次のように更新されます。

$Tp(t) = Tp(t) - B$

$Tc(t) = Tc(t) - B$

たとえば、CIR が 100 kbps、PIR が 200 kbps で、250 kbps のレートのデータ ストリームが 2 レート ポリサーで到着した場合、パケットは次のようにマークされます。

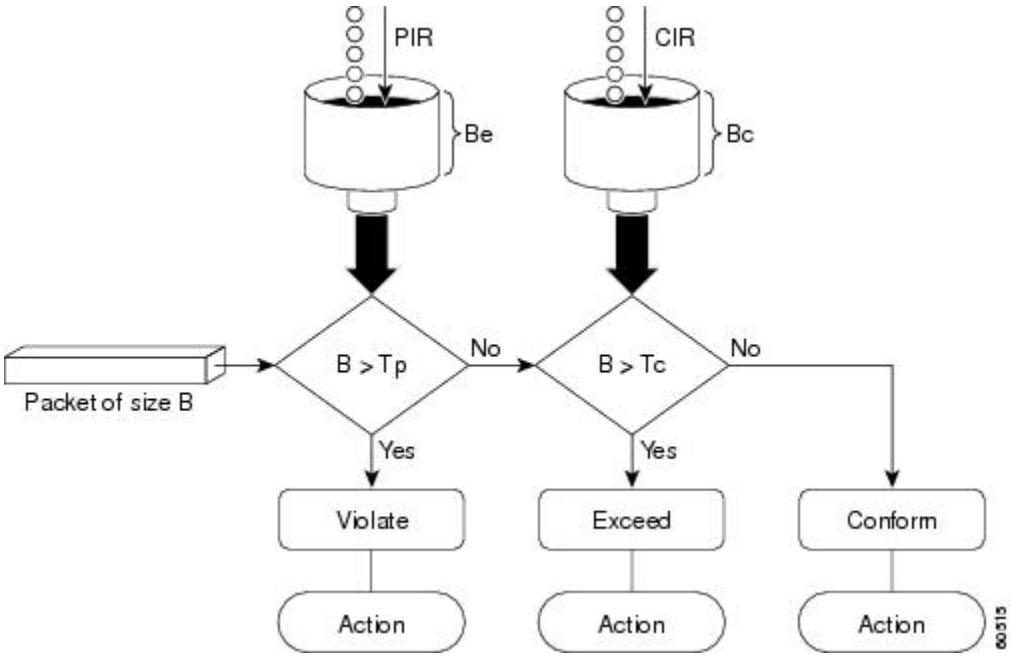
- 100 kbps は、レートに適合しているとマークされます。
- 100 kbps は、レートを超過しているとマークされます。

• 50 kbps は、レートに違反しているとマークされます。

パケットのマーキングとアクションの割り当てのフローチャート

この図のフローチャートは、2 レート ポリサーによるパケットのマーキング方法と、パケットへの対応アクション（違反、超過、または適合）の割り当て方法を示したものです。

図 *31 : 2* レート ポリサーでのパケットのマーキングとアクションの割り当て



Cisco 7600 シリーズ ルータ上の SIP および SPA の set-cos-inner-transmit アクションの使用

拡張 FlexWAN モジュールで MPB 機能を使用する場合や、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB 機能を使用する場合に、内部 CoS 値をポリシング アクションとしてマーキングすることをサポートするために、Cisco IOS Release 12.2(33)SRA で **set-cos-inner-transmit** キーワード アクションが導入されました。

このコマンドは、Cisco 7600 SIP-600 ではサポートされていません。

Cisco 7600 シリーズ ルータで、SIP によってサポートされる QoS と **police** コマンドの形式については、『*Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide*』を参照してください。

例

明示的なポリシング レートでのプライオリティの設定

次に、ネットワークの輻輳条件に関係なく、プライオリティ トラフィックが 1000 kbps の認定レートに限定される例を示します。

```
Router(config)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# police cir 1000000 conform-action transmit exceed-action drop
```

2 レート ポリシング機能

次の例では、500 kbps の平均認定レートと 1 Mbps のピーク レートにトラフィックを限定するために、2 レート トラフィック ポリシングがクラスに設定される例を示します。

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
 transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1
 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
```

平均認定レート（500 kbps）に準拠するとしてマークされたトラフィックは、そのまま送信されます。500 kbps を超過しているものの 1 Mbps は超過していないとマークされたトラフィックは、IP precedence 2 でマークされてから送信されます。1 Mbps を超過しているとマークされたトラフィックはすべてドロップされます。バースト パラメータは 10000 バイトに設定されています。

次に、1.25 Mbps のトラフィックがポリサー クラスに送信（「提供」）される例を示します。

```
Router# show policy-map interface serial3/0
 Serial3/0
  Service-policy output: policy1
   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps
   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
```

2 レート ポリサーにより、500 kbps のトラフィックが指定レートに適合とマークされ、500 kbps のトラフィックが指定レートを超過とマークされ、250 kbps のトラフィックが指定レートに違反とマークされます。レートに適合しているとマークされたパケットはそのまま送信され、レートを超過しているとマークされたパケットは IP precedence

2 でマークされてから送信されます。レートに違反しているとマークされたパケットはドロップされます。

Cisco 7600 シリーズ ルータ上の SIP および SPA のアクションとしての内部 CoS 値の設定：例

次に、仮想 LAN（VLAN）100 のすべてのトラフィックをクラス「vlan-inner-100」にフィルタリングし、vlan-inner-100 クラスのトラフィック シェーピング ポリシーを確立する QoS クラスの設定例を示します。このサービス ポリシーは、500 kbps の平均認定レートと 1 Mbps のピーク レートにトラフィックを制限し、内部 CoS 値を 3 に設定します。内部 CoS 値の設定はブリッジング機能を使用する場合に限ってサポートされるので、**bridge-domain** コマンドを使用して VLAN 100 にトラフィックをブリッジングする ATM SPA インターフェイスの相手先固定接続（PVC）に、出力ポリシーとして適用されるサービス ポリシーも示します。

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
set-cos-inner-transmit 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm3/0/0
Router(config-if)# pvc 100/100
Router(config-if-atm-vc)# bridge-domain 100 dot1q
Router(config-if-atm-vc)# service-policy output vlan-inner-100
Router(config-if-atm-vc)# end
```

関連コマンド

コマンド	説明
bridge-domain	RFC 1483 ATM ブリッジングまたは RFC 1490 フレーム リレー ブリッジングで、ブリッジ処理された VLAN の ATM PVC またはフレーム リレー DLCI へのマップをイネーブルにします。
police	トラフィック ポリシングを設定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
service-policy	ポリシー マップを入力インターフェイスまたは出力インターフェイスに付加して、そのインターフェイスのサービス ポリシーとして使用します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。

コマンド	説明
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

police rate（コントロールプレーン）

コントロールプレーンを宛先とするトラフィックのトラフィック ポリシングを設定するには、QoS ポリシーマップ クラス コンフィギュレーション モードまたはコントロール プレーン コンフィギュレーション モードで、**policerate** コマンドを使用します。トラフィック ポリシングを設定から削除するには、このコマンドの **no** 形式を使用します。

police rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action action**]
no police rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action action**]

パケット/秒（pps）の場合の構文
police rate units pps [**burst burst-in-packets packets**] [**peak-rate peak-rate-in-pps pps**] [**peak-burst peak-burst-in-packets packets**]
no police rate units pps [**burst burst-in-packets packets**] [**peak-rate peak-rate-in-pps pps**] [**peak-burst peak-burst-in-packets packets**]

バイト/秒（bps）の場合の構文
police rate *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]
no police rate *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]

割合の構文
police rate percent *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]
no police rate percent *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]

Cisco 10000 シリーズ ルータの場合の構文
police rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action action**] [**exceed-action action**] [**violate-action action**]
no police rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action action**] [**exceed-action action**] [**violate-action action**]

SIP-400 搭載の Cisco 7600 シリーズ ルータの場合の構文
police rate *units* [{**pps burst** *burst-in-packets* **packets**|**bps burst burst-in-bytes bytes**}]
no police rate *units* [{**pps burst** *burst-in-packets* **packets**|**bps burst** *burst-in-bytes* **bytes**}]

構文の説明

units	ポリシング レートです。ポリシング レートが pps 単位で指定される場合、値の有効な範囲は次のとおりです。 • Cisco 10000 シリーズ ルータ：有効な範囲は 1 ～ 500000 です。 • Cisco SIP-400 搭載の Cisco 7600 シリーズ ルータ：有効な範囲は 1 ～ 100 です。 • その他のプラットフォーム：有効な範囲は 1 ～ 2000000 です。 ポリシング レートが bps 単位で指定される場合、値の有効な範囲は次のとおりです。 • Cisco SIP-400 搭載の Cisco 7600 シリーズ ルータ：有効な範囲は 80 ～ 8000 です。 • その他のプラットフォーム：有効な範囲は 8000 ～ 128000000000（128 Gbps）です。
pps	トラフィックがポリシングされるレートの決定に使用されるパケット/秒（pps）を指定します。
burst *burst-in-packets* **packets**	（任意）トラフィック ポリシングに使用されるバースト レートをパケット単位で指定します。値の有効な範囲は次のとおりです。 • Cisco 10000 シリーズ ルータ：有効な範囲は 1 ～ 25000 です。 • Cisco SIP-400 搭載の Cisco 7600 シリーズ ルータ：有効な範囲は 1 ～ 1000 です。 • その他のプラットフォーム：有効な範囲は 1 ～ 512000 です。
peak-rate *peak-rate-in-pps* **pps**	（任意）トラフィック ポリシングと PIR の計算に使用される最大情報レート（PIR）を指定します。値の有効な範囲は次のとおりです。 • Cisco 10000 シリーズ ルータ：有効な範囲は 1 ～ 500000 です。 • その他のプラットフォーム：有効な範囲は 1 ～ 512000 です。
peak-burst *peak-burst-in-packets* **packets**	（任意）トラフィック ポリシングに使用されるピーク バースト値をパケット単位で指定します。値の有効な範囲は次のとおりです。 • Cisco 10000 シリーズ ルータ：有効な範囲は 1 ～ 25000 です。 • その他のプラットフォーム：有効な範囲は 1 ～ 512000 です。
bps	（任意）トラフィックがポリシングされるレートの決定に使用されるビット/秒（bps）を指定します。

burst *burst-in-bytes* **bytes**	（任意）トラフィック ポリシングに使用されるバースト レートをバイト単位で指定します。値の有効な範囲は次のとおりです。 • Cisco SIP-400 搭載の Cisco 7600 シリーズ ルータ：有効な範囲は 100 ～ 10000 です。 • その他のプラットフォーム：有効な範囲は 1000 ～ 2000000000（2 Gb）です。
peak-rate *peak-rate-in-bps* **bps**	（任意）ピーク レートのピーク レート値をバイト単位で指定します。有効な範囲は 1000 ～ 512000000 です。
peak-burst *peak-burst-in-bytes* **bytes**	（任意）トラフィック ポリシングに使用されるピーク バースト値をバイト単位で指定します。有効な範囲は 1000 ～ 2000000000（2 Gb）です。
percent	トラフィックがポリシングされるレートを決定するために使用されるインターフェイス帯域幅のパーセンテージを指定します。
percentage	帯域幅のパーセンテージです。有効な範囲は 1 ～ 100 です。
burst *ms* **ms**	（任意）トラフィック ポリシングに使用されるバースト レートをミリ秒単位で指定します。有効な範囲は 1 ～ 2000 です。
peak-ratepercent *percentage*	（任意）PIR の決定に使用されるインターフェイス帯域幅のパーセンテージを指定します。有効な範囲は 1 ～ 100 です。
peak-burst *ms* **ms**	（任意）トラフィック ポリシングに使用されるピーク バースト レートをミリ秒単位で指定します。有効な範囲は 1 ～ 2000 です。
conform-action *action*	（任意）ポリシング レート リミットに適合するパケットで実行されるアクションを指定します。指定可能なアクションについては、「使用上のガイドライン」セクションを参照してください。
exceed-action *action*	（任意）レート リミットを超過するパケットで実行されるアクションを指定します。指定可能なアクションについては、「使用上のガイドライン」セクションを参照してください。
violate-action *action*	（任意）ポリシング レート リミットを継続的に超過するパケットで実行されるアクションを指定します。指定可能なアクションについては、「使用上のガイドライン」セクションを参照してください。

コマンド デフォルト

無効

コマンド モード

QoS ポリシーマップ クラス コンフィギュレーション（config-pmap）

コントロール プレーン コンフィギュレーション（config-cp）

コマンド履歴

リリース	変更箇所
12.3(7)T	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが変更されました。このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
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。
12.2(31)SB2	このコマンドが Cisco IOS Release 12.2(31)SB2 に統合され、Cisco 10000 シリーズルータに実装されました。
12.2(33)SRC	このコマンドが、Cisco 7600 SIP-400 での CoPP 拡張をサポートするように変更されました。
15.0(1)SY	このコマンドが変更されました。*burst-in-bytes*、*peak-burst-in-bytes*、および *units* 引数の最大値が増えました。

使用上のガイドライン

パケット/秒（pps）、バイト/秒（bps）、またはインターフェイス帯域幅のパーセンテージでコントロールプレーンを宛先とするトラフィックを制限するには、**police rate** コマンドを使用します。

policerate コマンドが発行される場合で、レートが指定されていない場合、コントロールプレーンを宛先とするトラフィックは bps に基づいてポリシングされます。

次の表に、*action* 引数で指定できるアクションのリストを示します。

表 *30 : action* 引数の値

アクション	説明
drop	パケットをドロップします。これは、認定ポリシング レートを超過するか、認定ポリシング レートに違反するトラフィックに対するデフォルト アクションです。
set-clp-transmit *value*	ATM セルで、ATM セル損失率優先度（CLP）ビットを設定します。有効な値は、0 または 1 です。
set-discard-class-transmit *value*	パケットの廃棄クラス属性を設定し、設定した新しい廃棄クラスでパケットを送信します。有効な値は 0 ～ 7 です。
set-dscp-transmit *value*	IP Diffserv コード ポイント（DSCP）の値を設定し、設定した新しい IP DSCP 値でパケットを送信します。有効な値は 0 ～ 63 です。
set-dscp-tunnel-transmit *value*	トンネル パケット DSCP を再書き込みし、新しい DSCP の値でパケットを送信します。有効な値は 0 ～ 63 です。

アクション	説明
set-frde-transmit *value*	フレームリレーフレーム上のフレームリレー廃棄適格（DE）ビットを 0 から 1 に設定し、1 に設定した DE ビットが含まれるパケットを送信します。
set-mpls-exp-imposition-transmit *value*	強制ラベルのヘッダーでマルチプロトコル ラベル スイッチング（MPLS）の EXP ビットを設定し、設定した新しい MPLS EXP ビット値でパケットを送信します。有効な値は 0 ～ 7 です。
set-mpls-exp-transmit *value*	入力インターフェイス、出力インターフェイス、または両方の MPLS ラベル ヘッダーで、MPLS EXP フィールドの値を設定します。有効な値は 0 ～ 7 です。
set-prec-transmit *value*	IP precedence を設定し、設定した新しい IP precedence 値でパケットを送信します。有効な値は 0 ～ 7 です。
set-prec-tunnel-transmit *value*	トンネル パケットの IP precedence を設定し、設定した新しい IP precedence 値でパケットを送信します。有効な値は 0 ～ 7 です。
set-qos-transmit *value*	QoS グループを設定し、設定した新しい QoS グループ値でパケットを送信します。有効な値は 0 ～ 63 です。
transmit	パケットを送信します。パケットは変更されません。

例

次に、ポリシング レート リミットに適合するパケットで実行されるアクションを設定する例を示します。

```
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
Router(config)# access-list 140 permit tcp any any eq telnet
Router(config)# class-map match-any pps-1
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map copp-pps
Router(config-pmap)# class pps-1
Router(config-pmap)# police rate 10000 pps burst 100 packets peak-rate 10100 pps peak-burst
 150 packets conform-action transmit
Router(config-cmap)# exit
Router(config)# control-plane
Router(config-cp)# service-policy input copp-pps
Router(config-cp)# exit
```

関連コマンド

コマンド	説明
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

コマンド	説明
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。

police rate pdp

ポリシング レートを使用してパケット データ プロトコル（PDP）トラフィック ポリシングを設定するには、ポリシーマップ クラス コンフィギュレーション モードまたはポリシーマップ クラス ポリシング コンフィギュレーション モードで、**policeratepdp** コマンドを使用します。PDP トラフィック ポリシングを設定から削除するには、このコマンドの **no** 形式を使用します。

police rate pdp [**burst** *bytes*] [**peak-rate pdp** [**peak-burst** *bytes*]] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
no police rate pdp [**burst** *bytes*] [**peak-rate pdp** [**peak-burst** *bytes*]] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

構文の説明

burst *bytes*	（任意）認定バースト サイズをバイト単位で指定します。サイズは、使用する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。有効な範囲は 1000 ～ 2000000000（2 Gb）です。デフォルトは 1500 です。
peak-ratepdp	（任意）PDP トラフィックのポリシング時に、セッションのピーク レートが考慮されるように指定します。
peak-burst *bytes*	（任意）ピーク バースト サイズをバイト単位で指定します。サイズは、使用する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。有効な範囲は 1000 ～ 2000000000（2 Gb）です。デフォルトは 2500 です。
conform-action	適合バーストを下回るレートのパケットに対して実行するアクションを指定します。
exceed-action	適合バーストを超えるレートのパケットに対して実行するアクションを指定します。
violate-action	（任意）適合バーストを違反するレートのパケットに対して実行するアクションを指定します。
action	パケットに対して実行するアクションです。次のいずれかのキーワードを指定します。 • **drop**：パケットをドロップします。 • **set-dscp-transmit** *new-dscp-value*：IP DiffServ コード ポイント（DSCP）値を設定して、新しい IP DSCP 値でパケットを送信します。 • **set-prec-transmit** *new-prec-value*：IP プレシデンスを設定して、その新しい IP プレシデンス値でパケットを送信します。 • **transmit**：パケットをそのまま無変更で送信します。

コマンド デフォルト

PDP トラフィック ポリシングは無効になっています。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）
ポリシーマップ クラス ポリシング コンフィギュレーション（config-pmap-c-police）

コマンド履歴

リリース	変更箇所
12.3(8)XU	このコマンドが導入されました。
12.3(11)YJ	このコマンドが、Cisco IOS Release 12.3(11)YJ に組み込まれました。
12.3(14)YQ	このコマンドが、Cisco IOS Release 12.3(14)YQ に組み込まれました。
12.4(9)T	このコマンドが Cisco IOS Release 12.4(9)T に統合されました。
15.0(1)SY	このコマンドが変更されました。*bytes* 引数の最大値が増えました。

使用上のガイドライン

policeratepdp コマンドは、Cisco IOS Release 12.4(9)T で使用できる Flow-Based QoS for GGSN 機能に含まれています。

Flow-Based QoS for GGSN 機能は、Gateway General Packet Radio Service（GPRS）Support Node（GGSN）専用に設計されています。

PDP ごとのポリシング

Flow-Based QoS for GGSN 機能には、PDP ごとのポリシング（セッションベースのポリシング）が含まれています。

PDP ごとのポリシングは Gateway GPRS Support Node トラフィック コンディショナ（3G TS 23.107）の機能の 1 つで、特定の PDP コンテキストの Gi インターフェイス上で受信されるトラフィックの最大レートを制限するために使用できます。

このポリシング機能は、PDP コンテキストにコール アドミッション制御（CAC）ネゴシエーション データ レートを適用します。輻輳が発生した場合に、不適合トラフィックをドロップするか、または不適合トラフィックを優先ドロップとしてマーキングするように GGSN を設定できます。

使用されるポリシング パラメータは、次のように PDP コンテキストに依存します。

- R99 Quality of Service（QoS）プロファイルを持つ GTPv1 PDP の場合、CAC ネゴシエーション QoS プロファイルの最大ビット レート（MBR）および保証ビット レート（GBR）パラメータが使用されます。非リアルタイム トラフィックの場合、MBR パラメータだけが使用されます。
- R98 QoS プロファイルを持つ GTPv1 PDP および GTPv0 PDP の場合、CAC ネゴシエーション QoS ポリシーのピーク スループット パラメータが使用されます。

PDP ごとのポリシングを設定する前に、次の点に注意してください。

- GGSN で、Universal Mobile Telecommunications System（UMTS）QoS マッピングが有効になっている必要があります。

- Gi インターフェイスで、Cisco Express Forwarding（CEF）が有効になっている必要があります。
- ダウンリンク トラフィック用に PDP ごとのポリシングがサポートされるのは、Gi インターフェイスにおいてだけです。
- PDP コンテキストの初期パケットは、ポリシングされません。
- 階層型ポリシングはサポートされません。
- フローベースのポリシングを Access Point Network（APN）にアタッチされているポリシー マップ内で設定した場合、**showpolicy-mapapn** コマンドによって、ポリシングの前に受信されたパケットの総数が表示され、ポリシング カウンタは表示されません。

（注） **showpolicy-mapapn** コマンドによって表示されたポリシング カウンタをクリアするには、**cleargprsaccess-pointstatistics***access-point-index* コマンドを使用します。

- APN に適用されているサービス ポリシーは変更できません。サービス ポリシーを変更するには、APN からサービス ポリシーを削除し、サービス ポリシーを変更してから再適用します。
- それぞれに **matchflowpdp** が設定され、異なる DiffServ コード ポイント（DSCP）値が指定されている複数のクラスマップは、DSCP が信頼されている（**gprsumts-qosdscpunmodified** グローバル コンフィギュレーション コマンドが GGSN 上で設定されていない）場合にのみ、ポリシー マップでサポートされます。

詳細情報

GGSN の詳細と、Flow-Based QoS for GGSN 機能の設定手順については、『*Cisco GGSN Release 6.0 Configuration Guide*』、Cisco IOS Release 12.4(2)XB を参照してください。

（注） Flow-Based QoS for GGSN 機能を設定するには、「Configuring Per-PDP Policing」セクションの手順に従います。

showpolicy-mapapn コマンド、**gprsumts-qosdscpunmodified** コマンド、**cleargprsaccess-pointstatistics** コマンド、およびその他の GGSN 固有のコマンドの詳細については、『*Cisco GGSN Release 6.0 Command Reference*』、Cisco IOS Release 12.4(2)XB を参照してください。

例

次に、APN に適用される PDP ごとのポリシングのポリシー マップの例を示します。

```
class-map match-all class-pdp
 match flow pdp
!
! Configures a policy map and attaches this class map to it.
policy-map policy-gprs
```

```
 class class-pdp
  police rate pdp
    conform-action set-dscp-transmit 15
    exceed-action set-dscp-transmit 15
    violate-action drop
! Attaches the policy map to the APN.

gprs access-point-list gprs
  access-point 1
   access-point-name static
   service-policy input policy-gprs
```

関連コマンド

コマンド	説明
cleargprsaccess-pointstatistics	GGSN 上の特定のアクセス ポイントまたはすべてのアクセス ポイントの統計カウンタをクリアします。
gprsumts-qosdscpunmodified	加入者データグラムが、DSCP を変更することなしに GTP パスを介して転送されるように指定します。
matchflowpdp	PDP フローを、クラス マップ内の一致基準として指定します。
showpolicy-mapapn	APN にアタッチされているすべての入力および出力ポリシーの統計情報と設定情報を表示します。

policy-map

ポリシー マップ コンフィギュレーション モードを開始し、サービス ポリシーを指定する 1 つまたは複数のインターフェイスにアタッチ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。ポリシーマップを削除するには、このコマンドの **no** 形式を使用します。

Cisco 10000 および Cisco 7600 シリーズ ルータ以外でサポートされるプラットフォーム
policy-map [**type** {**stack**|**access-control**|**port-filter**|**queue-threshold**|**logging** *log-policy*}] *policy-map-name*
no policy-map [**type** {**stack**|**access-control**|**port-filter**|**queue-threshold**|**logging** *log-policy*}] *policy-map-name*

Cisco 10000 シリーズ ルータ
policy-map [**type** {**control**|**service**}] *policy-map-name*
no policy-map [**type** {**control**|**service**}] *policy-map-name*

Cisco CMTS、および 7600 シリーズ ルータ
policy-map [**type** {**class-routing ipv4 unicast** *unicast-name*|**control** *control-name*|**service** *service-name*}] *policy-map-name*
no policy-map [**type** {**class-routing ipv4 unicast** *unicast-name*|**control** *control-name*|**service** *service-name*}] *policy-map-name*

構文の説明

type	（任意）ポリシー マップ タイプを指定します。
stack	（任意）該当するプロトコル スタックで検索する完全一致パターンを決定します。
access-control	（任意）Flexible Packet Matching（FPM）機能用のポリシー マップをイネーブルにします。
port-filter	（任意）ポート フィルタ機能用のポリシー マップをイネーブルにします。
queue-threshold	（任意）キューのしきい値機能用のポリシーマップをイネーブルにします。
logging	（任意）コントロール プレーンのパケット ロギング機能用のポリシー マップをイネーブルにします。
log-policy	（任意）コントロール プレーン ロギングのログ ポリシーのタイプです。
policy-map-name	ポリシー マップ名です。
control	（任意）制御ポリシー マップを作成します。
control-name	制御ポリシー マップの名前です。
service	（任意）サービス ポリシー マップを作成します。

service-name	ポリシー マップ サービスの名前です。
class-routing	クラス ルーティング ポリシー マップを設定します。
ipv4	クラス ルーティング IPv4 ポリシー マップを設定します。
unicast	クラス ルーティング IPv4 ユニキャスト ポリシー マップを設定します。
unicast-name	ユニキャスト 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（config）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.4(4)T	このコマンドが変更されました。Flexible Packet Matching をサポートするために、**type** キーワードと **access-control** キーワードが追加されました。コントロールプレーン保護機能をサポートするために **port-filter** キーワードと **queue-threshold** キーワードが追加されました。
12.4(6)T	このコマンドが変更されました。コントロールプレーン パケット ロギングをサポートするために、**logging** キーワードが追加されました。
12.2(31)SB	このコマンドが変更されました。Cisco 10000 シリーズ ルータをサポートするために、**control** キーワードと **service** キーワードが追加されました。
12.2(18)ZY	このコマンドが変更されました。 • **type** キーワードと **access-control** キーワードが、Supervisor 32/Programmable Intelligent Services Accelerator（PISA）エンジンが搭載されている Catalyst 6500 シリーズ スイッチの Cisco IOS リリース 12.2(18)ZY に統合されました。 • このコマンドが、Supervisor 32/PISA エンジンが搭載されている Catalyst 6500 シリーズ スイッチの Network-Based Application Recognition（NBAR）機能を拡張するため、変更されました。
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。
12.2(33)SRC	このコマンドが変更されました。このコマンドのサポートが Cisco 7600 シリーズ ルータに実装されました。

リリース	変更箇所
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ ルータに実装されました。
12.2(33)SCF	このコマンドが、Cisco IOS リリース 12.2(33)SCF に統合されました。

使用上のガイドライン

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、作成、追加、または変更するポリシー マップの名前を指定するには、**policy-map** コマンドを使用します。**policy-map** コマンドにより、ポリシー マップ コンフィギュレーション モードが開始されます。このモードでは、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。**class-map** コマンドと **match** コマンドを使用して、クラスの一致基準を設定します。設定できるクラス マップは最大 64 個のため、Cisco 7600 システム上の Quality of Service（QoS）クラス マップ用に示されている場合を除いて、ポリシー マップに 64 個を超えるクラス ポリシーを含めることはできません。

（注） Cisco 7600 シリーズ ルータの QoS クラス マップでは、この制限はクラス マップが 1024 個、ポリシー マップのクラスが 256 個です。

ATM 設定セル損失率優先度（CLP）ビット QoS を含むポリシーマップは、PPP over X（PPPoX）セッションにアタッチできません。このポリシーマップは、**set atm-clp** コマンドを指定しない場合のみ適用できます。

1 つのポリシーマップは、同時に複数のインターフェイスに付加できます。特に注意が示されている場合以外では、ポリシー マップをインターフェイスに付加しようとするときに、インターフェイス上の使用可能な帯域幅が、ポリシー マップを構成しているクラス ポリシーで必要な合計帯域幅に満たない場合、付加は拒否されます。このとき、ポリシーマップが他のインターフェイスにすでにアタッチされている場合、そのインターフェイスからマップが削除されます。

（注） この制限は、Session Initiation Protocol（SIP）-400 アクセス対向ライン カードを搭載した Cisco 7600 シリーズ ルータには適用されません。

適用されたポリシー マップ内のクラス ポリシーを変更する場合、常にクラス ベース均等化キューイング（CBWFQ）が通知され、新しいクラスは CBWFQ システムのポリシー マップの一部としてインストールされます。

（注） サブスクライバ プロファイルを介したポリシー マップのインストールは、サポートされません。サポートされていないポリシーマップを設定した場合で、多数のセッションがある場合、同等数の多数のメッセージがコンソールに表示されます。たとえば、32,000のセッションがある場合、32,000 のメッセージが 9,600 ボーでコンソールに表示されます。

クラス キュー（Cisco 10000 シリーズ ルータのみ）

Performance Routing Engine（PRE）2 では、ポリシー マップで 31 個のクラス キューを設定できます。

ポリシー マップでは、PRE3 により 1 つのプライオリティ レベル 1 のキュー、1 つのプライオリティ レベル 2 のキュー、12 個のクラス キュー、および 1 つのデフォルト キューを設定できます。

制御ポリシー（Cisco 10000 シリーズ ルータのみ）

制御ポリシーは、指定されたイベントと条件に対応してシステムが実行するアクションを定義します。

制御ポリシーは 1 つ以上の制御ポリシー ルールで作成されます。制御ポリシー ルールは、制御クラスと 1 つ以上のアクションを関連付けたものです。制御クラスは、アクションが実行される前に満たされる必要がある条件を定義します。

制御ポリシーの定義には次の 3 つの手順があります。

1. **class-maptypecontrol** コマンドを使用して、1 つ以上の制御クラス マップを作成します。
2. **policy-maptypecontrol** コマンドを使用して、制御ポリシー マップを作成します。

制御ポリシー マップには 1 つ以上の制御ポリシー ルールが含まれます。制御ポリシー ルールは、制御クラス マップを 1 つ以上のアクションに関連付けます。アクションに番号が付けられ、順に実行されます。

1. **service-policytypecontrol** コマンドを使用して、コンテキストに制御ポリシーマップを適用します。

サービス ポリシー（Cisco 10000 シリーズ ルータのみ）

サービス ポリシー マップとサービス プロファイルには、トラフィック ポリシーとその他の機能のコレクションが含まれています。トラフィック ポリシーとは、どのセッション トラフィックにどの機能を適用するかを定義するものです。また、サービス ポリシー マップまたはサービスプロファイルには、ネットワーク転送ポリシーという、セッションデータ パケットをネットワークに転送する方法を指定する、特定のタイプのトラフィック ポリシーが含まれています。

ポリシー マップの制限（Catalyst 6500 シリーズ スイッチのみ）

Cisco IOS Release 12.2(18)ZY には、Supervisor 32/PISA エンジンが搭載された Catalyst 6500 シリーズスイッチ用のソフトウェアが含まれています。このリリースおよびプラットフォームには、ポリシー マップと **match** コマンドの使用に関する次の制限があります。

- ポリシー マップがインターフェイスにアタッチされている場合、既存のポリシー マップを変更することはできません。ポリシー マップを変更するには、**service-policy** コマンドの **no** 形式を使用して、インターフェイスからポリシー マップを削除します。
- ポリシー マップにはトラフィック クラスが含まれています。トラフィック クラスには、プロトコルタイプまたはアプリケーションに基づいてパケットを照合する（およびグループにまとめる）ために使用できる、1 つ以上の **match** コマンドが含まれています。必要に応じて任意の数のトラフィック クラスを作成できます。ただし、次の制限が適用されます。
  - 1 つのトラフィック クラスは、最大 8 個のプロトコルまたはアプリケーションに一致するように設定できます。
  - 複数のトラフィック クラスは、累積で最大 95 個のプロトコルまたはアプリケーションに一致するように設定できます。

例

次に、「policy1」と呼ばれるポリシーマップの作成方法と、そのポリシーマップに含まれる 2 つのクラス ポリシーの設定方法の例を示します。「class1」という名前のクラスポリシーにより、アクセスコントロールリスト（ACL）136 に一致するトラフィックのためのポリシーが指定されます。2 つ目のクラスは、設定されている一致基準を満たさないパケットが誘導されるデフォルト クラスです。

```
! The following commands create class-map class1 and define its match criteria:
class-map class1
 match access-group 136
! The following commands create the policy map, which is defined to contain policy
! specification for class1 and the default class:
policy-map policy1
class class1
 bandwidth 2000
 queue-limit 40
class class-default
 fair-queue 16
 queue-limit 20
```

次に、「policy9」という名前のポリシー マップの作成方法と、そのマップに属する 3 つのクラス ポリシーの設定方法の例を示します。これらのクラスのうち、2 つのクラスにより、番号付き ACL またはインターフェイス名のいずれかに基づいた一致基準を指定するクラス マップのクラスに対し、ポリシーが指定されます。また、1 つのクラスにより、設定されている一致基準を満たさないパケットが誘導される、「class-default」という名前のデフォルト クラスに対し、ポリシーが指定されます。

```
policy-map policy9

class acl136
 bandwidth 2000
 queue-limit 40
```

```
class ethernet101
 bandwidth 3000
 random-detect exponential-weighting-constant 10
class class-default
 fair-queue 10
 queue-limit 20
```

次に、セッションの開始時に QoS サービスを開始するように設定されたモジュラ QoS コマンドライン インターフェイス（MQC）ポリシー マップの例を示します。

```
Router> enable
Router# configure terminal
Router(config)# policy-map type control TEST
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1
 service-policy type service name QoS_Service
Router(config-control-policymap-class-control)# end
```

Cisco 10000 シリーズ ルータのみの例

次の例は、「rule4」という名前の制御ポリシーマップの設定を示しています。制御ポリシーマップ rule4 には、「class3」という名前の制御クラスと、ネットワーク アクセス サーバ（NAS）ポート ID を使用してサブスクライバを承認するためのアクションを関連付ける、1 つのポリシー ルールが含まれています。制御ポリシー マップをグローバルに適用するために、**service-policytypecontrol** コマンドが使用されています。

```
class-map type control match-all class3
 match vlan 400
 match access-type pppoe
 match domain cisco.com
 available nas-port-id
!
policy-map type control rule4
 class type control class3
  authorize nas-port-id
!
service-policy type control rule4
```

次の例は、「redirect-profile」という名前のサービス ポリシーマップの設定を示しています。

```
policy-map type service redirect-profile
 class type traffic CLASS-ALL
  redirect to group redirect-sg
```

Cisco CMTS ルータの例

次に、802.1p ドメインのポリシー マップを定義する例を示します。

```
enable
configure terminal
 policy-map cos7
  class cos7
```

```
  set cos 2
  end
```

次に、MPLS ドメインのポリシー マップを定義する例を示します。

```
enable
configure terminal
 policy-map exp7
  class exp7
  set mpls experimental topmost 2
  end
```

関連コマンド

Command	Description
bandwidth(policy-mapclass)	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
class(policy-map)	ポリシーを作成または変更するクラスの名前を指定し、ポリシーを設定する前にそのデフォルト クラスを指定します。
classclass-default	帯域幅が設定または変更されるデフォルト クラスを指定します。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
fair-queue(class-default)	デフォルト クラス ポリシーの一部として class-default クラスで使用するために予約するダイナミック キューの数を指定します。
matchaccess-group	指定した ACL をベースにクラス マップに対して一致基準を設定します。
queue-limit	ポリシー マップで設定されているクラス ポリシー用にキューで維持できるパケットの最大数の指定または修正を行います。
random-detect(interface)	WRED または DWRED をイネーブルにします。
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detectservice-policyprecedence	特定の IP precedence に対する WRED パラメータと DWRED パラメータを設定します。
service-policy	インターフェイスまたは VC のサービス ポリシーとして使用されるポリシー マップを入力のインターフェイスまたは VC（あるいは出力のインターフェイスまたは VC）にアタッチします。

Command	Description
set atm-clpprecedence	ポリシーマップを設定するときの ATM CLP ビットを設定します。

policy-map copp-peruser

コントロール プレーン ポリシングおよび保護（CoPP）のユーザごとのポリシーを定義するポリシー マップを作成するには、グローバル コンフィギュレーション モードで **policy-mapcopp-peruser** 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。

policy-map copp-peruser
no policy-map copp-peruser

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

ポリシー マップは設定されません。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。

使用上のガイドライン

CoPP を設定するときに、このコマンドを使用して CoPP のユーザごとのポリシーを作成します。

例

次の例では、CoPP のユーザごとのポリシー マップを作成します。

```
Router(config)# policy-map copp-peruser
Router(config-pmap)# class arp-peruser
Router(config-pmap-c)# police rate 5 pps burst 50 packets
Router(config-pmap-c)# class dhcp-peruser
Router(config-pmap-c)# police rate 10 pps burst 100 packets
```

関連コマンド

コマンド	説明
class-maparp-peruser	ARP のユーザごとのパケットの照合に使用するクラス マップを作成します。
matchsubscriberaccess	ポリシー マップに対する加入者アクセス トラフィックに一致します。

precedence

仮想回線（VC）バンドルへの割り当て、つまりそのバンドルのすべての VC メンバーへの適用が可能な VC クラスに優先レベルを設定するには、VC-class コンフィギュレーション モードで **precedence** コマンドを使用します。VC クラスから優先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。

バンドルの VC または相手先固定接続（PVC）メンバーの優先レベルを設定するには、ATM VC バンドル メンバーの bundle-VC コンフィギュレーション モード、または ATM 相手先選択接続（SVC）の SVC-bundle-member コンフィギュレーション モードで **precedence** を使用します。VC または PVC から優先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。

precedence [{**other***range*}]
no precedence

構文の説明

other	（任意）明示的には設定されない、0 ～ 7 の範囲の任意の優先レベルです。
range	（任意）0 ～ 7 の数値で指定される単一の優先レベル、またはハイフンで連結した範囲で指定される優先レベルの範囲です。

コマンド デフォルト

デフォルトの設定は、**other** で、明示的に設定されない、0 ～ 7 の範囲の任意の優先レベルになります。

コマンド モード

VC-class コンフィギュレーション（VC クラスの場合）
Bundle-VC コンフィギュレーション（ATM VC バンドル メンバーの場合）
SVC-bundle-member コンフィギュレーション（ATM SVC の場合）

コマンド履歴

リリース	変更箇所
11.1(22)CC	このコマンドが導入されました。
12.0(3)T	このコマンドが、Cisco IOS Release 12.0(3)T に統合されました。バンドルの VC メンバーの優先レベルを設定できるように拡張されました。
12.2(4)T	このコマンドが、SVC-bundle-member コンフィギュレーション モードで使用できるようになりました。
12.0(23)S	このコマンドが、Cisco 12000 シリーズ インターネット ルータで 8 ポートの OC-3 STM-1 ATM ライン カードの VC-class および bundle-vc コンフィギュレーション モードで使用できるようになりました。
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。

リリース	変更箇所
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

VC または PVC バンドル メンバーに優先レベルを割り当てると、IP precedence レベルを複数の VC/PVC バンドル メンバーに分散できるため、差別化サービスを作成できます。単一の優先レベルまたはレベルの範囲をバンドル内の個々の VC/PVC にマップできます。これにより、バンドル内の VC/PVC がさまざまな優先レベルによってマーク付けされたパケットを伝送できます。または、**precedenceother** コマンドを使用して、他の VC/PVC については、明示的に設定されない優先レベルにマーク付けされたトラフィックを VC/PVC によって伝送できることを示します。 **precedence other** コマンドを使用して設定可能なバンドル内の VC/PVC は 1 つのみです。この VC/PVC は、デフォルトと見なされます。

VC-class コンフィギュレーション モードでこのコマンドを使用するには、まずグローバル コンフィギュレーション モードで **vc-classatm** コマンドを入力します。**precedence** コマンドを含む VC クラスがスタンドアロン VC（バンドル メンバーではない VC）に付加されている場合、このコマンドは効果がありません。

precedence コマンドを使用して bundle-VC コンフィギュレーション モードで個々のバンドル メンバーを設定するには、まず **bundle** コマンドを入力して、設定対象の VC メンバーを追加または変更するバンドルにバンドル コンフィギュレーション モードを指定します。その後、**pvc-bundle** コマンドを使用して、作成または変更する VC を指定し、バンドル VC コンフィギュレーション モードにします。

VC バンドルの VC は、次の設定継承ガイドラインに従います（2 番目に高い優先順位の順にリストされています）。

- bundle-VC モードの VC 設定
- バンドル モードのバンドル コンフィギュレーション（および、割り当てられた VC-class コンフィギュレーションの影響）
- サブインターフェイス モードのサブインターフェイス設定

例

次は **precedence** コマンドを含む「control-class」という名前のクラスの設定例です。このコマンドは、バンドルに適用すると、そのバンドルのすべての VC メンバーが IP precedence レベル 7 のトラフィックを伝送するように設定します。ただし、このバンドルの VC メンバーは **precedence** コマンドを使用して、bundle-VC レベルで個々に設定される場合があることに注意してください。

```
vc-class atm control-class
 precedence 7
```

次は PVC 401（名前は「control-class」）の設定例で、4 ～ 2 の範囲の IP precedence レベルを持ったトラフィックを伝送し、VC-class コンフィギュレーションを使用した VC の優先レベル マッピング設定を上書きします。

```
pvc-bundle control-class 401
 precedence 4-2
```

関連コマンド

Command	Description
bump	VC バンドルに割り当てることができる VC クラスのバンピング ルールを設定します。
bundle	バンドルを作成するか、または既存のバンドルを修正してバンドル コンフィギュレーション モードを開始します。
class-vc	VC クラスを ATM PVC、SVC、または VC バンドル メンバーに割り当てます。
dscp(frame-relayvc-bundle-member)	特定のフレーム リレー PVC バンドル メンバーに対して DSCP 値を指定します。
matchprecedence	IP precedence 値を一致基準として識別します。
mplsexperimental	VCバンドルへのマッピング、つまりそのバンドルのすべての VC メンバーに適用する、VC クラスの MPLS EXP ビット値を設定します。
protect	VC バンドル メンバーへのアプリケーションの保護されたグループまたは保護された VC ステータスを持つ VC クラスを設定します。
pvc-bundle	バンドルに対してバンドルのメンバーとして PVC を追加し、PVC バンドル メンバーを設定するために bundle-vc コンフィギュレーション モードに入ります。
pvc	ATM PVC に名前を割り当て、ATM PVC のカプセル化タイプを指定し、interface-ATM-VC コンフィギュレーション モードに入ります。
ubr	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レートを指定します。
ubr+	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レートと出力最小保証セル レートを指定します。

Command	Description
vbr-nrt	可変ビット レート非リアルタイム（VBR-NRT）QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レート、出力平均セル レート、および、出力最大バースト セル サイズを指定します。
vc-classatm	ATM VC またはインターフェイスの VC クラスを設定します。

precedence（WRED グループ）

特定の IP プレシデンスの重み付けランダム早期検出（WRED）または VIP 分散 WRED（DWRED）を設定するには、ランダム検出グループ コンフィギュレーション モードで **precedence** コマンドを使用します。グループの各 IP プレシデンスの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。

precedence *precedence min-threshold max-threshold mark-probability-denominator*
no precedence *precedence min-threshold max-threshold mark-probability-denominator*

構文の説明

precedence	IP プレシデンス番号です。値の範囲は 0 ～ 7 です。
min-threshold	パケット数での最小しきい値。値の範囲は 1 ～ 4096 です。キューの平均の長さがこの数に達すると、WRED または DWRED は指定された IP プレシデンスを持つパケットをドロップし始めます。
max-threshold	パケット数での最大しきい値。値の範囲は、*min-threshold* ～ 4096 です。平均キューの長さがこの数を超えると、WRED または DWRED は指定された IP プレシデンスを持つすべてのパケットをドロップします。
mark-probability-denominator	平均キューの深さが *max-threshold* の場合にドロップされるパケットの割合の分母です。たとえば、分母が 512 の場合、平均キューが *max-threshold* のときに、512 パケットごとに 1 パケットがドロップされます。値は 1 ～ 65536 です。デフォルトは 10 です。つまり、*max-threshold* に達したときに、10 パケットにつき 1 つのパケットがドロップされます。

コマンド デフォルト

すべての IP プレシデンスについて、*mark-probability-denominator* 引数は 10 で、*max-threshold* 引数は出力バッファリング容量とインターフェイスの伝送速度に基づきます。

デフォルトの *min-threshold* 引数は IP プレシデンスに応じて異なります。IP プレシデンス 0 の *min-threshold* 引数は、*max-threshold* 引数の半分になります。残りの IP プレシデンスの値は、*max-threshold* 引数の半分から *max-threshold* 引数までの間に、等間隔に配置されます。各 IP プレシデンスのデフォルトの最小値の一覧については、以下の「使用上のガイドライン」のセクションにある表を参照してください。

コマンド モード

Random-detect-group コンフィギュレーション

コマンド履歴

リリース	変更箇所
11.1(22)CC	このコマンドが導入されました。
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。

リリース	変更箇所
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

WREDは、輻輳が存在するときにランダムにパケットをドロップすることでトラフィックを遅くする輻輳回避メカニズムです。DWREDはWREDに類似していますが、Route Switch Processor（RSP）の代わりにVersatile Interface Processor（VIP）が使用されます。

使用する場合、このコマンドは **random-detect-group** コマンドの後に発行します。

インターフェイスで **random-detectgroup** コマンドを設定すると、パケットの IP プレシデンスに基づいて、パケットに対する優先処理が行われます。異なる IP プレシデンスに対する処理を調節するには、**precedence** コマンドを使用します。

WRED または DWRED でドロップするパケットを決定する際に IP プレシデンスを無視する場合は、各 IP プレシデンスに同じパラメータでこのコマンドを入力します。最小しきい値および最大しきい値には、妥当な値を設定します。

（注） デフォルトの WRED または DWRED パラメータ値は、最適な使用可能データに基づきます。値を変更することでアプリケーションに利点があると判断した場合を除き、パラメータのデフォルト値を変更しないことを推奨します。

次の表に、各 IP プレシデンスのデフォルトの最小値を示します。

表 *31 :* デフォルト *WRED* 最小しきい値

IP precedence	最小しきい値（最大しきい値の分数）
0	8/16
1	9/16
2	10/16
3	11/16
4	12/16
5	13/16
6	14/16
7	15/16

例

次の例では、異なる IP プレシデンスについて、sanjose という名前の WRED パラメータ グループのパラメータを指定します。

```
random-detect-group sanjose
 precedence 0 32 256 100
 precedence 1 64 256 100
 precedence 2 96 256 100
 precedence 3 128 256 100
 precedence 4 160 256 100
 precedence 5 192 256 100
 precedence 6 224 256 100
 precedence 7 256 256 100
```

関連コマンド

Command	Description
exponential-weighting-constant	WRED パラメータ グループの平均キュー サイズ計算のための指数加重係数を設定します。
random-detect(perVC)	per-VC WRED または per-VC DWRED をイネーブルにします。
random-detect-group	WRED または DWRED パラメータ グループを定義します。
random-detectprecedence	特定の IP Precedence の WRED パラメータと DWRED パラメータを設定します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。
showqueueinginterface	インターフェイスまたは VC のキューイングの統計情報を表示します。

preempt-priority

アップストリームかダウンストリーム ネイバーまたはローカル クライアント アプリケーションからのシグナルがなかった場合に PATH および RESV メッセージに挿入するリソース予約プロトコル（RSVP）サービス品質（QoS）優先順位を指定するには、ローカル ポリシー設定モードで **preempt-priority** コマンドを使用します。優先順位を削除するには、このコマンドの **no** 形式を使用します。

preempt-priority [**traffic-eng** *x*] *setup-priority* [*hold-priority*]
no preempt-priority [**traffic-eng** *x*] *setup-priority* [*hold-priority*]

構文の説明

traffic-eng *x*	（任意）トラフィック エンジニアリング（TE）予約の優先順位の上限を示します。*x* 値の範囲は 0 ～ 7 で、番号が小さいほど予約の優先順位が高くなります。非 TE 予約の場合は、*x* 値の範囲は 0 ～ 65535 で、番号が大きくなるほど予約の優先順位が高くなります。
setup-priority	初回にインストールされる場合の予約の優先順位を示します。値の範囲は 0 ～ 7 です。0 は優先順位が最も高いことを意味します。TE 予約の場合、デフォルト値は 7 です。TE 以外の予約ではデフォルトは 0 です。
hold-priority	（任意）インストール済みの場合の予約の優先順位を示します。省略すると、この引数のデフォルトは *setup-priority* になります。値の範囲は 0 ～ 7 です。0 は優先順位が最も高いことを意味します。TE 予約の場合、デフォルト値は 7 です。TE 以外の予約ではデフォルトは 0 です。

コマンド デフォルト

これらの値を設定した後に RSVP QoS 優先順位を指定します。

コマンド モード

ローカル ポリシー設定

コマンド履歴

リリース	変更箇所
12.2(13)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

RSVP QoS または MPLS/TE セッションから発信できるセットアップまたは保持の最大優先度を指定するには、**preempt-priority** コマンドを使用します。これらの制限を超えると、PATHERROR、RESVERROR、またはローカル アプリケーション エラーが返されます。

受信メッセージに、このポリシーで許可されるよりも高い優先順位を要求するプリエンプション優先順位がある場合、メッセージは拒否されます。TE トンネルにプリエンプション優先順位を設定する場合は、tunnel mpls traffic-eng priority コマンドを使用します。

1 つのポリシーには、preempt-priority traffic-eng および preempt-priority コマンドを指定でき、このコマンドは、TE および TE 以外のエンドポイントまたはミッドポイントが混同して含まれる

サブネットを識別するアクセス コントロール リスト（ACL）にポリシーをバインドする場合に便利です。

プリエンプションの予約を選択すると、RSVP は低い優先順位の予約をプリエンプション処理した後に高い優先順位の予約を処理します。プリエンプション優先順位が同じ TE 以外の予約が複数ある場合、RSVP は最も古い予約を最初に選択します。

例

次は、セットアップ優先順位が 0 で、保持優先度が 5 の例です。

```
Router(config-rsvp-local-policy)# preempt-priority 0 5
```

関連コマンド

コマンド	説明
iprsvppolicylocal	RSVP 要求に対する認証の実行方法を決定します。
iprsvppolicypreempt	RSVP は低い優先順位の予約から帯域幅を取得して、新規の優先順位が高い予約に割り当てます。
tunnelmplstraffic-engpriority	MPLS TE トンネルのセットアップおよび予約優先順位を設定します。

priority

ポリシー マップ内のトラフィックのクラスに優先順位を割り当てるには、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 {*bandwidth-kbps*|**percent** *percentage*} [*burst*]
no priority {*bandwidth-kbps*|**percent** *percentage*} [*burst*]

構文の説明

bandwidth-kbps	プライオリティ トラフィックに許可される保証帯域幅（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。
percent	保証帯域幅の分量が、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。
percentage	プライオリティ クラス用に確保する使用可能な帯域幅の合計。指定できる値の範囲は 1 ～ 100 です。
burst	（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。

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(7)T	このコマンドが導入されました。
12.0(5)XE5	このコマンドが Cisco IOS Release 12.0(5)XE5 に統合されて、Versatile Interface Processor（VIP）に分散型低遅延キューイング（VIP 用の低遅延キューイング）機能の一部として実装されました。
12.0(9)S	このコマンドが Cisco IOS Release 12.0(9)S に統合されて、VIP に分散型低遅延キューイング（VIP 用の低遅延キューイング）機能の一部として実装されました。
12.1(2)E	このコマンドが変更されました。*burst* 引数がキーワードが追加されました。

リリース	変更箇所
12.1(3)T	このコマンドが Cisco IOS Release 12.1(3)T に統合されました。
12.1(5)T	このコマンドが Cisco IOS Release 12.1(5)T に統合されて、VIP に分散型低遅延キューイング（VIP 用の低遅延キューイング）機能の一部として実装されました。
12.2(2)T	このコマンドが変更されました。**percent** キーワードおよび *percentage* 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE 2.1 に統合され、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。
15.1(1)T	このコマンドが変更されました。*bandwidth-kbps* 引数に使用できる値が変更されました。値は 8 ～ 2,000,000 kbps である必要があります。
15.2(1)T	このコマンドが変更されました。*bandwidth-kbps* 引数に使用できる値が変更されました。値は 1 ～ 2,000,000 kbps である必要があります。
15.4(1)S	このコマンドが、Cisco ASR 901 シリーズ ルータに実装されました。

使用上のガイドライン

このコマンドは、クラスベース均等化キューイング（CBWFQ）の絶対優先キューイング（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。

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を設定し、優先順位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 **iprtppriority** コマンドを使用すると、UDP ポート番号のみに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 では使用できません。

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。しかしこれらのコマンドは、同じポリシー マップ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。

帯域割り当ての詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Congestion Management Overview」を参照してください。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、*bandwidth-kbps* や *percentage* などの条件付きプライオリティ レート リミッタの使用は、3 レイヤ ポリシー マップ設定の最下位レベル（孫またはリーフ）ではサポートされません。3 レベル ポリシーの最下位レベルでは、条件付きリミッタは適用されません。ただし、完全ポリサーによるプライオリティは、このレベルの階層でサポートされます。この制約は、フラットまたは 2 レベル階層型ポリシーマップには適用されません。

例

次に、policy1 という名前のポリシー マップで、50 kbps の保証帯域幅と 60 バイトの 1 回限りのバースト サイズで PQ を設定する例を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50 60
```

次に、policy1 という名前のポリシーマップが適用されているインターフェイス上で、使用可能な帯域幅の 10% を voice という名前のクラス用に予約する例を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority percent 10
```

関連コマンド

コマンド	説明
bandwidth	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
iprtppriority	UDP 宛先ポートの範囲に属する RTP パケット フロー セットについて、完全プライオリティ キューを予約します。
iprtpreserve	UDP宛先ポートの範囲に属するRTPパケットフローのセット用に、特殊キューを確保します。

コマンド	説明
max-reserved-bandwidth	CBWFQ、LLQ、および IP RTP プライオリティに割り当てるインターフェイス帯域幅のパーセント比率を変更します。
showinterfacesfair-queue	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。

priority（10000 シリーズ）

ポリシー マップでトラフィック クラスに優先順位を割り当てるには、Cisco 10000 シリーズ ルータの QoS 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。クラスの優先処理を削除するには、このコマンドの **no** 形式を使用します。

priority
no priority

構文の説明

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

QoS ポリシー クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(17)SL	このコマンドが導入されました。
12.0(20)ST	このコマンドが拡張され、パーセントベース帯域幅レートをサポートするようになりました。
12.0(25)S	このコマンドが変更され、ESR-PRE1 で絶対優先キューイングが使用できるようになりました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。
12.3(7)XI1	このコマンドが変更され、ESR-PRE2 で絶対優先キューイングが使用できるようになりました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。

使用上のガイドライン

Cisco IOS Release 12.0(25)S および Release 12.3(7)XI1 以降の priority コマンドでは、絶対優先キューイングを使用できます。帯域幅レートをキロビット/秒（kbps）またはリンク帯域幅のパーセンテージで指定するには、police または police percent コマンドを使用します。

絶対優先キューイングを使用すると、リンク上の現在の輻輳レベルに関係なく、優先キューに入れるパケットの低遅延を保証します。

（注） Cisco IOS Release 12.0(25)S および Release 12.3(7)XI より前のリリースで帯域幅レートを指定する場合、priority コマンドを使用します。

priority コマンドを使用すると、ポリシー マップでトラフィック クラスに優先順位を割り当てられます。ルータは優先処理をプライオリティ クラスに割り当てるため、プライオリティ

キューイングでは音声など遅延の影響を受けやすいデータを、他のキューのパケットより前にキュー解除して送信できます。

police コマンドで帯域幅パラメータを指定すると、プライオリティ クラスに帯域幅を保証し、そのプライオリティ クラスからのパケットのフローを制限します。

priority コマンドを使用すると、次のインターフェイスでプライオリティ キューイングがサポートされます。

- Physical
- マルチリンク PPP およびマルチリンク フレーム リレー
- ATM 整形（ピーク セル レートを指定）未指定ビット レート（UBR）の相手先固定接続（PVC）およびポイントツーポイント サブインターフェイス
- ATM 固定ビット レート（CBR）PVC およびポイントツーポイント サブインターフェイス
- ATM 可変ビット レート（VBR）PVC およびポイントツーポイント サブインターフェイス
- ラベル制御 ATM（LC-ATM）サブインターフェイス
- フレーム リレー PVC、ポイントツーポイント サブインターフェイス、およびマップ クラス
- イーサネット VLAN

priority コマンドを使用しても、次のインターフェイスではプライオリティ キューイングはサポートされません。

- ATM 非整形（ピーク セル レートを指定しない）UBR PVC およびポイントツーポイント サブインターフェイス
- IP トンネル
- 仮想アクセス

Cisco 10000 シリーズ ルータ

Cisco 10000 シリーズ ルータでは、発信インターフェイスでのみ priority コマンドをサポートしています。着信インターフェイスでは、priority コマンドはサポートされません。

プライオリティ キューイングの制限事項

- 各ポリシー マップで指定できるプライオリティ クラスは 1 つのみです。
- プライオリティ サービスでは random-detect または bandwidth コマンドを設定できません。

例

次の例では、ポリシー マップ policy1 の class-default に優先順位を割り当てます。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# priority
```

関連コマンド

Command	Description
bandwidth(policy-mapclass)	ポリシーマップに属しているクラスに割り当てる帯域幅を指定します。
police	インターフェイスで送受信するトラフィックの最大レートを制御します。
police （percent）	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
randomdetect （perVC）	VC 単位 WRED または VC 単位 VIP 分散 WRED を有効にします。

priority（SIP400）

クラス マップに絶対スケジュール優先を設定するには、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 **priority** コマンドを使用します。以前に指定したクラスの優先度レベルを削除するには、このコマンドの **no** 形式を引数を指定せずに使用します。

priority [**level** {**1**|**2**}] [{*kbps* [*burst*]|**percent** *percentage* [*burst*]}]
no priority

構文の説明

level {**1** | **2**	（任意）複数レベルの絶対優先サービス モデルを定義します（1 は高レベル、2 は低レベル）。特定のレベルの優先サービスが設定されたトラフィック クラスをイネーブルにすると、その特定のレベルの優先サービスがイネーブルにされたすべてのトラフィックに、単一の優先キューが関連付けられることになります。デフォルトは 1 です。
kbps	（任意）プライオリティ トラフィックに対して許可される、kbps 単位での保証帯域幅です。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。範囲：1 ～ 2480000。
burst	（任意）バースト サイズをバイト単位で指定します。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。*burst* 引数を指定しないと、デフォルトのバースト値が使用されます。範囲：18 ～ 2000000。デフォルト：設定された帯域幅レートで 200 ミリ秒のトラフィックです。
percent *percentage*	（任意）プライオリティ クラス用に残しておく合計の利用可能な帯域幅のパーセンテージを指定します。範囲は 1 ～ 100 です。

コマンド デフォルト

すべてのトラフィックで低いプライオリティ キューが使用されます。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.2(33)SXI	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 つのポリシー マップ内に 2 つのレベルのプライオリティ キューを作成するには、**priority** コマンドを入力します。レベル 2 のプライオリティ キューからのパケットは、レベル 1 プライオリティ キューが空のときのみ送信されるようにスケジュールされます。

優先帯域幅およびパーセンテージには次の制限事項があります。

- 出力方向のみでサポートされます。

- ATM 共有ポート アダプタ（SPA）ではサポートされません。

優先度レベルには次の制限事項があります。

- 2 つの優先度レベル（priority または priority level 1 と priority level 2）のみがサポートされます。
- 優先順位は出力方向のみでサポートされます。
- 優先順位は、ATM SPA でサポートされていません。

プライオリティ機能の厳密なレベルおよびレベルごとのカウントを表示するには、**showpolicy-mapinterface** コマンドを入力します。

同じポリシー マップ内では、**bandwidth** コマンドおよび **prioritylevel** 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 マップでは使用できます。

同じポリシー マップ内では、**shape** コマンドおよび **prioritylevel** 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 マップでは使用できます。

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。ルータは単一のプライオリティ キューを同じ優先度レベルが有効になっているすべてのトラフィックに関連付け、ハイレベル プライオリティ キューが空になると、次レベルのプライオリティ キューと非プライオリティ キューを処理します。

同じポリシー マップ内の異なる 2 つのクラスに同じ優先度レベルを指定することはできません。

同じポリシー マップ内の異なる 2 つのクラスに **priority** コマンドおよび **prioritylevel** コマンドは指定できません。たとえば、**priority***kbps* または **prioritypercent***percentage* コマンドおよび **prioritylevel** コマンドを異なるクラスに指定することはできません。

prioritylevel コマンドが特定レベルのプライオリティ サービスで設定されている場合、**queue-limit** および **random-detect** コマンドは、その優先度レベルの単一クラスが設定されている場合のみ使用できます。

いかなる優先度レベルであっても、デフォルト キューをプライオリティ キューに設定することはできません。

例

次の例は、複数レベルのプライオリティ キューの設定方法を示しています。この例では、Customer1 という名前のトラフィック クラスに高い優先順位（レベル 1）が割り当てられており、Customer2 という名前のクラスにはレベル 2 の優先順位が割り当てられています。Customer2 トラフィックが妨げられないように、Customer1 トラフィックは使用可能な帯域幅の 30% でポリシングされています。

```
Router# config terminal
Router(config)# policy-map Business
Router(config-pmap)# class Customer1
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 30
Router(config-pmap-c)# exit
```

```
Router(config-pmap)# class Customer2
Router(config-pmap-c)# priority level 2
```

次に、policy1 という名前のポリシー マップで、50 kbps の保証された帯域幅と 60 バイトの 1 回限りのバースト サイズでプライオリティ キューを設定する例を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50 60
```

次の例では、policy1 という名前のポリシーマップが付加されているインターフェイス上で、使用可能な帯域幅の 10% が音声クラス用に確保されます。

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority percent 10
```

関連コマンド

コマンド	説明
bandwidth	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
priority	トラフィック クラスに優先順位を割り当てます。
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。
random-detect	インターフェイスで重み付けランダム早期検出（WRED）を有効にします。
shape	発信トラフィックのクラスに最大データ レートを指定します。
showpolicy-mapinterface	インターフェイスに対応付けられているポリシーの統計情報および設定を表示します。

priority-group

（注） Cisco IOS Release 15.1(3)T では、**priority-group** コマンドは表示されません。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンドラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンド シーケンス）を使用する必要があります。代わりに使用するコマンドのリストなど、詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

指定された優先リストをインターフェイスに割り当てるには、インターフェイス コンフィギュレーション モードで **priority-group** コマンドを使用します。指定された優先度グループの割り当てを削除するには、このコマンドの **no** 形式を使用します。

priority-group *list-number*
no priority-group *list-number*

構文の説明

list-number	インターフェイスに割り当てられた優先リスト番号。1 ～ 16 の数字。

コマンド デフォルト

無効

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
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。このコマンドが非表示になりました。

使用上のガイドライン

1 つのインターフェイスに 1 つのリストのみを割り当てることができます。優先出力キューイングには、インターフェイスから送信されるパケットの優先順位付け機能があります。

出力キューの現在のステータスを表示するには、**showqueueing** および **showinterfaces** コマンドを使用します。

例

次の例では、シリアル インターフェイス 0 の伝送パケットが優先リスト 1 に分類されます。

```
interface serial 0
 priority-group 1
```

次は、シリアル トンネル（STUN）接続のシリアル リンクのアドレスに基づいてキューイング プライオリティを確立する例です。優先度グループを出力インターフェイスに割り当てるには、**priority-group** インターフェイス コンフィギュレーション コマンドを使用する必要があることに注意してください。

```
stun peer-name 172.16.0.0
stun protocol-group 1 sdlc
!
interface serial 0
! Disable the ip address for interface serial 0:
no ip address
! Enable the interface for STUN:
encapsulation stun
!
stun group 2
stun route address 10 tcp 172.16.0.1 local-ack priority
!
! Assign priority group 1 to the input side of interface serial 0:
priority-group 1
! Assign a low priority to priority list 1 on serial link identified
! by group 2 and address A7:
priority-list 1 stun low address 2 A7
```

関連コマンド

Command	Description
locaddr-priority-list	LUアドレスに基づいてキューイング プライオリティを確立する手順の 1 つとして、LU を キューイング プライオリティにマップします。
priority-listdefault	優先リストの他の規則に一致しないパケット用にプライオリティ キューを割り当てます。
priority-listinterface	特定のインターフェイスから着信するパケットのキューイング プライオリティを確立します。
priority-listprotocol	プロトコル タイプに基づいてキューイングの優先順位を設定します。
priority-listprotocoliptcp	TCP ポートに基づいて BSTUN または STUN キューイング プライオリティを確立します。
priority-listprotocolstunaddress	シリアル リンクのアドレスに基づいて、STUN キューイング プライオリティを確立します。
priority-listqueue-limit	各プライオリティ キューで待機可能なパケットの最大数を指定します。

Command	Description
showinterfaces	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。
showqueue	特定のインターフェイスまたはVCのキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

priority level

複数のプライオリティ キューを設定するには、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 **priority level** コマンドを使用します。以前に指定したクラ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 *level*
no priority level *level*

構文の説明

level	複数レベルの絶対優先サービス モデルを定義します。特定のレベルのプライオリティ サービスが設定されたトラフィック クラスを有効にすると、その特定のレベルのプライオリティ サービスが有効にされたすべてのトラフィックに、単一のプライオリティ キューが関連付けられることになります。 有効な値は、1（高プライオリティ）～ 4（低プライオリティ）です。デフォルトは 1 です。Cisco ASR 1000 シリーズ ルータおよび Cisco ASR 903 シリーズ ルータの有効な値は、1（高プライオリティ）～ 2（低プライオリティ）です。デフォルトは 1 です。

コマンド デフォルト

優先度レベルのデフォルト レベルは 1 です。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.2(31)SB2	このコマンドが、複数レベルの絶対優先キューイングをサポートするために追加され、PRE3 用の Cisco 10000 シリーズ ルータに実装されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。
Cisco IOS XE リリース 3.7S	このコマンドが Cisco ASR 903 シリーズ ルータに実装されました。

使用上のガイドライン

同じポリシー マップ内では、**bandwidth** および **priority level** コマンドを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 マップでは使用できます。

同じポリシー マップ内では、**shape** および **priority level** コマンドを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 マップでは使用できます。

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。ルータは単一のプライオリティ キューを同じ優先度レベルが有効になっているすべてのトラフィックに関連付け、空になるまでハイレベル プライオリティ キューを処理した後、次レベルのプライオリティ キューと非プライオリティ キューを処理します。

同じポリシー マップ内の異なる 2 つのクラスに同じ優先度レベルを指定することはできません。

同じポリシー マップ内の異なる 2 つのクラスに **priority** コマンドおよび **priority level** コマンドは指定できません。たとえば、**priority bandwidth** *kbps* または **priority percent** *percentage* コマンドおよび **priority level** コマンドを異なるクラスに指定することはできません。

priority level コマンドが特定レベルのプライオリティ サービスで設定されている場合、**queue-limit** および **random-detect** コマンドは、その優先度レベルの単一クラスが設定されている場合のみ使用できます。

いかなる優先度レベルであっても、デフォルト キューをプライオリティ キューに設定することはできません。

Cisco 10000 シリーズ ルータ、Cisco ASR 1000 シリーズ ルータ、および Cisco ASR 903 シリーズ ルータ

Cisco 10000 シリーズ ルータ、Cisco ASR 1000 シリーズ ルータ、および Cisco ASR 903 シリーズ ルータでは、プライオリティ サービスの 2 つのレベルであるレベル 1（高）およびレベル 2（低）がサポートされます。優先度レベルを指定しないと、ルータではデフォルトのレベル 1 が使用されます。レベル 1 では、トラフィック クラスに低遅延動作が割り当てられる必要があります。ハイ レベル キューが空になるまで処理された後、次レベル キューと非プライオリティ キューが処理されます。

例

次の例は、複数レベルのプライオリティ キューの設定方法を示しています。この例では、Customer1 という名前のトラフィック クラスに高い優先順位（レベル 1）が割り当てられており、Customer2 という名前のクラスにはレベル 2 の優先順位が割り当てられています。Customer2 トラフィックでの帯域幅不足を防ぐために、Customer1 トラフィックは使用可能な帯域幅の 30% でポリシングされています。

```
Router> enable
Router# config terminal
Router(config)# policy-map Business
Router(config-pmap)# class Customer1
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 30
Router(config-pmap-c)# exit
Router(config-pmap)# class Customer2
Router(config-pmap-c)# priority level 2
```

関連コマンド

コマンド	説明
bandwidth	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
priority	トラフィック クラスに優先順位を割り当てます。

コマンド	説明
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。設定されているすべての優先度レベルの統計情報が表示されます。

priority-list default

優先リストの他のどのルールにも一致しないパケットにプライオリティ キューを割り当てるには、グローバル コンフィギュレーション モードで **priority-listdefault** コマンドを使用します。デフォルトに戻すか、デフォルトとして **normal** を割り当てるには、このコマンドの **no** 形式を使用します。

priority-list *list-number* **default** {**high**|**medium**|**normal**|**low**}
no priority-list *list-number* **default**

構文の説明

list-number	優先リストを識別する 1 ～ 16 の番号。
high | **medium** | **normal** | **low**	プライオリティ キューのレベル。このコマンドの **no** 形式を使用する場合は、**normal** キューになります。

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

グローバル設定

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
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。

使用上のガイドライン

複数のルールを使用する場合、システムでは表示された順序で優先順位設定が読み取られることに注意してください。パケットの分類時に、システムは **priority-list** コマンドで指定されたルール リストから一致するプロトコルまたはインターフェイス タイプを検索します。一致すると、パケットが適切なキューに割り当てられます。システムは指定された順序でリストを検索し、ルールとの初回の一致で検索は終了します。

例

次は、優先リストの他のどのルールにも一致しないパケットのプライオリティ キューを低プライオリティに設定する例です。

```
priority-list 1 default low
```

関連コマンド

Command	Description
priority-group	指定した優先リストをインターフェイスに割り当てます。

Command	Description
priority-listinterface	特定のインターフェイスから着信するパケットのキューイング プライオリティを確立します。
priority-listprotocol	プロトコル タイプに基づいてキューイングの優先順位を設定します。
priority-listqueue-limit	各プライオリティ キューで待機可能なパケットの最大数を指定します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

priority-list interface

特定のインターフェイスから着信するパケットのキューイング プライオリティを確立するには、グローバル コンフィギュレーション モードで **priority-listinterface** コマンドを使用します。リストからエントリを削除するには、このコマンドの **no** 形式を適切な引数を指定して使用します。

priority-list *list-number* **interface** *interface-type interface-number* {**high**|**medium**|**normal**|**low**}
no priority-list *list-number* **interface** *interface-type interface-number* {**high**|**medium**|**normal**|**low**}

構文の説明

list-number	優先リストを識別する 1 ～ 16 の番号。
interface-type	インターフェイスのタイプ。
interface-number	インターフェイスの番号。
high | **medium** | **normal** | **low**	プライオリティ キューのレベル。

コマンド デフォルト

デフォルトでは、キューイング プライオリティは確立されません。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
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。

使用上のガイドライン

複数のルールを使用する場合、システムでは表示された順序で優先順位設定が読み取られることに注意してください。パケットの分類時に、システムは **priority-list** コマンドで指定されたルール リストから一致するプロトコルまたはインターフェイス タイプを検索します。一致すると、パケットが適切なキューに割り当てられます。システムは指定された順序でリストを検索し、ルールとの初回の一致で検索は終了します。

例

次は、シリアル インターフェイス 0 に着信するリストを中プライオリティのキュー レベルに割り当てる例です。

```
priority-list 3 interface serial 0 medium
```

（注） このコマンドは、インターフェイスへのパケットの割り当て方法を指定するルールを定義します。ルールを定義したら、**priority-group** コマンドを使用してパケットを実際にインターフェイスへ割り当てます。

関連コマンド

Command	Description
priority-group	指定した優先リストをインターフェイスに割り当てます。
priority-listdefault	優先リストの他の規則に一致しないパケット用にプライオリティ キューを割り当てます。
priority-listprotocol	プロトコル タイプに基づいてキューイングの優先順位を設定します。
priority-listqueue-limit	各プライオリティ キューで待機可能なパケットの最大数を指定します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

priority-list protocol

プロトコル タイプに基づいてキューイング プライオリティを確立するには、グローバル コンフィギュレーション モードで **priority-listprotocol** コマンドを使用します。プロトコル タイプ別に割り当てられた優先リスト エントリを削除するには、このコマンドの **no** 形式を適切な引数を指定して使用します。

priority-list *list-number* **protocol** *protocol-name* {**high**|**medium**|**normal**|**low**} *queue-keyword keyword-value*
no priority-list *list-number* **protocol** *protocol-name* {**high**|**medium**|**normal**|**low**} *queue-keyword keyword-value*

構文の説明

list-number	優先リストを識別する 1 ～ 16 の番号。
protocol-name	プロトコル タイプ：**aarp**、**appletalk**、**arp**、**bridge**（透過）、**clns**、**clns_es**、**clns_is**、**compressedtcp**、**cmns**、**decnet**、**decnet_node**、**decnet_router-l1**、**decnet_router-l2**、**dlsw**、**ip**、**ipx**、**pad**、**rsrb**、**stun**、および **x25**。
high | **medium** | **normal** | **low**	プライオリティ キューのレベル。
queue-keyword keyword-value	使用可能なキーワードは、**fragments**、**gt**、**list**、**lt**、**tcp**、および **udp** です。キーワードと値の詳細については、「使用上のガイドライン」セクションの表 20 を参照してください。

コマンド デフォルト

キューイング プライオリティは確立されません。

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	変更箇所
10.0	このコマンドが導入されました。
12.2(13)T	このコマンドが変更されました。**apollo**、**vines**、および **xns** キーワードはプロトコル タイプのリストから削除されました。これらのプロトコルは、Release 12.2(13)T で Apollo Domain、Banyan VINES、および Xerox Network Systems（XNS）が削除されたため、削除されました。
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。

使用上のガイドライン

単一プロトコルで複数のルールを使用する場合、システムでは表示された順序で優先順位設定が読み取られることに注意してください。パケットの分類時に、システムは **priority-list** コマンドで指定されたルール リストから一致するプロトコル タイプを検索します。一致すると、パケットが適切なキューに割り当てられます。システムは指定された順序でリストを検索し、ルールとの初回の一致で検索は終了します。

decnet_router-l1 キーワードはすべてのレベル 1 ルータ（エリア内ルータ）のマルチキャスト アドレスを示し、**decnet_router-l2** キーワードはすべてのレベル 2 ルータ（エリア間ルータ）を示します。

dlsw、**rsrb**、および **stun** キーワードはダイレクト カプセル化のみを意味します。

次の表を使用して、ご使用のシステムに対応したキューイング プライオリティを設定します。

表 *32:* プロトコル プライオリティ キューのキーワードと値

オプション	説明
fragments	定義済みの優先度レベルをフラグメント化された IP パケットに割り当てます（IP のみで使用する場合）。具体的には、このコマンドはフラグメント オフセット フィールドがゼロではない IP パケットに一致します。フラグメント化された IP パケットの最初のフラグメントはフラグメント オフセットがゼロのため、このようなパケットはこのコマンドでは一致しません。 （注） フラグメント オフセットがゼロではないパケットには、TCP または User Datagram Protocol（UDP）ヘッダーがないため、**tcp** または **udp** キーワードを使用するこのコマンドの他のインスタンスでは、このようなパケットが一致することはありません。
gt *byte-count*	バイト数の最小値を指定します。パケット サイズが *byte-count* 引数に入力された値よりも大きい場合に、割り当てられた優先度レベルが有効になります。 （注） 発信インターフェイスで MAC カプセル化を行うためのバイト数もパケット サイズに追加する必要があります。
list *list-number*	AppleTalk、ブリッジング、IP、IPX、VINES、または XNS で使用する場合、トラフィック プライオリティを指定されたリストに従って割り当てます。*list-number* 引数は、指定された *protocol-name* に対応した、**access-list** グローバル コンフィギュレーション コマンドで指定したアクセス リスト番号です。たとえば、プロトコルが AppleTalk の場合、*list-number* は AppleTalk の有効なアクセス リスト番号である必要があります。
lt *byte-count*	バイト数の最大値を指定します。パケット サイズが *byte-count* 引数に入力された値よりも小さい場合に、割り当てられた優先度レベルが有効になります。 （注） 発信インターフェイスで MAC カプセル化を行うためのバイト数もパケット サイズに追加する必要があります。

オプション	説明
tcp ポート	定義済みの優先度レベルを、指定されたポートで送受信する TCP セグメントに割り当てます（IP のみで使用する場合）。表 21 に一般的な TCP サービスとそのポート番号を示します。
udp ポート	定義済みの優先度レベルを、指定されたポートで送受信する UDP パケットに割り当てます（IP のみで使用する場合）。表 22 に一般的な UDP サービスとそのポート番号を示します。

表 ***33:*** 一般的な ***TCP*** サービスとそのポート番号

サービス	ポート
FTP data	20
FTP	21
簡易メール転送プロトコル（SMTP）	25
Telnet	23

（注） TCP サービスとそのポート番号の完全なリストを表示するには、Router(config)# などのヘルプ文字列を入力します。**prioritylist4protocolipmediumtcp?**

表 ***34:*** 一般的な ***UDP*** サービスとそのポート番号

サービス	ポート
ドメイン ネーム システム（DNS）	53
ネットワーク ファイル システム（NFS）	2049
リモート プロシージャ コール（RPC）	111
SNMP	161
TFTP	69

（注） UDP サービスとそのポート番号の完全なリストを表示するには、Router(config)# などのヘルプ文字列を入力します。**prioritylist4protocolipmediumudp?**

（注） 上の表には、より一般的な TCP および UDP ポート番号の一部が示されています。ただし、任意のポート番号を指定して優先順位付けができるため、このリストに制限されるわけではありません。TFTP、FTP などのプロトコルでは、初回のリクエストのみポート 69 を使用します。後続のパケットで使用するのは、ランダムに選択されたポート番号です。これらのプロトコルタイプの場合、ポート番号を使用すると、キュー登録済みのトラフィックを管理する方法としては有効に機能しません。

例

次の例では、任意の優先リスト番号として 1 を割り当て、DECnet をプロトコル タイプに指定し、このインターフェイスから送信する DECnet パケットの優先度レベルを高にします。

```
priority-list 1 protocol decnet high
```

次の例では、200 バイトよりも大きいサイズのすべての DECnet パケットで優先度レベルを中にする方法を示します。

```
priority-list 2 protocol decnet medium gt 200
```

次の例では、200 バイトよりも小さいサイズのすべての DECnet パケットで優先度レベルを中にする方法を示します。

```
priority-list 4 protocol decnet medium lt 200
```

次の例は、IP アクセス リスト 10 に一致するトラフィックの優先度レベルを高にする方法を示します。

```
priority-list 1 protocol ip high list 10
```

次の例は、Telnet パケットの優先度レベルを中にする方法を示します。

```
priority-list 4 protocol ip medium tcp 23
```

次の例は、UDP DNS パケットの優先度レベルを中にする方法を示します。

```
priority-list 4 protocol ip medium udp 53
```

次の例は、イーサネット タイプ コード アクセス リスト 201 に一致するトラフィックの優先度レベルを高にする方法を示します。

```
priority-list 1 protocol bridge high list 201
```

次の例は、TCP カプセル化を使用した Data-Link Switching Plus（DLSw+）の優先度レベルを高にする方法を示します。

```
priority-list 1 protocol ip high tcp 2065
```

次の例は、ダイレクト カプセル化を使用した DLSw+ トラフィックの優先度レベルを高にする方法を示します。

```
priority-list 1 protocol dlsw high
```

（注） このコマンドは、インターフェイスへのパケットの割り当て方法を指定するルールを定義します。ルールを定義したら、**priority-group** コマンドを使用してパケットを実際にインターフェイスへ割り当てます。

関連コマンド

Command	Description
priority-group	指定した優先リストをインターフェイスに割り当てます。
priority-listdefault	優先リストの他の規則に一致しないパケット用にプライオリティキューを割り当てます。
priority-listinterface	特定のインターフェイスから着信するパケットのキューイング プライオリティを確立します。
priority-listqueue-limit	各プライオリティキューで待機可能なパケットの最大数を指定します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

priority-list queue-limit

各プライオリティ キューに待機可能なパケットの最大数を指定するには、グローバル コンフィギュレーション モードで **priority-listqueue-limit** を使用します。normal キューを選択するには、このコマンドの **no** 形式を使用します。

priority-list *list-number* **queue-limit** *high-limit medium-limit normal-limit low-limit*
no priority-list *list-number* **queue-limit**

構文の説明

list-number	優先リストを識別する 1 ～ 16 の番号。
high-limit medium-limit normal-limit low-limit	プライオリティ キューの最大長。4 つの引数のいずれかに 0 値を指定すると、その特定のキューではサイズが無制限になります。これらの引数のデフォルト値については、次の表を参照してください。

コマンド デフォルト

なし。このコマンドの「使用上のガイドライン」セクションの次の表で、デフォルトのキュー制限引数のリストを参照してください。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
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。

使用上のガイドライン

プライオリティ キューがオーバーフローすると、超過したパケットは破棄され、該当する場合はそのプロトコルに関するメッセージを送信できます。

次の表にデフォルトのキュー制限値を示します。

表 *35* : デフォルトのプライオリティ キューのパケット制限数

プライオリティ キューの引数	パケットの制限
high-limit	20
medium-limit	40
normal-limit	60

プライオリティ キューの引数	パケットの制限
low-limit	80

（注） プライオリティ キューイングが有効で、キュー内にアクティブな統合サービス デジタル網（ISDN）コールがある場合、**priority-listqueue-limit** コマンドの設定を変更すると、キューからそのコールがドロップされます。プライオリティ キューイングの詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』を参照してください。

例

次に、プライオリティ キューの最大パケット数を 10 に設定する例を示します。

```
Router(config)# priority-list 2 queue-limit 10 40 60 80
```

関連コマンド

Command	Description
priority-group	指定した優先リストをインターフェイスに割り当てます。
priority-listdefault	優先リストの他の規則に一致しないパケット用にプライオリティ キューを割り当てます。
priority-listinterface	特定のインターフェイスから着信するパケットのキューイング プライオリティを確立します。
priority-listprotocol	プロトコル タイプに基づいてキューイングの優先順位を設定します。
showqueue	特定のインターフェイスまたはVCのキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

priority-queue cos-map

インターフェイス コンフィギュレーション コマンド モードでCoS 値を受信/送信絶対優先キューにマップするには、**priority-queuecos-map** コマンドを使用します。デフォルト マッピングに戻すには、このコマンドの **no** 形式を使用します。

priority-queue cos-map *queue-id cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]
no priority-queue cos-map

構文の説明

queue-id	キュー番号。有効値は **1** です。
cos1	CoS 値。有効値は 0 ～ 7 です。
...cos8	（任意）CoS 値。有効値は、0 ～ 7 です。

コマンド デフォルト

デフォルト マッピングはキュー 1 で、次の受信および送信完全プライオリティ キューで CoS 5 にマッピングされます。

- 1p1q4t 受信キュー
- 1p1q0t 受信キュー
- 1p1q8t 受信キュー
- 1p2q2t 送信キュー
- 1p3q8t 送信キュー
- 1p7q8t 送信キュー
- 1p3q1t 送信キュー
- 1p2q1t 送信キュー

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

完全優先キューに CoS 値をマッピングする場合、次の点に注意してください。

- キュー番号は、常に **1** です。
- キューにマッピングする、最大 8 つの CoS 値を入力できます。

例

次に、ギガビット イーサネット ポート 1/1 の完全プライオリティ キューに、CoS 値 7 をマッピングする例を示します。

```
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)#
```

関連コマンド

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

priority-queue queue-limit

インターフェイスにプライオリティ キューの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 **priority-queuequeue-limit** コマンドを使用します。デフォルトのプライオリティ キュー サイズに戻すには、このコマンドの **no** 形式を使用します。

priority-queue queue-limit パーセント
no priority-queue queue-limit パーセント

構文の説明

パーセント	プライオリティ キュー サイズ（%）。有効な値は 1 ～ 100 です。

コマンド デフォルト

グローバル サービス品質（QoS）が有効な場合は、プライオリティ キュー サイズは 15 です。グローバル QoS が無効な場合は、プライオリティ キュー サイズは 0 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(18)SXF2	このコマンドが導入されました。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

このコマンドは、次のモジュールでサポートされています。

- WS-X6501-10GE--1p2q1t[17]
- WS-X6148A-GE--1p3q8t[18]
- WS-X6148-45--1p3q8t
- WS-X6148-FE-SFP--1p3q8t
- WS-X6748-SFP--1p3q8t
- WS-X6724-SFP--1p7q8t [19]

[17] 1p2q1t：絶対優先キューが 1 つ、各キューに WRED 廃棄しきい値が 1 つ、設定不可（100%）のテールドロップしきい値が 1 つ指定された標準キューが 2 つ。
[18] 1p3q8t：絶対優先キューが 1 つ、各キューに WRED 廃棄しきい値が 8 つ指定された標準キューが 3 つ。
[19] 1p7q8t：絶対優先キューが 1 つ、各キューに WRED 廃棄しきい値が 8 つ指定された標準キューが 7 つ。

- WS-X6704-10GE--1p7q4t[20]
- WS-SUP32-10GB-3E--1p7q4t
- WS-SUP32-GB-3E--1p3q8t
- WS-X6708-10GE--1p7q4t

例

次の例では、インターフェイスにプライオリティ キューサイズを設定する方法を示しています。

```
priority-queue queue-limit 15
```

関連コマンド

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

[20] 1p7q4t：絶対優先キューが 1 つ、各キューに WRED 廃棄しきい値が 4 つ指定された標準キューが 7 つ。

pvc-bundle

仮想回線（VC）をバンドルのメンバーとしてバンドルに追加し、bundle-VC コンフィギュレーション モードにして VC バンドル メンバーを設定するには、バンドル コンフィギュレーション モードで **pvc-bundle** コマンドを使用します。バンドルから VC を削除するには、このコマンドの **no** 形式を使用します。

pvc-bundle *pvc-name* [*vpi/*] [*vci*]
no pvc-bundle *pvc-name* [*vpi/*] [*vci*]

構文の説明

pvc-name	相手先固定接続（PVC）バンドルの名前。
vpi /	（任意）この PVC の ATM ネットワーク仮想パス識別子（VPI）。/ と *vpi* 値がない場合の *vpi* 値のデフォルトは 0 です。 Cisco 7200 および 7500 シリーズ ルータでは、値の範囲は 0 ～ 255 です。Cisco 4500 および 4700 ルータでの値の範囲は 0 ～ 1 で、8192 を **atmvc-per-vp** コマンドで設定した値で割ったときの商より小さい値です。 *vpi* および *vci* 引数は両方を 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。
vci	（任意）この PVC の ATM ネットワーク仮想チャネル識別子（VCI）。この値は 0 ～ 1 の範囲で、**atmvc-per-vp** コマンドによってこのインターフェイスに対して設定された最大値未満です。一般的に、低い値 0 ～ 31 は、特定のトラフィック（運用管理および保守（OAM）、相手先選択接続（SVC）シグナリング、統合ローカルマネジメントインターフェイス（ILMI）など）のために予約されており、使用できません。 VCI は、ATM セルのヘッダーの 16 ビット フィールドです。VCI 値はローカルにだけ意味があるため、単一リンク上でだけ一意であり、ATM ネットワーク全体では一意ではありません。 *vpi* および *vci* 引数は両方を 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。

コマンド デフォルト

なし

コマンド モード

バンドル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
12.0(26)S	このコマンドが Cisco 10000 シリーズ ルータに実装されました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。

リリース	変更箇所
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB 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

各バンドルには、異なるサービス品質（QoS）属性を持つ複数の VC を追加できます。このコマンドは、VC をバンドルに関連付け、そのバンドルのメンバーにします。VC をバンドルに追加するには、バンドルが必要です。**bundle** コマンドを使用してバンドルを作成します。バンドルに追加済みの VC を設定する場合もこのコマンドを使用できます。同様にコマンドを入力して、VC バンドル メンバーの名前を指定します。

pvc-bundle コマンドで bundle-VC コンフィギュレーション モードにして、VC に VC 固有および VC クラスの属性を指定できます。

例

次の例では、bundle1 という名前の既存のバンドルを指定して、バンドル コンフィギュレーション モードにします。その後に 2 つの VC をバンドルに追加します。追加する VC それぞれで、bundle-VC モードにして、VC クラスを VC に割り当て、設定します。

```
bundle bundle1
 pvc-bundle bundle1-control 207
 class control-class
 pvc-bundle bundle1-premium 206
 class premium-class
```

次の例は、bundle1-control という名前の PVC（bundle1 という名前のバンドルの既存のメンバー）を設定し、クラスベース均等化キューイング（CBWFQ）を使用します。この設定例では、policy1 という名前のポリシーマップを PVC に割り当てます。ポリシーマップを割り当てると、policy1 を含むクラスによって、PVC bundle1-control のサービス ポリシーが決定されます。

```
bundle bundle1
 pvc-bundle bundle1-control 207
 class control-class
 service-policy output policy1
```

関連コマンド

Command	Description
atmvc-per-vp	VPI ごとにサポートする VCI の最大数を設定します。
bump	VC バンドルに割り当てることができる VC クラスのバンピング ルールを設定します。
class-bundle	指定された VC クラスに含まれるバンドル レベルのコマンドで VC バンドルを設定します。

Command	Description
class-vc	VC クラスを ATM PVC、SVC、または VC バンドル メンバーに割り当てます。
precedence	バンドルの VC メンバーまたは VC バンドルに割り当て可能な VC クラスに優先レベルを設定します。
protect	VC バンドル メンバーへのアプリケーションの保護されたグループまたは保護された VC ステータスを持つ VC クラスを設定します。
pvc	ATM PVC に名前を割り当て、ATM PVC のカプセル化タイプを指定し、interface-ATM-VC コンフィギュレーション モードに入ります。
ubr	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レートを指定します。
ubr+	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レートと出力最小保証セル レートを指定します。
vbr-nrt	可変ビット レート非リアルタイム（VBR-NRT）QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レート、出力平均セル レート、および、出力最大バースト セル サイズを指定します。

Q から R

- qos police order parent-first （973 ページ）
- qos pre-classify （974 ページ）
- qos shape-timer （976 ページ）
- queue-depth （978 ページ）
- queue-limit （980 ページ）
- queue-limit atm clp （987 ページ）
- queue-list default （989 ページ）
- queue-list interface （991 ページ）
- queue-list lowest-custom （993 ページ）
- queue-list protocol （995 ページ）
- queue-list queue byte-count （998 ページ）
- queue-list queue limit （1000 ページ）
- random-detect （1002 ページ）
- random-detect（VC 単位） （1008 ページ）
- random-detect aggregate （1012 ページ）
- random-detect atm-clp-based （1016 ページ）
- random-detect clp （1018 ページ）
- random-detect cos-based （1020 ページ）
- random-detect discard-class （1022 ページ）
- random-detect discard-class-based （1026 ページ）
- random-detect dscp （1027 ページ）
- random-detect dscp（aggregate） （1035 ページ）
- random-detect ecn （1040 ページ）
- random-detect exponential-weighting-constant （1041 ページ）
- random-detect flow （1045 ページ）
- random-detect flow average-depth-factor （1047 ページ）
- random-detect flow count （1049 ページ）
- random-detect prec-based （1051 ページ）
- random-detect precedence （1053 ページ）

- random-detect precedence（aggregate） （1058 ページ）
- random-detect-group （1062 ページ）
- rate （1065 ページ）
- rate-limit （1066 ページ）
- rcv-queue bandwidth （1071 ページ）
- rcv-queue cos-map （1073 ページ）
- rcv-queue queue-limit （1075 ページ）
- rcv-queue random-detect （1077 ページ）
- rcv-queue threshold （1079 ページ）
- recoverable-loss （1082 ページ）
- redirect interface （1084 ページ）
- refresh max-period （1086 ページ）
- refresh max-time （1088 ページ）
- refresh rtp （1090 ページ）
- rtp （1092 ページ）

qos police order parent-first

サービス品質（QoS）ポリシングアクションを子から親の順序（デフォルト）から親から子の順序に変更するには、グローバル コンフィギュレーション モードで **qospoliceorderparent-first** コマンドを使用します。親が先の順序を無効にし、デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

qos police order parent-first
no qos police order parent-first

構文の説明

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

qospoliceorderparent-first コマンドを入力しないと、子ポリシング アクションが最初に実行され、親ポリシング アクションが次に実行されます。

コマンド モード

グローバル コンフィギュレーション (#)

コマンド履歴

リリース	変更箇所
15.1(1)S	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 Release 15.1(1)S より前のリリースの階層型ポリシング ポリシー マップ（ポリシングを設定した親ポリシーが、同様にポリシングを設定した子ポリシーを含むクラス内にある）では、親ポリシング アクションが最初に実行され、次が子ポリシング アクションでした。

Cisco IOS Release 15.1(1)S 以降では、順序が逆になります。デフォルトでは、子ポリシング アクションが最初で、親ポリシング アクションはその後です。この変更は、ソフトウェア データプレーン ポリサー実装（Cisco 7200、Cisco 7301、および Cisco 7600 FlexWAN および SIP200 ライン カード）のみに適用されます。

子ポリシングアクションが最初に実行されるため、この新しい動作によって、送信後ドロップアクションの結果が向上します。ただし、親および子ポリサーが競合するマーク後送信アクションを実行する場合、親アクションが後に実行されるため、子ではなく親のマーキングが有効になります。

Release 15.1(1)S より前のリリースで有効だったポリシングの順序に戻す必要がある場合のみ、**qospoliceorderparent-first** コマンドを使用します。

例

次の例では、子優先（デフォルト）から親が先で子は後にポリシングの順序を変更する方法を示します。

```
Router# qos police order parent-first
```

qos pre-classify

サービス品質（QoS）事前分類を有効にするには、インターフェイス コンフィギュレーション モードで **qospre-classify** コマンドを使用します。QoS 事前分類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。

qos pre-classify
no qos pre-classify

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

QoS 事前分類は無効です。

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	変更箇所
12.0(5)XE3	このコマンドが導入されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.2(2)T	このコマンドが Cisco 2600 および Cisco 3600 シリーズ ルータに実装されました。
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。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

このコマンドは、トンネルインターフェイス、仮想テンプレート、およびクリプトマップに限定されます。**qospre-classify** コマンドは、その他すべてのインターフェイス タイプで使用できません。

qospre-classify コマンドは IP パケットのみに有効にできます。

（注） QoS 事前分類は、すべてのフラグメント化されたパケットではサポートされません。パケットがフラグメント化される場合、各フラグメントは異なる事前分類を受信できます。

例

次の例では、トンネルインターフェイスおよび仮想テンプレートにバーチャルプライベート ネットワーク（VPN）の QoS 機能を有効にします。

```
Router(config-if)# qos pre-classify
```

関連コマンド

コマンド	説明
showinterfaces	ルータまたはアクセス サーバ上に設定されているインターフェイスの統計情報を表示します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。

qos shape-timer

階層型キューイング フレームワーク（HQF）シェーパー タイマー間隔を指定するには、グローバル コンフィギュレーション モードで **qos shape-timer** コマンドを使用します。シェーパー タイマー間隔設定を削除し、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。

qos shape-timer {**1ms**|**4ms**}

no qos shape-timer {**1ms**|**4ms**}

構文の説明

1ms	HQF シェーパー タイマーを 1 ミリ秒（ms）に設定します。
4ms	HQF シェーパー タイマーをデフォルト値 4 ms に設定します。

コマンド デフォルト

シェーパー タイマー間隔は 4 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	変更箇所
15.1(4)M5	このコマンドが導入されました。

使用上のガイドライン

シェーパー タイマーのデフォルト値は 4 ms ですが、高速なインターフェイスでこの設定をすると、トークン バケットが空になるまで 4 ms ごとのライン レートでバーストが発生する可能性があります。直下にローエンドデバイスがあると、バーストのたびにパケットがドロップされる可能性があります。不要なバースト動作をなくすには、**qos shape-timer** コマンドを使用して、トークン バケットの補充時間を 4 ms から 1 ms に減らします。

シェーパー タイマー間隔を設定するには、まず **qos shape-timer** コマンドを使用して、シェーパー タイマー間隔を設定した後、QoS サービス ポリシーを作成して平均シェープ レートを指定し、最後にそのポリシーをインターフェイスに適用します。ポリシーをインターフェイスに適用すると、シェーパーのトークン バケット補充間隔が、**qos shape-timer** コマンドを使用して設定したパラメータによって決定されます。

（注） **qos shape-timer** コマンドは、ハードウェア補助タイマーがないすべてのサービス統合型ルータ（ISR）で使用できます。

例

次の例では、サービス ポリシーを作成して、インターフェイスに割り当て、シェーパー タイマー間隔を 1 ms に設定します。

```
Router(config)# policy-map myservicepolicy
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 256000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# service-policy output myservicepolicy
Router(config-if)# exit
Router(config)# qos shape-timer 1ms
```

関連コマンド

コマンド	説明
class	ポリシーを作成または変更するクラスの名前を指定するか、デフォルト クラスを指定します。
policy-map	設定するサービス ポリシーの名前を指定します。
service-policy	インターフェイスに付加するサービス ポリシーの名前を指定します。
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。

queue-depth

Open Shortest Path First（OSPF）プロセスがそのキューに保持できる着信パケット数を設定するには、ルータ コンフィギュレーション モードで **queue-depth** コマンドを使用します。キューの深さ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。

queue-depth {**hello**|**update**} {*queue-size*|**unlimited**}
no queue-depth {**hello**|**update**}

構文の説明

hello	OSPF Hello プロセスのキューの深さを指定します。
update	OSPF ルータ プロセス キューのキューの深さを指定します。
queue-size	キュー内のパケットの最大数。指定できる範囲は 1 ～ 2147483647 です。
unlimited	キューの深さを無制限にします。

コマンド デフォルト

キューのサイズが設定されていない場合、OSPF Hello プロセス キューの深さは無制限になり、OSPF ルータ プロセス（更新）キューの深さは 200 パケットになります。

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	変更箇所
12.2(25)S	このコマンドが導入されました。

使用上のガイドライン

すべての着信 OSPF パケットは最初 Hello キューに入ります。OSPF Hello パケットはこのキューから直接処理されますが、その他すべての OSPF パケット タイプは更新キューに移動します。

ルータに多数のネイバーと大規模なデータベースを設定する場合、Hello およびルータ キューのサイズを調整するには、**queue-depth** コマンドを使用します。これを実行しないと、キュー制限が原因でパケットがドロップされ、OSPF 隣接関係が失われる場合があります。

例

次の例では、OSPF 更新キューを 1500 パケットに設定する方法を示します。

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# router ospf 1
Router(config-router)# queue-depth update 1500
```

関連コマンド

コマンド	説明
queue-limit	クラスのキュー制限（サイズ）をバイト単位、ミリ秒（ms）単位、またはパケット単位で指定または変更します。
queue-listqueuelimit	キューに対してキューの長さ制限を指定します。

queue-limit

バイト単位、ミリ秒（ms）単位、マイクロ秒（us）単位、またはパケット単位で、クラスのキュー制限（サイズ）を指定または変更するには、QoS 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-limit** コマンドを使用します。クラスからキューの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* [{**bytes**|**ms**|**us**|**packets**}]
no queue-limit

Cisco ASR 1000 Series Router
queue-limit *queue-limit-size* [{**bytes**|**packets**}]
no queue-limit

Cisco 7600 シリーズ ルータ
queue-limit *queue-limit-size* **[packets]**
no queue-limit

構文の説明

queue-limit-size	キューの最大サイズ。最大値は、指定されたオプションの測定単位キーワード（**bytes**、**ms**、**us**、または **packets**）によって異なります。 （注） オプションの測定単位を指定しなかった場合、デフォルトの測定単位はプラットフォームによって異なります。 （注） Cisco ASR 1000 アグリゲーション サービス ルータでは、バイトが推奨モードです。
bytes	（任意）測定単位がバイトで指定されていることを示します。有効なバイト単位の範囲は 1 ～ 8192000 です。 （注） **bytes** キーワードは、Cisco 7600 シリーズ ルータではサポートされません。 （注） Cisco ASR 1000 シリーズ ルータの場合、バイトの有効な範囲は 1 ～ 64000000 です。

ms	（任意）測定単位がミリ秒で指定されていることを示します。有効なミリ秒単位の範囲は 1 ～ 3400 です。 （注） Cisco 7600 および Cisco ASR 1000 シリーズ ルータでは、**ms** キーワードはサポートされていません。
us	（任意）測定単位がマイクロ秒で指定されていることを示します。有効なマイクロ秒の範囲は 1 ～ 512000 です。

packets	（任意）測定単位がパケットで指定されていることを示します。有効なミリ秒単位の範囲は 1 ～ 32768 ですが、プラットフォームとリリースによって、次のようにさまざまな値になります。 • ESR-PRE1 の場合：パケットのキュー サイズの制限は 32 ～ 16384 の数字で、この数は 2 の累乗にする必要があります。指定する数が 2 の累乗でない場合、デバイスはその数を至近の 2 の累乗の数に変換します。 • Cisco IOS リリース 12.2(15)BX 以降のリリース：パケットのキュー サイズの制限は 32 ～ 16384 の数字です。この数は 2 の累乗にする必要はありません。 • Cisco IOS リリース 12.2(31)SB2 以降のリリース：パケットのキュー サイズの制限は 16 ～ 32767 の数字です。 • Cisco IOS リリース 12.3(7)XI 以降のリリース：インターフェイスに 500 MB 未満のメモリがある場合、パケットのキュー サイズの制限は 8 ～ 4096 の数字で、この数は 2 の累乗にする必要があります。インターフェイスに 500 MB を超えるメモリがある場合、パケットのキュー サイズの制限は 128 ～ 64000 の数字であり、2 の累乗にする必要があります。そうでない場合、デバイスがその数を至近の 2 の累乗に変換します。 • Cisco IOS XE リリース 2.1 以降のリリース：パケットのキュー サイズの制限は 1 ～ 8192000 の数字です。

コマンド デフォルト

Weighted Random Early Detection（WRED）を使用する場合と使用しない場合のクラス キューの **queue-limit** コマンドのデフォルト動作は次のとおりです。

- WRED を使用した場合のクラス キュー：デバイスでは、最も大きい WRED の最大しきい値の 2 倍のデフォルト キュー制限値を至近の 2 の累乗に丸めて使用します。

（注） Cisco IOS Release 12.2(16)BX の場合、デバイスはこの値を至近の 2 の累乗に丸めません。

- WRED を使用しない場合のプライオリティ キューとクラス キュー：デバイスには、ライン レートで 32 パケット以上、256 バイトのパケットの最大 50 ms のバッファがあります。

コマンド モード

QoS ポリシー クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。VIP 対応の Cisco 7500 シリーズ ルータのサポートが追加されました。
12.0(17)SL	このコマンドが Cisco 10000 アグリゲーション シリーズ ルータに実装されました。
12.1(5)T	このコマンドが、VIP 対応の Cisco 7500 シリーズ ルータに実装されました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
12.3(7)XI	このコマンドが Cisco IOS Release 12.3(7)XI 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。
12.4(20)T	次の引数とキーワードの組み合わせが追加されました。 • *queue-limit-size* **bytes** • *queue-limit-size* **ms** • *queue-limit-size* **packets** （注） **bytes** キーワードは Cisco 7600 シリーズ ルータではサポートされず、**ms** キーワードは Cisco 7600 および Cisco ASR 1000 シリーズ ルータでサポートされていません。

リリース	変更箇所
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。
15.0(1)S1	このコマンドが変更され、キュー制限と最小/最大しきい値の計算が向上しました。
15.0(1)M5	このコマンドが変更されました。階層型キューイング フレームワーク（HQF）機能が向上しました。
15.2(2)T	このコマンドが変更されました。**us** キーワードが追加されました。デフォルトの測定単位がパケット数からプラットフォーム依存の単位に変更になりました。
15.4(1)S	このコマンドが、Cisco ASR 901 シリーズ ルータに実装されました。

使用上のガイドライン

重み付け均等化キューイング

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。クラスの一致基準を満たすパケットは、送信されるまでクラス用に確保されているキューに蓄積されます。Fair Queueingプロセスによって、キューでサービスが実行されると、送信が発生します。クラス用に定義した最大パケットしきい値に到達すると、それ以降にクラス キューで待ち状態になるパケットでは、テール ドロップが発生します。または、クラスで WRED が設定されている場合、パケットのドロップが行われます。

Cisco IOS Release 15.0(1)S1 の変更点

Cisco IOS Release 15.0(1)S1 より前のリリースでは、キュー制限が設定されていない場合、現在のクラスのキュー制限は、使用可能なバッファの親値および現在のクラスに割り当てられた帯域幅から計算されました。暗黙の WRED 最小/最大シナリオでは、しきい値は使用可能なバッファから計算されました。

各クラスについては、しきい値は使用可能な集約キュー制限値から計算されました。ユーザ定義のキュー制限設定があっても、WRED 最小/最大しきい値は調整されませんでした。最小/最大しきい値は、このトラフィック クラスから参照可能な「visible_bw」値から取得されました。この一貫性のないキュー制限と最小/最大しきい値の計算が原因で WRED 機能にエラーが発生する可能性がありました。

Cisco IOS Release 15.0(1)S1 以降では、キュー制限は常に親キュー制限と現在のクラスに割り当てられた帯域幅から計算されます。**queue-limit** コマンドを使用して明示的に値を設定する場合、これらの値はキュー制限の定義に使用されます。

機能を最適化するには、**queue-limit** コマンドを使用して、キュー制限設定に基づいて各 WRED クラスの最小/最大しきい値を適切に設定します。

Cisco IOS Release 15.2(2)T の変更点

Cisco IOS Release 15.2(2)T より前のリリースでは、オプションの測定単位が指定されないと、使用する測定単位はパケット数でした。Cisco IOS Release 15.2(2)T 以降では、オプションの測定単位が指定されないと、使用する測定単位はプラットフォーム依存になります。

bandwidth コマンドによるキュー制限の上書き

特定のクラスに対する帯域幅を指定するには、モジュラ QoS CLI（MQC）で **bandwidth** コマンドを使用します。MQC で使用される場合、**bandwidth** コマンドには、クラスにデフォルトのキュー制限があります。このキュー制限は、**queue-limit** コマンドを使用して変更でき、**bandwidth** コマンドによって設定されたデフォルトが上書きされます。

（注） インターフェイスで必要な最小限の保証帯域幅を満たすために、高速インターフェイスでは、**queue-limit** コマンドを使用してデフォルトのキュー制限を変更することが、特に重要です。

階層型キューイング フレームワーク（HQF）の導入以前、メイン インターフェイスにホールドキューが設定されていなかった場合のサブインターフェイスのデフォルトの最大キュー制限は 512 でした。

HQF の一部として、Cisco IOS リリース 15.0(1)M5 以降、この制約は削除されました。現在、最大キュー制限は、メイン インターフェイスのホールドキュー サイズと同程度に高く設定できます。

メインインターフェイスにホールドキューが設定されていない場合、集約キューの制限は1000に引き上げることができます。メインインターフェイスにホールドキューが明示的に設定されている場合、集約キューの制限はホールドキューの値まで引き上げることができます。サブインターフェイス単位の制限はありません。

より高い制限値の集約キューを求めるユーザに対し、設定可能な最大ホールドキュー値 4096 を 240,000 まで引き上げました。ただし、キュー制限とホールドキュー値を高く設定することは推奨しません。

queue-limit コマンドを使用して設定した値は、**qos default queue-limit** コマンドを使用して設定した値を上書きします。

例

次に、policy11 という名前のポリシー マップを設定する例を示します。ポリシー マップ policy11 には、acl203 という名前のクラスが含まれています。このクラス用に確保されているキューの最大キュー サイズが 40 パケットになるよう、このクラスのポリシー マップが設定されます。

```
Device(config)# policy-map policy11
Device(config-pmap)# class acl203
Device(config-pmap-c)# bandwidth 2000
Device(config-pmap-c)# queue-limit 40 packets
```

関連コマンド

Command	Description
bandwidth	H.323 トラフィックの最大集約帯域幅を指定し、宛先ゲートキーパーで使用可能な帯域幅を確認します。

Command	Description
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
classclass-default	帯域幅が設定または変更されるデフォルト トラフィック クラスを指定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
qos default queue-limit	バイト数単位、ミリ秒（ms）単位、マイクロ秒（us）単位、またはパケット数単位で、デバイスのすべての QoS ベース クラスにデフォルトのキュー制限を設定します。

queue-limit atm clp

特定のトラフィック クラスにキューの最大サイズ（セル単位、マイクロ秒単位、またはミリ秒単位）を指定するには、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-limitatmclp** コマンドを使用します。クラスからキュー制限の ATM セル損失率優先度（CLP）値を削除するには、このコマンドの **no** 形式を使用します。

queue-limit atm clp *queue-size* {**cells**|**ms**|**us**}
no queue-limit atm clp

構文の説明

queue-size	しきい値。指定できる範囲は、1 ～ 262144 です。
cells | **ms** | **us**	キュー サイズの測定単位（ms はミリ秒、us はマイクロ秒）。

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

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(30)S	このコマンドが導入されました。

使用上のガイドライン

重み付け均等化キューイング（WFQ）など、他のキューイング機能を指定した場合のみ **queue-limitatmclp** コマンドを使用できます。WFQ では、クラス マップを定義するすべてのクラスにキューが作成されます。ATM CLP ベースの **queue-limit** コマンドを使用して作成したポリシーマップは、Cisco 12000 シリーズ ルータの ATM インターフェイスのみに適用できます。

同じトラフィック クラスを使用して **queue-limit** コマンドを実行した後でないと、**queue-limitatmclp** コマンドを使用できません。

設定済みの場合に、グローバル queue-limit queue-size 値と queue-limit atm clp queue-size 値を削除する場合は、**noqueue-limit** コマンドを使用します。

クラスの一致基準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、重み付け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 キューへの追加パケットのキューイングは、テール ドロップされます。

CLP キュー制限しきい値はセル単位、ミリ秒（ms）単位、またはマイクロ秒（us）単位で指定できます。ただし、測定単位は混在できません。たとえば、CLP キュー制限しきい値をミリ秒で指定した場合は、グローバル キュー制限しきい値もミリ秒で指定する必要があります。

（注） キュー制限しきい値をセル単位、ミリ秒単位、またはマイクロ秒単位で指定すると、内部ではクラスまたはATM仮想回線（VC）で使用可能な表示帯域幅を使用して、セル数に変換されます。

例

次の例では、「POLICY-ATM」という名前のポリシー マップが設定されます。「POLICY-ATM」ポリシー マップには、「CLASS-ATM」という名前のクラスが含まれています。このクラスの帯域幅はパーセンテージ（20）に指定されており、**queue-limit** コマンドによってグローバル キュー制限しきい値が 1000 セルに指定されます。**queue-limitatmclp** コマンドでは、ATM CLP データのキュー制限しきい値が 100 セルに設定されます。

```
Router> enable
Router# configure terminal
Router(config)# policy-map POLICY_ATM
Router(config-pmap)# class CLASS-ATM
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap-c)# queue-limit 1000 cells
Router(config-pmap-c)# queue-limit atm clp 100 cells
Router(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
bandwidth(policy-mapclass)	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。
classclass-default	帯域幅が設定または変更されるデフォルト トラフィック クラスを指定します。
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
queue-limit	ポリシーマップで設定されているクラスに対してキューが保持できるパケットの最大数を指定または変更します。

queue-list default

キュー リストの他のどのルールにも一致しないパケットにプライオリティ キューを割り当てるには、グローバル コンフィギュレーション モードで **queue-listdefault** 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。

queue-list *list-number* **default** *queue-number*
no queue-list *list-number* **default** *queue-number*

構文の説明

list-number	キュー リストの番号。キュー リストを識別するための 1 ～ 16 の番号。
queue-number	キューの番号。1 ～ 16 の数字。

コマンド デフォルト

無効

キュー リストのデフォルトの番号は、キュー番号 1 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	変更箇所
10.0	このコマンドが導入されました。
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。

使用上のガイドライン

複数のルールを使用する場合、システムでは **queue-list** コマンドが表示された順序で読み取られることに注意してください。パケットの分類時に、システムは **queue-list** コマンドで指定されたルール リストから一致するプロトコルまたはインターフェイス タイプを検索します。一致すると、パケットが適切なキューに割り当てられます。システムは指定された順序でリストを検索し、ルールとの初回の一致で検索は終了します。

キュー番号 0 はシステム キューです。その他のキューが処理される前は空です。システムによって、キープアライブなどの高優先度パケットがこのキューに追加されます。

出力キューの現在のステータスを表示するには、**showinterfaces** コマンドを使用します。

例

次の例では、リスト 10 のデフォルト キューがキュー番号 2 に設定されています。

```
queue-list 10 default 2
```

関連コマンド

Command	Description
custom-queue-list	カスタム キュー リストをインターフェイスに割り当てます。
queue-listinterface	インターフェイスに着信するパケットのキューイング プライオリティを確立します。
queue-listprotocol	プロトコル タイプに基づいてキューイング プライオリティを設定します。
queue-listqueuebyte-count	特定のサイクル中に特定のキューからシステムが配信できるバイト数を指定します。
queue-listqueuelimit	キューに対してキューの長さ制限を指定します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

queue-list interface

インターフェイスに着信するパケットのキューイング プライオリティを確立するには、グローバル コンフィギュレーション モードで **queue-listinterface** コマンドを使用します。リストからエントリを削除するには、このコマンドの **no** 形式を使用します。

queue-list *list-number* **interface** *interface-type interface-number queue-number*
no queue-list *list-number* **interface** *interface-type interface-number queue-number*

構文の説明

list-number	キュー リストの番号。キュー リストを識別するための 1 ～ 16 の番号。
interface-type	インターフェイスのタイプ。
interface-number	インターフェイスの番号。
queue-number	キューの番号。1 ～ 16 の数字。

コマンド デフォルト

キューイング プライオリティは確立されません。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
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。

使用上のガイドライン

複数のルールを使用する場合、システムでは **queue-list** コマンドが表示された順序で読み取られることに注意してください。パケットの分類時に、システムは **queue-list** コマンドで指定されたルール リストから一致するプロトコルまたはインターフェイス タイプを検索します。一致すると、パケットが適切なキューに割り当てられます。リストは指定された順序で検索されます。ルールとの初回の一致で検索は終了します。

例

この例では、キュー リスト 4 により、インターフェイス トンネル 3 に着信するパケットにキューイング プライオリティが設定されます。割り当てられたキュー番号は 10 です。

```
queue-list 4 interface tunnel 3 10
```

関連コマンド

Command	Description
custom-queue-list	カスタム キュー リストをインターフェイスに割り当てます。
queue-listdefault	キュー リストの他のルールに一致しないパケット用にプライオリティ キューを割り当てます。
queue-listprotocol	プロトコル タイプに基づいてキューイング プライオリティを設定します。
queue-listqueuebyte-count	特定のサイクル中に特定のキューからシステムが配信できるバイト数を指定します。
queue-listqueue limit	キューに対してキューの長さ制限を指定します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

queue-list lowest-custom

カスタム キューとして処理されるキューに最小の番号を設定するには、グローバル コンフィギュレーション モードで **queue-listlowest-custom** 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。

queue-list *list-number* **lowest-custom** *queue-number*
no queue-list *list-number* **lowest-custom** *queue-number*

構文の説明

list-number	キュー リストの番号。キュー リストを識別するための 1 ～ 16 の番号。
queue-number	キューの番号。1 ～ 16 の数字。

コマンド デフォルト

カスタム キューの最小番号のデフォルト値は 1 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	変更箇所
11.0	このコマンドが導入されました。
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。

使用上のガイドライン

キュー 0 から **queue-listlowest-custom** コマンドで指定されたキューの前までは、すべてのキューでプライオリティ キューが使用されます。（キュー 0 の優先順位が最高になります。）

queue-listlowest-custom コマンドで指定されたキューからキュー 16 までは、すべてラウンドロビン スケジューラを使用します。

現在のカスタム キュー設定を表示するには、**showqueueingcustom** コマンドを使用します。

例

次の例では、キュー リスト 4 の最小カスタム値を 2 に設定します。

```
queue-list 4 lowest-custom 2
```

関連コマンド

Command	Description
custom-queue-list	カスタム キュー リストをインターフェイスに割り当てます。
queue-listinterface	インターフェイスに着信するパケットのキューイング プライオリティを確立します。

Command	Description
queue-listprotocol	プロトコル タイプに基づいてキューイング プライオリティを設定します。
queue-listqueue byte-count	特定のサイクル中に特定のキューからシステムが配信できるバイト数を指定します。
queue-listqueuelimit	キューに対してキューの長さ制限を指定します。
showqueue	特定のインターフェイスまたはVCのキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

queue-list protocol

プロトコル タイプに基づいてキューイング プライオリティを確立するには、グローバル コンフィギュレーション モードで **queue-listprotocol** コマンドを使用します。リストからエントリを削除するには、このコマンドの **no** 形式を使用します。

queue-list *list-number* **protocol** *protocol-name queue-number queue-keyword keyword-value*
no queue-list *list-number* **protocol** *protocol-name queue-number queue-keyword keyword-value*

構文の説明

list-number	キュー リストの番号。1 ～ 16 の数字。
protocol-name	プロトコル タイプ：**aarp**、**appletalk**、**arp**、**bridge**（透過）、**clns**、**clns_es**、**clns_is**、**cmns**、**compressedtcp**、**decnet**、**decnet_node**、**decnet_routerl1**、**decnet_routerl2**、**dlsw**、**ip**、**ipx**、**pad**、**rsrb**、**stun** および **x25**。
queue-number	キューの番号。1 ～ 16 の数字。
queue-keyword keyword-value	使用可能なキーワードは、**fragments, gt, list, lt, tcp** および **udp** です。このキーワードの詳細については、**priority-listprotocol** コマンドを参照してください。

コマンド デフォルト

キューイング プライオリティは確立されません。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
12.2(13)T	このコマンドが変更され、プロトコル タイプのリストから Apollo、VINES、および XNS が削除されました。これらのプロトコルは、Release 12.2(13)T で Apollo Domain、Banyan VINES、および Xerox Network Systems（XNS）が削除されたため、削除されました。
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。

使用上のガイドライン

単一プロトコルで複数のルールを使用する場合、システムでは表示された順序で **queue-list** コマンドが読み取られることに注意してください。パケットの分類時に、システムは **queue-list** コマンドで指定されたルール リストから一致するプロトコルを検索します。一致すると、パ

ケットが適切なキューに割り当てられます。システムは指定された順序でリストを検索し、ルールとの初回の一致で検索は終了します。

decnet_router-l1 キーワードはすべてのレベル 1 ルータ（エリア内ルータ）のマルチキャストアドレスを示し、**decnet_router-l2** キーワードはすべてのレベル 2 ルータ（エリア間ルータ）を示します。

dlsw、**rsrb**、および **stun** キーワードはダイレクト カプセル化のみを意味します。

priority-listprotocol コマンドのドキュメントに記載されている表を使用して、ご使用のシステムのキューイング プライオリティを設定します。

例

次の例では、カスタム キュー リストに 1 を割り当て、プロトコル タイプは DECnet を指定し、このインターフェイスから送信するパケットのキュー番号に 3 を割り当てています。

```
queue-list 1 protocol decnet 3
```

次の例では、200 バイトを超えるサイズの DECnet パケットをキュー番号 2 に割り当てています。

```
queue-list 2 protocol decnet 2 gt 200
```

次の例では、サイズが 200 バイト未満の DECnet パケットをキュー番号 2 に割り当てています。

```
queue-list 4 protocol decnet 2 lt 200
```

次の例では、IP アクセス リスト 10 に一致するトラフィックをキュー番号 1 に割り当てています。

```
queue-list 1 protocol ip 1 list 10
```

次の例では、Telnet パケットをキュー番号 2 に割り当てています。

```
queue-list 4 protocol ip 2 tcp 23
```

次の例では、User Datagram Protocol（UDP）ドメイン ネーム サービス パケットをキュー番号 2 に割り当てています。

```
queue-list 4 protocol ip 2 udp 53
```

次の例では、イーサネット タイプ コード アクセス リスト 201 に一致するトラフィックをキュー番号 1 に割り当てています。

```
queue-list 1 protocol bridge 1 list 201
```

関連コマンド

Command	Description
custom-queue-list	カスタム キュー リストをインターフェイスに割り当てます。

Command	Description
queue-listdefault	キュー リストの他のルールに一致しないパケット用にプライオリティ キューを割り当てます。
queue-listqueuebyte-count	特定のサイクル中に特定のキューからシステムが配信できるバイト数を指定します。
queue-listqueuelimit	キューに対してキューの長さ制限を指定します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

queue-list queue byte-count

特定のサイクル中に特定のキューからシステムが配信できるバイト数を指定するには、グローバル コンフィギュレーション モードで **queue-listqueuebyte-count** コマンドを使用します。バイト カウン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。

queue-list *list-number* **queue** *queue-number* **byte-count** *byte-count-number*
no queue-list *list-number* **queue** *queue-number* **byte-count** *byte-count-number*

構文の説明

list-number	キュー リストの番号。1 ～ 16 の数字。
queue-number	キューの番号。1 ～ 16 の数字。
byte-count-number	特定のサイクル中に特定のキューからシステムが配信できる平均バイト数です。

コマンド デフォルト

このコマンドはデフォルトでは無効になっています。デフォルトのバイト カウントは 1500 バイトです。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
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。

例

次の例では、キュー リスト 9 によって、キュー番号 10 にバイト カウント 1400 を設定します。

```
queue-list 9 queue 10 byte-count 1400
```

関連コマンド

Command	Description
custom-queue-list	カスタム キュー リストをインターフェイスに割り当てます。
queue-listdefault	キュー リストの他のルールに一致しないパケット用にプライオリティ キューを割り当てます。

Command	Description
queue-listinterface	インターフェイスに着信するパケットのキューイング プライオリティを確立します。
queue-listprotocol	プロトコル タイプに基づいてキューイング プライオリティを設定します。
queue-listqueuebyte-count	特定のサイクル中に特定のキューからシステムが配信できるバイト数を指定します。
queue-listqueuelimit	キューに対してキューの長さ制限を指定します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

queue-list queue limit

キューにキューの長さ制限を指定するには、グローバル コンフィギュレーション モードで **queue-listqueuelimit** コマンドを使用します。キューの長さ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。

queue-list *list-number* **queue** *queue-number* **limit** *limit-number*
no queue-list *list-number* **queue** *queue-number* **limit** *limit-number*

構文の説明

list-number	キュー リストの番号。1 ～ 16 の数字。
queue-number	キューの番号。1 ～ 16 の数字。
limit-number	いつでもキューに追加できるパケットの最大数。範囲は 0 ～ 32767 キュー エントリです。この値が 0 の場合、キューのサイズは無制限です。

コマンド デフォルト

デフォルトのキューの長さ制限は 20 エントリです。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
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。

例

次の例では、キュー 10 のキューの長さを 40 に増やします。

```
queue-list 5 queue 10 limit 40
```

関連コマンド

Command	Description
custom-queue-list	カスタム キュー リストをインターフェイスに割り当てます。
queue-listdefault	キュー リストの他のルールに一致しないパケット用にプライオリティ キューを割り当てます。
queue-listinterface	インターフェイスに着信するパケットのキューイング プライオリティを確立します。

Command	Description
queue-listprotocol	プロトコル タイプに基づいてキューイング プライオリティを設定します。
queue-listqueuebyte-count	特定のサイクル中に特定のキューからシステムが配信できるバイト数を指定します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

random-detect

（注） Cisco IOS Release 15.0(1)S および Cisco IOS Release 15.1(3)T のインターフェイス コンフィギュレーション モードでは、**random-detect** コマンドは表示されません。このコマンドは、Cisco IOS ソフトウェアで引き続き使用できますが、コマンドラインで疑問符を入力しても、CLI インタラクティブ ヘルプに表示されません。このコマンドは今後のリリースで、インターフェイス コンフィギュレーション モードから完全に削除されます。つまり、適切な代替コマンド（または一連のコマンド）を使用する必要があります。代わりに使用するコマンドのリストなど、詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

インターフェイス上で重み付けランダム早期検出（WRED）または分散 WRED（DWRED）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 **random-detect** コマンドを使用します。ポリシー マップのクラスに WRED を設定するには、QoS 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 **random-detect** コマンドを使用します。WRED または DWRED を無効にするには、このコマンドの **no** 形式を使用します。

random-detect [{**dscp-based**|**prec-based**}]
no random-detect

構文の説明

dscp-based	（任意）パケットの廃棄確率を計算する場合、WRED で Diffserv コード ポイント（DSCP）の値を使用するよう、指定します。
prec-based	（任意）パケットの廃棄確率を計算する場合、WRED で IP precedence の値を使用するよう、指定します。

コマンド デフォルト

WRED と DWRED は、デフォルトでは無効です。

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）
QoS ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
12.1(5)T	このコマンドが Cisco IOS Release 12.1(5)T に統合されました。差別化サービス（DiffServ）と相対的優先転送（AF）Per Hop Behavior（PHB）をサポートするための引数が追加されました。

リリース	変更箇所
12.1(5a)E	ポリシー マップ クラス コンフィギュレーション モードでのみ、このコマンドが Cisco IOS Release 12.1(5a)E に統合されました。このコマンドが、Versatile Interface Processor（VIP）対応の Cisco 7500 シリーズ ルータと、FlexWAN モジュールが搭載された Catalyst 6000 ファミリ スイッチに、実装されました。
12.0(15)S	QoS ポリシーマップ クラス コンフィギュレーション モードのみで、このコマンドが Cisco IOS Release 12.0(15)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.0(28)S	QoS 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、このコマンドが Cisco IOS Release 12.0(28)S に統合されました。
12.2(28)SB	QoS 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、このコマンドが Cisco IOS Release 12.2(28)SB に統合されました。
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。
12.4(20)T	モジュラ Quality of Service（QoS）CLI（MQC）を使用した階層型キューイング フレームワーク（HQF）のサポートが追加されました。
15.0(1)S	このコマンドが変更されました。このコマンドがインターフェイス コンフィギュレーション モードで非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドがインターフェイス コンフィギュレーション モードで非表示になりました。
Cisco IOS XE 3.6S	このコマンドが変更されました。Cisco ASR 903 ルータのサポートが追加されました。

キーワード

dscp-based キーワードまたは **prec-based** キーワードのいずれも使用しない場合、WRED では、IP プレシデンス値（デフォルト方式）を使用して、パケットの廃棄確率が計算されます。

アベイラビリティ

random-detect コマンドは、Cisco IOS Release 12.1E または 12.0S のインターフェイス レベルでは使用できません。**random-detect** コマンドは、Cisco IOS Releases 12.1E、12.0S、およびそれ以降のリリースのみ、ポリシーマップ クラス コンフィギュレーション モードで使用できます。

WRED の機能

WREDは輻輳回避メカニズムであり、輻輳が存在するときにパケットをランダムにドロップすることで、トラフィックを遅くします。DWRED は WRED に似ていますが、Route Switch Processor（RSP）ではなく、Versatile Interface Processor（VIP）を使用します。WRED と DWRED は、転送速度を下げることによってドロップされるパケットに応答する、Transport Control Protocol（TCP）のようなプロトコルで最も効果的です。

ルータで、WRED計算で使用するパラメータが自動的に定義されます。これらのパラメータを変更するには、**random-detectprecedence** コマンドを使用します。

DWRED をサポートしているプラットフォーム

DWRED 機能は、RSP 7000 カード搭載 Cisco 7000 シリーズ ルータおよび VIP2-40 以降のインターフェイス プロセッサ搭載Cisco 7500 シリーズ ルータでのみサポートされます。VIP のポート アダプタの集約ライン レートが DS3 を上回る場合は、VIP2-50 インターフェイス プロセッサを強く推奨します。OC-3 レートには VIP2-50 インターフェイス プロセッサが必要です。

DWRED を使用するには、まず分散型シスコ エクスプレス フォワーディング スイッチングをインターフェイスで有効にする必要があります。分散型シスコ エクスプレス フォワーディングの詳細については、『*Cisco IOS Switching Services Configuration Guide*』および『*Cisco IOS Switching Services Command Reference*』を参照してください。

ポリシー マップでの WRED

標準クラスまたはデフォルトクラスのポリシーマップの一部として、WREDを指定できます。WRED **random-detect** コマンドおよび重み付け均等化キューイング（WFQ）**queue-limit** コマンドは、どちらか一方を使用します。WRED を設定している場合、そのパケット ドロップ機能を使用して、設定されている最大カウントを超えるパケットがキューで待ち状態になったときのキューが管理されます。WFQ **queue-limit** コマンドを設定すると、テール ドロップが使用されます。

ポリシーマップを設定し、クラスポリシーを作成するには、**policy-map** および **class** (ポリシーマップ) コマンドを使用します。ポリシー マップ内でクラスを作成する場合、次のいずれかのコマンドとともに **random-detect** コマンドを使用できます。

- **bandwidth** (policy-map class)
- **fair-queue** (class-default)：デフォルト クラスのみ

（注） ポリシー マップの 1 つまたは複数のクラスで、テール ドロップの代わりに WRED パケット ドロップを使用する場合、ポリシー マップが付加されているインターフェイスに WRED が設定されていないことを確認する必要があります。

（注） DWRED は、ポリシー マップのクラスではサポートされません。

パケットの廃棄確率を計算する 2 つの方式

このコマンドには、**dscp-based** と **prec-based** の 2 つのオプションのキーワードが含まれており、WRED がパケットの廃棄確率の計算に使用する方式が決定されます。

WRED で使用する方式を決める際には、次の点に注意してください。

- **dscp-based** キーワードを指定すると、WRED では DSCP 値（つまり、IP タイプ オブ サービス（ToS）バイトの最初の 6 ビット）を使用して廃棄確率が計算されます。
- **prec-based** キーワードを指定すると、WRED では IP プレシデンス値を使用して、廃棄確率が計算されます。
- **dscp-based** および **prec-based** キーワードは、どちらかを指定します。
- いずれの引数も指定されない場合、WRED では、IP precedence の値を使用して廃棄確率が計算されます（デフォルト方式）。

例

次の例は、High-Speed Serial Interface（HSSI）0/0/0 インターフェイスで WRED を設定します。

```
interface Hssi0/0/0
 random-detect
```

次に、class1 という名前のクラスに対するポリシーの指定が含まれる、policy1 という名前のポリシーマップを設定する例を示します。輻輳が発生している間は、テール ドロップではなく、WRED パケット ドロップが使用されます。

```
! The following commands create the class map called class1:
class-map class1
 match input-interface fastethernet0/1
! The following commands define policy1 to contain policy specification for class1:
policy-map policy1
 class class1
  bandwidth 1000
  random-detect
```

次に、DSCP 値 8 を使用して、WRED をイネーブルにする例を示します。DSCP 値 8 の最小しきい値は 24 で、最大しきい値は 40 です。この設定はインターフェイス レベルで実行されました。

```
Router(config)# interface serial0/0
Router(config-if)# random-detect dscp-based
Router(config-if)# random-detect dscp 8 24 40
```

次に、クラス c1 の DSCP 値 8 を使用して、WRED をイネーブルにする例を示します。DSCP 値 8 の最小しきい値は 24 で、最大しきい値は 40 です。最後の行では、出力ポリシーまたは仮想回線（VC）p1 に、サービス ポリシーが付加されます。

```
Router(config-if)# class-map c1
Router(config-cmap)# match access-group 101
Router(config-if)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# bandwidth 48
```

```
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial0/0
Router(config-if)# service-policy output p1
```

関連コマンド

コマンド	説明
bandwidth	ポリシー マップに属するクラスに割り当てられる帯域幅を指定するか、変更します。または ATM オーバーヘッド アカウンティングを有効にします。
class	作成または変更するポリシーのクラス名を指定するか、ポリシーを設定する前にデフォルト クラス（一般に class-default クラスといいます）を指定します。
fair-queue	デフォルト クラス ポリシーの一部として class-default クラスで使用するために予約するダイナミック キューの数を指定します。
policy-map	ポリシー マップを作成して、ユーザ ポリシーごとにコントロール プレーン ポリシングおよび保護（CoPP）を定義します。
queue-limit	クラスのキュー制限（サイズ）をバイト単位、ミリ秒（ms）単位、マイクロ秒（us）単位、またはパケット単位で指定または変更します。
random-detectdscp	DSCP 値の最小および最大パケットしきい値を変更します。
random-detectexponential-weighting-constant	平均キュー サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detectflow	フローベース WRED をイネーブルにします。
random-detectprecedence	特定の IP プレシデンスに WRED パラメータと DWRED パラメータを設定します。

コマンド	説明
showinterfaces	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。
showtech-supportrsvp	すべての RSVP 関連情報のレポートを生成します。

random-detect（VC 単位）

（注） Cisco IOS Release 15.1(3)T では、**random-detect**（VC 単位）コマンドは表示されません。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンドラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、今後のリリースで完全に削除されます。詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

仮想回線（VC）単位重み付けランダム早期検出（WRED）または VC 単位 VIP 分散 WRED（DWRED）を有効にするには、VC サブモード モードで **random-detect** コマンドを使用します。VC 単位 WRED および VC 単位 DWRED を無効にするには、このコマンドの **no** 形式を使用します。

random-detect [**attach** *group-name*]
no random-detect [**attach** *group-name*]

構文の説明

attach *group-name*	（任意）WRED または DWRED グループの名前。

コマンド デフォルト

WRED と DWRED は、デフォルトでディセーブルにされます。

コマンド モード

VC サブモード

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
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。このコマンドが非表示になりました。

使用上のガイドライン

WRED は、輻輳が存在するときにランダムにパケットをドロップすることでトラフィックを遅くする輻輳回避メカニズムです。DWRED は WRED に類似していますが、Route Switch Processor（RSP）の代わりに Versatile Interface Processor（VIP）が使用されます。WRED と DWRED は、転送速度を小さくすることによってドロップされるパケットに応答する、TCP のようなプロトコルで最も効果的です。

WRED および DWRED は、インターフェイスおよび VC 単位レベルで設定できます。VC レベルの WRED および DWRED 設定は、WRED および DWRED がインターフェイス レベルでも設定されている場合は、インターフェイス レベル設定をオーバーライドします。

バンドルのメンバーとして単一 ATM VC または VC を設定するには、このコマンドを使用します。

random-detect（VC 単位）コマンドを使用する際には、次の点に注意してください。

- オプションの **attach** キーワードを指定せずにこのコマンドを使用すると、デフォルトの WRED または DWRED パラメータ（最小、最大しきい値など）が使用されます。
- オプションの **attach** キーワードを指定してこのコマンドを使用すると、指定した WRED または DWRED パラメータ グループで定義されたパラメータが使用されます。（WRED または DWRED パラメータ グループは、**random-detect-group** コマンドで定義されます。）指定した WRED または DWRED グループが存在しない場合、VC はデフォルトの WRED または DWRED パラメータで設定されます。

インターフェイス レベル WRED または DWRED グループの設定にこのコマンドを使用して、VC 単位 WRED または DWRED をドロップ ポリシーとして追加する場合、設定した WRED または DWRED グループ パラメータは次の条件で継承されます。

- すべての既存の VC（VC レベル WRED または DWRED グループで明示的に設定されていないリソース予約プロトコル（RSVP）相手先選択接続（SVC）を含む）では、インターフェイス レベル WRED または DWRED グループ パラメータが継承されます。
- シグナリングに使用する VC および暫定ローカル管理インターフェイス（ILMI）VC を除き、インターフェイス レベル DWRED グループの設定後に作成されたすべての VC ではそのパラメータが継承されます。

インターフェイス レベル WRED または DWRED グループ設定が削除されると、VC 単位 WRED または DWRED パラメータが、設定済みインターフェイス レベル WRED または DWRED グループからパラメータを継承した VC すべてから削除されます。

インターフェイス レベル WRED または DWRED グループ設定が変更されると、VC 単位 WRED または DWRED パラメータは、設定済みインターフェイス レベル WRED または DWRED グループ設定からパラメータを継承した場合、それに従って変更されます。

このコマンドは、VC レベル キューイングが可能なインターフェイスでのみサポートされます。現在サポートされているインターフェイスは、拡張 ATM ポート アダプタ（PA-A3）です。

DWRED 機能は、RSP 7000 カード搭載 Cisco 7000 シリーズ ルータおよび VIP2-40 以降のインターフェイス プロセッサ搭載 Cisco 7500 シリーズ ルータでのみサポートされます。VIP のポート アダプタの集約ライン レートが DS3 を上回る場合は、VIP2-50 インターフェイス プロセッサを強く推奨します。OC-3 レートには VIP2-50 インターフェイス プロセッサが必要です。

DWRED を使用するには、まず分散型シスコ エクスプレス フォワーディング（dCEF）スイッチングをインターフェイスで有効にする必要があります。dCEF の詳細については、『Cisco IOS Switching Services Configuration Guide』および『Cisco IOS Switching Services Command Reference』を参照してください。

例

次の例では、cisco という名前の相手先固定接続（PVC）の VC 単位 WRED を設定します。 **attach** キーワードは指定しないため、WRED にはデフォルトのパラメータが使用されます。

```
pvc cisco 46
 random-detect
```

次の例では、Rome という名前の DWRED グループを作成し、パラメータ グループを ATM PVC に適用します。

```
! The following commands create the DWRED parameter group Rome:
random-detect-group Rome
 precedence rsvp 46 50 10
 precedence 1 32 50 10
 precedence 2 34 50 10
 precedence 3 36 50 10
 precedence 4 38 50 10
 precedence 5 40 50 10
 precedence 6 42 50 10
 precedence 7 44 50 10
 exit
exit
! The following commands create a PVC on an ATM interface and then apply the
! DWRED group Rome to that PVC:
interface ATM2/0.23 point-to-point
 ip address 10.9.23.10 255.255.255.0
 no ip mroute-cache
 pvc vc1 201/201
  random-detect attach Rome
  vbr-nrt 2000 1000 200
  encapsulation aal5snap
```

次の **showqueueing** コマンドは、VC 単位 DWRED 設定に従って、各 IP プレシデンスの現在の設定を表示します。

```
Router# show queueing random-detect interface atm2/0.23 vc 201/201
random-detect group Rome:
exponential weight 9
class    min-threshold    max-threshold    mark-probability
------------------------------------------------------------
0        30               50               1/10
1        32               50               1/10
2        34               50               1/10
3        36               50               1/10
4        38               50               1/10
5        40               50               1/10
6        42               50               1/10
7        44               50               1/10
rsvp     46               50               1/10
```

関連コマンド

Command	Description
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。

Command	Description
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detect-group	WRED または DWRED パラメータ グループを定義します。
random-detectprecedence	特定の IP Precedence の WRED パラメータと DWRED パラメータを設定します。
showinterfaces	シリアル インターフェイスに固有の統計情報を表示します。
showqueue	特定のインターフェイスまたはVCのキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

random-detect aggregate

集約重み付けランダム早期検出（WRED）を有効にするには、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 **random-detectaggregate** コマンドを使用します。集約 WRED を無効にするには、このコマンドの **no** 形式を使用します。

random-detect [{**precedence-based**|**dscp-based**}] **aggregate** [**minimum-thresh** *min-thresh* **maximum-thresh** *max-thresh* **mark-probability** *mark-prob*]
no random-detect [{**precedence-based**|**dscp-based**}] **aggregate**

構文の説明

precedence-based	（任意）IP プレシデンス値に基づいて集約 WRED を有効にします。これがデフォルトです。
dscp-based	（任意）DiffServ コードポイント（DSCP）値に基づいて集約 WRED を有効にします。
minimum-thresh *min-thresh*	（任意）個別に設定されていないすべてのサブクラス（IP プレシデンスまたは DSCP 値）に使用する最小しきい値（パケット数）のデフォルト値を設定します。有効な値は 1 ～ 12288 です。
maximum-thresh *max-thresh*	（任意）個別に設定されていないすべてのサブクラス（IP プレシデンスまたは DSCP 値）に使用する最大しきい値（パケット数）のデフォルト値を設定します。有効な値は、最小しきい値引数から 12288 までの範囲です。
mark-probability *mark-prob*	（任意）キューの平均の深さが最大しきい値にあるときにドロップされたパケットの割合の分母のデフォルト値を設定します。この値は、個別に設定されていないすべてのサブクラス（IP プレシデンスまたは DSCP 値）に使用します。有効な値は 1 ～ 255 です。

コマンド デフォルト

precedence-based および **dscp-based** キーワードがこのコマンドで指定されない場合、デフォルトは **precedence-based** です。

デフォルトの集約クラスのオプション パラメータが定義されていない場合、明示的に設定されていないすべてのサブクラス値では、プレーン（重み付けなし）RED ドロップ動作が使用されます。これは、デフォルトでは WRED 動作を常に使用する標準 random-detect コンフィギュレーションとは異なります。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(18)SXE	このコマンドが導入されました。
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。

リリース	変更箇所
12.2(31)SB2	このコマンドが PRE3 用の Cisco 10000 シリーズ ルータで Cisco IOS Release 12.2(31)SB2 に統合されました。

使用上のガイドライン

ATM インターフェイスの場合、集約 WRED 機能では ATM SPA カードが Cisco 7600 SIP-200 キャリア カードまたは Cisco 7600 SIP-400 キャリア カードにインストールされている必要があります。

ATM インターフェイスに WRED を設定するには、random-detect aggregate コマンドを使用する必要があります。標準 random-detect コマンドは ATM インターフェイスでサポートされなくなりました。

precedence-based および **dscp-based** キーワードは、どちらかを指定します。どちらのキーワードも指定しないと、**precedence-based** がデフォルトになります。

デフォルト集約クラスの WRED プロファイル パラメータ値は定義を省略できます。デフォルト集約クラスに適用される WRED プロファイル パラメータが定義されている場合は、明示的に設定されていないすべてのサブクラスにこのパラメータが適用されます。有効なすべての IP precedence または DSCP 値がサブクラスとして定義されている場合は、デフォルト値は指定する必要がありません。デフォルト集約クラスのオプション パラメータが定義されず、IP プレシデンスまたは DSCP 値が未設定のパケットがインターフェイスに着信した場合、プレーン（重み付けなし）RED ドロップ動作が使用されます。

特定の IP プレシデンスまたは DSCP 値に、集約重み付けランダム早期検出（WRED）パラメータを設定するには、ポリシー マップ コンフィギュレーション内でこのコマンドと **random-detectprecedence**(aggregate) または **random-detectdscp**(aggregate) コマンドを使用します。

ポリシー マップが定義された後で、ポリシー マップを VC レベルで割り当てる必要があります。

集約サブクラスの統計情報を表示するには、**showpolicy-mapinterface** コマンドを使用します。

例

次に、ATM インターフェイスのプレシデンス ベース集約 WRED 設定例を示します。まず、prec-aggr-wred という名前のポリシーマップをデフォルト クラスに定義します。次にプレシデンス ベース集約 WRED を **random-detectaggregate** コマンドで有効にした後、一連の **random-detectprecedence**(aggregate) コマンドでサブクラスと WRED パラメータ値を割り当てます。最後に **interface** および **service-policy** コマンドで ATM VC レベルでポリシー マップを割り当てます。

```
Router (config)# policy-map prec-aggr-wred
Router (config-pmap)# class class-default
Router (config-pmap-c)# random-detect aggregate
Router (config-pmap-c)# random-detect precedence values 0 1 2 3 minimum thresh 10
maximum-thresh 100 mark-prob 10
Router (config-pmap-c)# random-detect precedence values 4 5 minimum-thresh 40
maximum-thresh 400 mark-prob 10
Router (config-pmap-c)# random-detect precedence values 6 minimum-thresh 60 maximum-thresh
 600 mark-prob 10
```

```
Router (config-pmap-c)# random-detect precedence values 7 minimum-thresh 70 maximum-thresh
 700 mark-prob 10
Router (config-pmap-c)# interface ATM4/1/0.10 point-to-point
Router (config-subif)# ip address 10.0.0.2 255.255.255.0
Router (config-subif)# pvc 10/110
Router (config-subif)# service-policy output prec-aggr-wred
```

次に、ATM インターフェイスの DSCP ベース集約 WRED 設定例を示します。まず、dscp-aggr-wred という名前のポリシー マップをデフォルト クラスに定義します。次に DSCP ベース集約 WRED を **random-detectdscp-basedaggregate** コマンドで有効にした後、一連の **random-detectdscp** (aggregate) コマンドでサブクラスと WRED パラメータ値を割り当てます。最後に **interface** および **service-policy** コマンドで ATM VC レベルでポリシー マップを割り当てます。

```
Router (config)# policy-map dscp-aggr-wred
Router (config-pmap)# class class-default
Router (config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
 10 mark-prob 10
Router (config-pmap-c)# random-detect dscp values 0 1 2 3 4 5 6 7 minimum-thresh 10
maximum-thresh 20 mark-prob 10
Router (config-pmap-c)# random-detect dscp values 8 9 10 11 minimum-thresh 10
maximum-thresh 40 mark-prob 10
Router (config)# interface ATM4/1/0.11 point-to-point
Router (config-subif)# ip address 10.0.0.2 255.255.255.0
Router (config-subif)# pvc 11/101
Router (config-subif)# service-policy output dscp-aggr-wred
```

関連コマンド

コマンド	説明
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
interface	インターフェイス タイプを設定し、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。
policy-map	1 つまたは複数のインターフェイスに付加してサービス ポリシーを指定するためのポリシーマップを作成します。
random-detectprecedence(aggregate)	特定の IP プレシデンス値に集約 WRED パラメータを設定します。
random-detectdscp(aggregate)	特定の DSCP 値に集約 WRED パラメータを設定します。
service-policy	入力インターフェイスまたはVC、あるいは出力インターフェイスまたはVCに、そのインターフェイスまたはVCのサービス ポリシーとして使用するポリシーマップを対応付けます。

コマンド	説明
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

random-detect atm-clp-based

パケットのATMセル損失率優先度（CLP）に基づいて、重み付けランダム早期検出（WRED）を有効にするには、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 **random-detectatm-clp-based** コマンドを使用します。WRED をディセーブルにするには、このコマンドの **no** 形式を使用します。

random-detect atm-clp-based *clp-value*
no random-detect atm-clp-based

Cisco 10000 シリーズ ルータ
random-detect atm-clp-based *min-thresh-value max-thresh-value mark-probability-denominator-value*
no random-detect atm-clp-based

構文の説明

clp-value	CLP の値。有効な値は、0 または 1 です。
min-thresh-value	パケット数での最小しきい値。有効な値は 1 ～ 4096 です。
max-thresh-value	パケット数での最大しきい値。有効な値は 1 ～ 4096 です。
max-probability-denominator-value	平均キューの深さが最大しきい値の場合にドロップされたパケットの割合の分母。有効な値は 1 ～ 65535 です。

コマンド デフォルト

WREDが設定される場合、最小と最大のデフォルトしきい値は、インターフェイスの出力バッファリング容量と伝送速度に基づいて、決定されます。

デフォルトの最大確率分母は 10 です。

Cisco 10000 シリーズ ルータでは、デフォルトは無効です。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(28)S	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SB	このコマンドが Cisco 10000 シリーズ ルータの PRE3 と PRE4 に追加されました。
12.4(20)T	モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）を使用した階層型キューイング フレームワーク（HQF）のサポートが追加されました。

使用上のガイドライン

同じ HQF 設定では、**random-detectatm-clp-based** コマンドを **random-detectcos-based** コマンドと併用することはできません。**norandom-detectcos-based** コマンドを使用して無効化した後に、**random-detectatm-clp-based** コマンドを設定する必要があります。

例

次の例では、ATM CLP に基づいて WRED が設定されます。この設定では、**random-detectatm-clp-based** コマンドが設定され、ATM CLP に 1 が指定されます。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect atm-clp-based 1
Router(config-pmap-c)#

end
```

関連コマンド

コマンド	説明
random-detectclp	WRED をイネーブルにするために使用される、パケットの ATM CLP の値、最小しきい値、最大しきい値、最大確率分母を指定します。
random-detectcos	WRED をイネーブルにするために使用される、パケットの CoS 値、最小しきい値、最大しきい値、最大確率分母を指定します。
random-detectcos-based	パケットの CoS 値に基づいて、WRED をイネーブルにします。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

random-detect clp

重み付けランダム早期検出（WRED）の有効化に使用する、パケットの ATM セル損失率優先度（CLP）値、最小および最大しきい値、最大確率分母を指定するには、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 **random-detectclp** を使用します。指定された ATM CLP のしきい値と最大確率分母をデフォルト値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。

random-detect clp *clp-value min-threshold max-threshold max-probability-denominator*
no random-detect clp *clp-value min-threshold max-threshold max-probability-denominator*

構文の説明

clp-value	CLP の値。有効な値は、0 または 1 です。
min-threshold	パケット数での最小しきい値。有効な値は 1 ～ 512000000 の範囲です。
max-threshold	パケット数での最大しきい値。有効な値は 1 ～ 512000000 の範囲です。
max-probability-denominator	平均キューの深さが最大しきい値の場合にドロップされたパケットの割合の分母。有効な値は 1 ～ 65535 です。

コマンド デフォルト

min-threshold および *max-threshold* 引数のデフォルト値は、インターフェイスの出力バッファリング容量と伝送速度で決まります。

max-probability-denominator 引数のデフォルト値は 10 です。つまり、10 個のパケットのうち 1 個は最大しきい値でドロップされます。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(28)S	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
15.2(2)T	このコマンドが変更されました。最大しきい値と最小しきい値の範囲が変更されました。

使用上のガイドライン

random-detectclp コマンドを使用する際には、次の点に注意してください。

- 平均キューの長さが最小しきい値に達すると、WRED では、指定された IP precedence で一部のパケットがランダムにドロップされます。
- キューの平均の長さが最大しきい値を超えると、WRED は指定された IP プレシデンス値のすべてのパケットをドロップします。

- *min-threshold* 引数と *max-threshold* 引数の値の範囲は 1 ～ 512000000 ですが、指定可能な実際の値は設定するランダム検出のタイプに応じて異なります。たとえば、最大しきい値がキューの制限を超えることはできません。
- *max-probability-denominator* 引数は、平均キュー深度が最大しきい値に達した場合にドロップするパケットの割合です。たとえば、分母が 512 の場合、平均キューが最大しきい値のときに、512 パケットごとに 1 パケットがドロップされます。

例

次の例では、**random-detectclp** コマンドを使用して WRED を有効にします。**random-detectclp** コマンドを使用して、ATM CLP、最小および最大しきい値、最大確率分母を指定します。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect clp 1 12 25 1/10
Router(config-pmap-c)# end
```

関連コマンド

コマンド	説明
random-detectatm-clp-based	パケットの ATM CLP に基づいて、WRED をイネーブルにします。
random-detectcos	WRED をイネーブルにするために使用される、パケットの CoS 値、最小しきい値、最大しきい値、最大確率分母を指定します。
random-detectcos-based	パケットの CoS 値に基づいて、WRED をイネーブルにします。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

random-detect cos-based

パケットのサービス クラス（CoS）に基づいて、Weighted Random Early Detection（WRED）をイネーブルにするには、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 **random-detectcos-based** コマンドを使用します。WRED をディセーブルにするには、このコマンドの **no** 形式を使用します。

random-detect cos-based *cos-value*
no random-detect cos-based

構文の説明

cos-value	0 ～ 7 の、IEEE 802.1Q CoS の特定の値。

コマンド デフォルト

WRED が設定される場合、最大と最小のしきい値は、出力バッファリング容量とインターフェイスの送信速度に基づいて、決定されます。

デフォルトの最大確率分母は 10 です。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(28)S	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.4(20)T	モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）を使用した階層型キューイング フレームワーク（HQF）のサポートが追加されました。

使用上のガイドライン

同じ HQF 設定では、**random-detectcos-based** コマンドを **random-detectatm-clp-based** コマンドと併用することはできません。**norandom-detectatm-clp-based** コマンドを使用して無効化した後に、**random-detectcos-based** コマンドを設定する必要があります。

例

次の例では、CoS 値に基づいて WRED が設定されます。この設定では、**random-detectcos-based** コマンドが設定され、CoS 値に 2 が指定されます。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect cos-based 2
Router(config-pmap-c)#

end
```

関連コマンド

コマンド	説明
random-detectatm-clp-based	パケットの ATM CLP に基づいて、WRED をイネーブルにします。
random-detectclp	WRED をイネーブルにするために使用される、パケットの ATM CLP の値、最小しきい値、最大しきい値、最大確率分母を指定します。
random-detectcos	WRED をイネーブルにするために使用される、パケットの CoS 値、最小しきい値、最大しきい値、最大確率分母を指定します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

random-detect discard-class

ポリシーマップで廃棄クラス値用の重み付けランダム早期検出（WRED）パラメータをクラスポリシーに設定するには、 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 **random-detectdiscard-class** コマンドを使用します。廃棄クラス値を無効にするには、このコマンドの **no** 形式を使用します。

random-detect discard-class *value min-threshold max-threshold max-probability-denominator*
no random-detect discard-class *value min-threshold max-threshold max-probability-denominator*

構文の説明

value	廃棄クラスです。これは、パケットの廃棄適格を指定する番号です。有効な値は 0 ～ 7 です。
min-threshold	キューで使用可能なパケットの最小数を指定します。平均キューの長さが最小しきい値に達すると、WRED では、指定された DSCP、IP precedence、または廃棄クラスの値で一部のパケットがランダムにドロップされます。有効な最小しきい値は 1 ～ 512000000 です。
max-threshold	キューで使用可能なパケットの最大数。平均キューの長さが最大しきい値を超えると、WRED では、指定された DSCP、IP precedence、または廃棄クラスの値ですべてのパケットがドロップされます。有効な最大しきい値の範囲は 1 ～ 512000000 です。
max-probability-denominator	平均キューの深さが最大しきい値の場合にドロップされたパケットの割合の分母。たとえば、分母が 512 の場合、平均キューが最大しきい値のときに、512 パケットごとに 1 パケットがドロップされます。有効な値は 1 ～ 65535 です。

コマンド デフォルト

すべての優先レベルについて、*max-probability-denominator* のデフォルトは 10 パケットです。つまり、最大しきい値の場合、10 パケットごとに 1 パケットがドロップされます。

コマンド モード

ポリシー マップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
12.2(13)T	このコマンドが Cisco IOS Release 12.2(13)T に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。

リリース	変更箇所
15.2(2)T	このコマンドが変更されました。最大しきい値と最小しきい値の範囲が変更されました。

使用上のガイドライン

インターフェイスで **random-detectdiscard-class** コマンドを設定すると、パケットの廃棄クラスに基づいて、パケットに対する優先処理が行われます。廃棄クラスの異なる廃棄クラス値を調整するには、**random-detectdiscard-class** コマンドを使用します。

（注） *min-threshold* 引数と *max-threshold* 引数の値の範囲は 1 ～ 512000000 ですが、指定可能な実際の値は設定するランダム検出のタイプに応じて異なります。たとえば、最大しきい値がキューの制限を超えることはできません。

Cisco 10000 シリーズ ルータ

random-detectdiscard-class-based コマンドを使用して、最初にドロップ モードを有効にする必要があります。これにより、**random-detectdiscard-class** コマンドを使用して、廃棄確率プロファイルを設定できます。

次の表は、DiffServ コード ポイント（DSCP）、IP プレシデンス、および廃棄クラスに基づいた WRED のデフォルト廃棄しきい値です。廃棄確率は、ルータが 10 パケットあたり 1 パケットをドロップすることを示します。

表 *36 : WRED* のデフォルト廃棄しきい値

DSCP、プレシデンス、および廃棄クラス値	最小しきい値（キュー サイズに対する割合）	最大しきい値（キューサイズに対する割合）	廃棄確率
すべての DSCP	1/4	1/2	1/10
0	1/4	1/2	1/10
1	9/32	1/2	1/10
2	5/16	1/2	1/10
3	11/32	1/2	1/10
4	3/8	1/2	1/10
5	13/32	1/2	1/10
6	7/16	1/2	1/10
7	15/32	1/2	1/10

例

次に、平均キューが 100 パケットの最小しきい値に到達したときに、パケットをランダムにドロップする廃棄クラス 2 を設定し、平均キューが 200 パケットの最大しきい値の場合に 10 パケット中 1 パケットがドロップされる例を示します。

```
policy-map set-MPLS-PHB
 class IP-AF11
  bandwidth percent 40
  random-detect discard-class-based
  random-detect-discard-class 2 100 200 10
```

Cisco 10000 シリーズ ルータ

次の例では、廃棄クラス ベースの WRED を有効にする方法を示します。この例では Silver という名前のクラス マップを、廃棄クラス 3 と 5 に基づいてトラフィックを分類するように設定します。廃棄クラス 3 と 5 に一致するトラフィックは、Premium という名前のポリシー マップの Silver という名前のクラスに割り当てられます。Silver では、最小しきい値が 500、最大しきい値が 1500、mark-probability-denominator が 200 に設定された WRED パケット ドロップが廃棄クラス 5 に基づいて実行されます。QoS ポリシーは、送信方向のポイントツーポイント ATM サブインターフェイス 2/0/0.2 の PVC 1/81 に適用されます。

```
Router(config)# class-map Silver
Router(config-cmap)# match discard-class 3 5
Router(config-cmap)# exit
Router(config)# policy-map Premium
Router(config-pmap)# class Silver
Router(config-pmap-c)# bandwidth percent 30
Router(config-pmap-c)# random-detect discard-class-based
Router(config-pmap-c)# random-detect discard-class 5 500 1500 200
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 2/0/0
Router(config-if)# atm pxf queuing
Router(config-if)# interface atm 2/0/0.2 point-to-point
Router(config-subif)# pvc 1/81
Router(config-subif-atm-vc)# ubr 10000
Router(config-subif-atm-vc)# service-policy output Premium
```

関連コマンド

コマンド	説明
bandwidth(policy-mapclass)	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
matchdiscard-class	特定の廃棄クラスのパケットに一致させます。
random-detectdiscard-class-based	WRED の基礎をパケットのクラス廃棄値にします。
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。

コマンド	説明
random-detectprecedence	特定の IP precedence に対する WRED パラメータと DWRED パラメータを設定します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

random-detect discard-class-based

パケットの廃棄クラス値に基づいて、重み付けランダム早期検出（WRED）を指定する場合は、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 **random-detectdiscard-class-based** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

random-detect discard-class-based
no random-detect discard-class-based

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトはルータにより異なります。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。

使用上のガイドライン

WRED が、IP precedence フィールドではなく廃棄クラスに基づくようにするよう、このコマンドを入力します。

例

次に、パケットの廃棄クラス値に基づいたランダム検出の例をします。

```
policy-map name
 class-name
  bandwidth percent 40
  random-detect discard-class-based
```

関連コマンド

コマンド	説明
matchdiscard-class	特定の廃棄クラスのパケットを照合します。

random-detect dscp

（注） Cisco IOS Release 15.1(3)T のインターフェイス コンフィギュレーション モードでは、**random-detectdscp** は表示されません。このコマンドは、Cisco IOS ソフトウェアで引き続き使用できますが、コマンド ラインで疑問符を入力しても、CLI インタラクティブ ヘルプに表示されません。このコマンドは今後のリリースで、インターフェイス コンフィギュレーション モードから完全に削除されます。つまり、適切な代替コマンド（または一連のコマンド）を使用する必要があります。代替コマンドのリストなど、詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

Diffserv コード ポイント（DSCP）の値に対する最小と最大のパケットしきい値を変更するには、インターフェイスまたは QoS 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 **random-detectdscp** コマンドを使用します。最小および最大パケットしきい値を DSCP 値の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。

random-detect dscp *dscp-value min-threshold max-threshold* [*mark-probability-denominator*]
no random-detect dscp *dscp-value min-threshold max-threshold* [*mark-probability-denominator*]

構文の説明

dscp-value	DSCP 値。DSCP 値には 0 ～ 63 の数値、または次のキーワードのいずれかを指定できます。**af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs7**、**ef**、または **rsvp**。
min-threshold	パケット数での最小しきい値。この引数に指定できる値の範囲は、1 ～ 512000000 です。平均キューの長さが最小しきい値に達すると、重み付けランダム早期検出（WRED）または分散 WRED（DWRED）によって、指定された DSCP の値で一部のパケットがランダムにドロップされます。
max-threshold	パケット数での最大しきい値。この引数の値の範囲は、*min-threshold* 引数の最小値から 512000000 までです。平均キューの長さが最大しきい値を超えると、WRED または DWRED では、指定された DSCP の値ですべてのパケットがドロップされます。
mark-probability-denominator	（任意）キューの平均の深さが最大しきい値にあるときにドロップされたパケットの割合の分母。たとえば、分母が 512 の場合、平均キューが最大しきい値のときに、512 パケットごとに 1 パケットがドロップされます。値の範囲は、1 ～ 65536 です。デフォルトは 10 です。最大しきい値に達したときに、10 パケットにつき 1 つのパケットがドロップされます。

コマンド デフォルト

random-detectdscp コマンドのデフォルト値は、Versatile Interface Processor（VIP）対応の Cisco 7500 シリーズ ルータおよび FlexWAN モジュール（DWRED）が搭載された Catalyst 6000 ファミリ スイッチでは異なります。WRED が動作する他のすべてのプラットフォームには、別のセットのデフォルト値があります。**random-detectdscp** のデフォルト値の詳細については、「使用上のガイドライン」セクションを参照してください。

コマンド モード

インターフェイス コンフィギュレーション（config-if）
QoS ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.1(5)T	このコマンドが導入されました。
12.1(5a)E	ポリシー マップ クラス コンフィギュレーション モードでのみ、このコマンドが Cisco IOS Release 12.1(5a)E に統合されました。このコマンドが、VIP 対応 Cisco 7500 シリーズ ルータと、FlexWAN モジュールが搭載された Catalyst 6000 ファミリ スイッチに実装されました。
12.0(15)S	QoS 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、このコマンドが Cisco IOS Release 12.0(15)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。このコマンドがインターフェイス コンフィギュレーション モードで非表示になりました。
15.2(2)T	このコマンドが変更されました。最大しきい値と最小しきい値の範囲が変更されました。
Cisco IOS XE Release 3.6S	このコマンドが変更されました。Cisco ASR 903 ルータのサポートが追加されました。

使用上のガイドライン

インターフェイス コンフィギュレーション モードで、**random-detect dscp** コマンドを **random-detect** コマンドとともに使用します。

random-detectdscp コマンドは、**random-detect** コマンドをインターフェイス コンフィギュレーション モードで使用しているときに *DSCP* ベースの引数を指定した場合にのみ使用できます。

（注） **random-detectdscp** コマンドは、Cisco IOS Release 12.1E または Release 12.0S のインターフェイス レベルでは使用できません。**random-detectdscp** コマンドは、Cisco IOS Release 12.1E の QoS ポリシーマップ クラス コンフィギュレーション モードだけで使用できます。

VIP 対応 Cisco 7500 シリーズ ルータおよび FlexWAN モジュール搭載 Catalyst 6000 ファミリ スイッチ

すべての IP プレシデンス値については、*mark-probability-denominator* のデフォルト値は 10 で、*max-threshold* 値は、インターフェイスの出力バッファリング容量と伝送速度で決まります。

デフォルトの *min-threshold* 値は IP プレシデンス値に応じて異なります。IP プレシデンス 0 の *min-threshold* の値は、*max-threshold* の値の半分になります。残りの IP プレシデンス値に対応する値は、*max-threshold* の値の半分から *max-threshold* の値までの間に、等間隔に配置されます。

（注） *min-threshold* 引数と *max-threshold* 引数の値の範囲は 1 ～ 512000000 ですが、指定可能な実際の値は設定するランダム検出のタイプに応じて異なります。たとえば、最大しきい値がキューの制限を超えることはできません。

DSCP 値の最大および最小しきい値をユーザが設定しない場合、すべての DSCP 値にはプレシデンス 0 に指定されたものと同じ最小しきい値および最大しきい値が設定されます。

DSCP 値の指定

random-detectdscp コマンドを使用すると、トラフィック クラスごとに DSCP 値を指定できます。DSCP 値には 0 ～ 63 の数値、または次のキーワードのいずれかを指定できます。**af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs7**、**ef**、または **rsvp**。

特定のトラフィック クラスでは、トラフィック クラスごとに 8 つの DSCP の値を設定できます。8 つの precedence の値、12 の相対的優先転送（AF）コード ポイント、1 つの完全優先転送コード ポイント、8 つのユーザ定義の DSCP の値の、あわせて 29 の値を設定できます。

Assured Forwarding コード ポイント

AF コード ポイントを使用すると、ドメインで、他のドメイン（カスタマーなど）から受信する IP パケットに対し、4 つの異なるレベル（4 つの異なる AF クラス）の転送保証を利用できるようになります。4 つの AF クラスのそれぞれに、一定の転送サービス（バッファ スペースおよび帯域幅）が割り当てられます。

それぞれの AF クラスでは、IP パケットが、3 つのドロップ precedence の値（バイナリ 2{010}、4{100}、または 6{110}）の 1 つでマーク付けされます。この 3 つの値は、DSCP ヘッダーの下位 3 つのビットとして存在します。輻輳ネットワーク環境では、パケットのドロップ precedence の値により、AF クラス内のパケットの重要度が決定されます。より高いドロップ precedence

の値を持つパケットは、より低いドロップ precedence の値を持つパケットより先に、廃棄されます。

DSCP 値の上位 3 ビットにより、AF クラスが決定され、下位 3 ビットにより、廃棄確率が決定されます。

Expedited Forwarding コード ポイント

通常、EF コード ポイントは、優先順位が高く、時間依存のデータのマーキングに使用されます。EF コード ポイント マーキングは、precedence の最大値と等しくなります。したがって、EF コード ポイントは、常に、precedence の値 7 と等しくなります。

クラス セレクタの値

クラス セレクタの（CS）の値は、IP precedence の値と等しくなります（たとえば、cs1 は、IP precedence 1 と同じです）。

デフォルト値

次の表は、分散型プラットフォーム上の各 IP プレシデンス値に対応するデフォルトの WRED 最小しきい値です。

表 *37:* 分散型プラットフォームのデフォルトの *WRED* 最小しきい値

IP（優先順位）	クラス セレクタ（CS）の値	最小しきい値（最大しきい値の分数）	値についての注意事項
0	cs0	8/16	ユーザによって設定されていないすべての DSCP の値のしきい値は、IP precedence 0 のしきい値と同じです。
1	cs1	9/16	--
2	cs2	10/16	--
3	cs3	11/16	--
4	cs4	12/16	--
5	cs5	13/16	--
6	cs6	14/16	--
7	cs7	15/16	EF コード ポイントは、IP precedence 7 と常に等しくなります。

VIP 対応 Cisco 7500 シリーズ ルータおよび FlexWAN モジュール搭載 Catalyst 6000 ファミリ スイッチ以外のデフォルト値

VIP 対応 Cisco 7500 シリーズ ルータおよび Catalyst 6000 を除くすべてのプラットフォームには、次の表に示すデフォルト値があります。

WRED で DSCP の値を使用してパケットの廃棄率を計算する場合、DSCP テーブルの 64 のすべてのエントリは、次の表に示すデフォルト値で初期化されます。

表 *38 : random-detect dscp* のデフォルト設定

DSCP（優先順位）	最小しきい値	最大しきい値	マーク確率
0 (0)	20	40	1/10
1	22	40	1/10
2	24	40	1/10
3	26	40	1/10
4	28	40	1/10
5	30	40	1/10
6	32	40	1/10
7	34	40	1/10
8 (1)	22	40	1/10
9	22	40	1/10
10	24	40	1/10
11	26	40	1/10
12	28	40	1/10
13	30	40	1/10
14	32	40	1/10
15	34	40	1/10
16 (2)	24	40	1/10
17	22	40	1/10
18	24	40	1/10
19	26	40	1/10

DSCP（優先順位）	最小しきい値	最大しきい値	マーク確率
20	28	40	1/10
21	30	40	1/10
22	32	40	1/10
23	34	40	1/10
24 (3)	26	40	1/10
25	22	40	1/10
26	24	40	1/10
27	26	40	1/10
28	28	40	1/10
29	30	40	1/10
30	32	40	1/10
31	34	40	1/10
32 (4)	28	40	1/10
33	22	40	1/10
34	24	40	1/10
35	26	40	1/10
36	28	40	1/10
37	30	40	1/10
38	32	40	1/10
39	34	40	1/10
40 (5)	30	40	1/10
41	22	40	1/10
42	24	40	1/10
43	26	40	1/10
44	28	40	1/10
45	30	40	1/10

DSCP（優先順位）	最小しきい値	最大しきい値	マーク確率
46	36	40	1/10
47	34	40	1/10
48 (6)	32	40	1/10
49	22	40	1/10
50	24	40	1/10
51	26	40	1/10
52	28	40	1/10
53	30	40	1/10
54	32	40	1/10
55	34	40	1/10
56 (7)	34	40	1/10
57	22	40	1/10
58	24	40	1/10
59	26	40	1/10
60	28	40	1/10
61	30	40	1/10
62	32	40	1/10
63	34	40	1/10
rsvp	36	40	1/10

例

次に、DSCP 値 8 を使用して、WRED をイネーブルにする例を示します。DSCP 値 8 の最小しきい値は 20、最大しきい値は 40、マーク付けの率は 1/10 です。

```
random-detect dscp 8 20 40 10
```

関連コマンド

コマンド	説明
random-detect	WRED または DWRED をイネーブルにします。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

コマンド	説明
showqueueinginterface	インターフェイスまたはVCのキューイングの統計情報を表示します。

random-detect dscp（aggregate）

特定の DiffServ コード ポイント（DSCP）値に集約重み付けランダム早期検出（WRED）パラメータを設定するには、QoS 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 **random-detectdscpvalues(aggregate)** コマンドを使用します。集約 WRED DSCP 値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。

random-detect dscp *sub-class-val1 sub-class-val2 sub-class-val3 sub-class-val4 min-thresh max-thresh mark-prob*
no random-detect dscp *sub-class-val1 sub-class-val2 sub-class-val3 sub-class-val4 min-thresh max-thresh mark-prob*

Cisco 10000 シリーズ ルータ（PRE3）
random-detect dscp values sub-class-val1 [**. . . [sub-class-val8]**] **minimum-thresh** *min-thresh-value* **maximum-thresh** *max-thresh-value* **mark-prob** *mark-prob-value*
no random-detect dscp values sub-class-val1 [**. . . [sub-class-val8]**] **minimum-thresh** *min-thresh-value* **maximum-thresh** *max-thresh-value* **mark-prob** *mark-prob*

構文の説明

sub-class-val1 *sub-class-val2* *sub-class-val3* *sub-class-val4*	次の WRED プロファイル パラメータ指定に対する DSCP の値が適用されます。最大 8 のサブクラス（DSCP の値）が、コマンドライン インターフェイス（CLI）エントリごとに指定できます。有効な DSCP 値のリストについては、「使用上のガイドライン」を参照してください。
min-thresh	キューで使用可能なパケットの最小数。平均キューの長さが最小しきい値に達すると、WRED では、指定された DSCP の値で一部のパケットがランダムにドロップされます。有効な最小しきい値は 1 ～ 16384 です。
max-thresh	キューで使用可能なパケットの最大数。キューの平均の長さが最大しきい値を超えると、WRED は指定した DSCP 値のすべてのパケットをドロップします。有効な最大しきい値の範囲は 1 ～ 16384 です。
mark-prob	平均キューの深さが最大しきい値の場合にドロップされたパケットの割合の分母。たとえば、分母が 512 の場合、平均キューが最大しきい値のときに、512 パケットごとに 1 パケットがドロップされます。有効な値は 1 ～ 65535 です。
Cisco10000SeriesRouter	

values *sub-class-val1*[...[*subclass-val8*]]	次の WRED プロファイル パラメータ指定に対する DSCP の値が適用されます。最大 8 つのサブクラス（DSCP 値）を各 CLI エントリに指定できます。DSCP 値は、0 ～ 63 の値にすることができます。または、次のキーワードのいずれかにすることができます。**ef**、**af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、または **cs7**
minimum-thresh *min-thresh*	キューで使用可能なパケットの最小数を指定します。平均キューの長さが最小しきい値に達すると、WRED では、指定された DSCP の値で一部のパケットがランダムにドロップされます。有効な最小しきい値は 1 ～ 16384 です。
maximum-thresh *max-thresh*	キューで使用可能なパケットの最大数。キューの平均の長さが最大しきい値を超えると、WRED は指定した DSCP 値のすべてのパケットをドロップします。有効な最大しきい値の範囲は 1 ～ 16384 です。
mark-probability *mark-prob*	平均キュー深度が最大しきい値に達した場合にドロップされるパケットの割合を示す分母を指定します。たとえば、分母が 512 の場合、平均キューが最大しきい値のときに、512 パケットごとに 1 パケットがドロップされます。有効な値は 1 ～ 65535 です。

コマンド デフォルト

すべての優先レベルについて、デフォルトの mark-prob の値は 10 パケットです。

コマンド モード

QoS ポリシーマップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(18)SXE	このコマンドが導入されました。
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。
12.2(31)SB2	このコマンドが Cisco IOS Release 12.2(31)SB2 に統合され、Cisco 10000 シリーズ ルータに実装されました。

使用上のガイドライン

ATM インターフェイスの場合、集約 WRED 機能では ATM SPA カードが Cisco 7600 SIP-200 キャリア カードまたは Cisco 7600 SIP-400 キャリア カードにインストールされている必要があります。

ATM インターフェイスに WRED を設定するには、**random-detectaggregate** コマンドを使用する必要があります。標準 random-detect コマンドは ATM インターフェイスでサポートされなくなりました。

ポリシー マップ コンフィギュレーション内で、このコマンドと **random-detectaggregate** コマンドを使用します。

WREDパラメータを共有しているDSCPの値の各セットについて、このコマンドを繰り返します。

ポリシーマップが定義された後で、ポリシーマップをこのコマンドを仮想回線（VC）レベルで付加する必要があります。

random-detectdscp(aggregate)CLI で定義されたサブクラス（DSCP プレシデンス）値のセットは、単一のハードウェアWREDリソースに集約されます。これらのサブクラスの統計情報も、集約されます。

集約サブクラスの統計情報を表示するには、**showpolicy-mapinterface** コマンドを使用します。

Cisco 10000 シリーズ ルータ

PRE2 の場合、random-detect コマンドでキューのデフォルト プロファイルを指定します。PRE3 の場合、代わりに aggregate random-detect コマンドを使用して、WRED に集約パラメータを設定します。PRE3 でも PRE2 の random-detect コマンドを隠しコマンドとして使用できます。

PRE2 の場合、デフォルト プロファイルのアカウンティングはプレシデンスごとに行います。PRE3 の場合、デフォルトプロファイルのアカウンティングと設定はクラス マップごとに行います。

PRE2 の場合、明示的なしきい値設定をしないと、DSCP またはプレシデンス値のデフォルトしきい値は、プレシデンスごとに指定します。PRE3 の場合、デフォルトしきい値には WRED を設定しません。

PRE2の場合、デフォルトプロファイル内の各プレシデンスのドロップ カウンタには、特定のプレシデンス値と一致するドロップ カウンタのみが含まれます。PRE2 にはデフォルト プロファイルのデフォルトしきい値があるため、CBQOSMIB にはデフォルトしきい値が表示されます。PRE3の場合、デフォルトプロファイル内の各プレシデンスのドロップ カウンタには、デフォルトプロファイルの集約カウンタが含まれており、特定のプレシデンスに対応した個別のカウンタはありません。デフォルト プロファイルにしきい値を設定していない場合、PRE3 のデフォルト プロファイルでは、CBQOSMIB のデフォルトしきい値は表示されません。

DSCP 値

1 つまたは複数の Diffserv コード ポイント（DSCP）値を入力する必要があります。コマンドには、次の任意の組み合わせを含めることができます。

- Differentiated Service Code Point 値を表す数字（0 ～ 63）
- 特定の AF DSCP を識別する af 番号（af11 など）
- 特定の CS DSCP を識別する cs 番号（cs1 など）
- **default**：デフォルト DSCP を持つパケットに一致します。
- **ef**：EF DSCP を持つパケットに一致します。

たとえば、0、1、2、3、4、5、6、または 7 の DCSP 値が必要な場合（指定したすべての IP DSCP 値ではなく、1 つの IP DSCP 値だけが正常な一致基準であることに注意）、**matchdscp01234567** コマンドを入力します。

例

次に、map1 という名前のクラス マップを作成し、map2 という名前のポリシー マップに関連付ける例を示します。設定により、DSCP 8 の最小しきい値 24 と最大しきい値 40 に基づいて、設定によって WRED から map1 パケットがドロップされます。map2 ポリシー マップは、発信 ATM インターフェイス 1/0/0 に割り当てられます。

```
Router(config-if)# class-map map1
Router(config-cmap)# match access-group 10
Router(config-cmap)# exit
Router(config)# policy-map map2
Router(config-pmap)# class map1
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0
Router(config-if)# service-policy output map2
```

次に、ATM インターフェイスの DSCP ベース集約 WRED 設定例を示します。まず、dscp-aggr-wred という名前のポリシー マップをデフォルト クラスに定義します。次に DSCP ベース集約 WRED を **random-detectdscp-basedaggregate** コマンドで有効にした後、一連の **random-detectdscp(aggregate)** コマンドでサブクラスと WRED パラメータ値を割り当てます。最後に **interface** および **service-policy** コマンドで ATM VC レベルでポリシー マップを割り当てます。

```
Router(config)# policy-map dscp-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
 10 mark-prob 10
!
! Define an aggregate subclass for packets with DSCP values of 0-7 and assign the WRED
! profile parameter values for this subclass
Router(config-pmap-c)# random-detect dscp 0 1 2 3 4 5 6 7 minimum-thresh 10 maximum-thresh
 20 mark-prob 10
Router(config-pmap-c) random-detect dscp 8 9 10 11 minimum-thresh 10 maximum-thresh 40
mark-prob 10
Router(config)# interface ATM4/1/0.11 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
Router(config-subif) pvc 11/101
Router(config-subif)# service-policy output dscp-aggr-wred
```

Cisco 10000 シリーズ ルータ

次に、Gold という名前のクラス マップを作成し、Business という名前のポリシー マップに関連付ける例を示します。DSCP 8 の最小しきい値 24 と最大しきい値 40 に基づいて、設定によって WRED は Gold パケットをドロップします。Business ポリシー マップは、発信 ATM インターフェイス 1/0/0 に割り当てられます。

```
Router(config-if)# class-map Gold
```

```
Router(config-cmap)# match access-group 10
Router(config-cmap)# exit
Router(config)# policy-map Business
Router(config-pmap)# class Gold
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp values 8 minimum-thresh 24 maximum-thresh 40
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0
Router(config-if)# service-policy output Business
```

関連コマンド

コマンド	説明
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
interface	インターフェイス タイプを設定し、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。
policy-map	1 つまたは複数のインターフェイスに付加してサービス ポリシーを指定するためのポリシー マップを作成します。
random-detectaggregate	集約 WRED をイネーブルにし、オプションで、デフォルト集約クラスに対するデフォルト WRED パラメータの値を指定します。このデフォルト クラスは、明示的に設定されていないすべてのサブクラスに使用されます。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

random-detect ecn

明示的輻輳通知（ECN）を有効にするには、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 **random-detectecn** コマンドを使用します。ECN を無効にするには、このコマンドの **no** 形式を使用します。

random-detect ecn
no random-detect ecn

構文の説明

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

ECN はデフォルトでディセーブルになっています。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(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

ECN がイネーブルの場合、Weighted Random Early Detection（WRED）が IP precedence の値に基づいている場合でも Diffserv コード ポイント（DSCP）の値に基づいている場合でも、ECN を使用できます。

例

次に、「pol1」という名前のポリシー マップで ECN を有効にする例を示します。

```
Router(config)# policy-map pol1
Router(config-pmap)# class class-default
Router(config-pmap)# bandwidth per 70
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect ecn
```

関連コマンド

コマンド	説明
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

random-detect exponential-weighting-constant

（注） Cisco IOS Release 15.0(1)S および Cisco IOS Release 15.1(3)T のインターフェイス コンフィギュレーション モードでは、**random-detectexponential-weighting-constant** コマンドは表示されません。このコマンドはCisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは今後のリリースで、インターフェイス コンフィギュレーション モードから完全に削除されます。つまり、適切な代替コマンド（または一連のコマンド）を使用する必要があります。代わりに使用するコマンドのリストなど、詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

キューの平均キュー サイズ計算に、重み付けランダム早期検出（WRED）および分散 WRED（DWRED）指数加重係数を設定するには、インターフェイス コンフィギュレーション モードで **random-detectexponential-weighting-constant** を使用します。クラス用に予約されるキューの平均キュー サイズ計算に指数加重係数を設定するには、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 **random-detectexponential-weighting-constant** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

random-detect exponential-weighting-constant *exponent*
no random-detect exponential-weighting-constant

構文の説明

exponent	平均キュー サイズの計算で使用される 1 ～ 16 の指数。

コマンド デフォルト

デフォルトの指数加重係数は 9 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（インターフェイスで使用される場合）
ポリシーマップ クラス コンフィギュレーション（ポリシー マップでクラス ポリシーの指定に使用される場合、またはモジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）で使用される場合）

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
12.0(5)T	このコマンドは、QoS ポリシー マップ コンフィギュレーション コマンドとして使用可能になりました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合され、Versatile Interface Processor（VIP）対応型 Cisco 7500 シリーズ ルータに実装されました。

リリース	変更箇所
12.1(5)T	このコマンドが Cisco IOS Release 12.1(5)T に統合され、VIP 対応型 Cisco 7500 シリーズ ルータに実装されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
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。
15.0(1)S	このコマンドが変更されました。このコマンドがインターフェイス コンフィギュレーション モードで非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドがインターフェイス コンフィギュレーション モードで非表示になりました。

使用上のガイドライン

WREDは、輻輳が存在するときにランダムにパケットをドロップすることでトラフィックを遅くする輻輳回避メカニズムです。DWREDはWREDに類似していますが、Route Switch Processor（RSP）の代わりにVIPが使用されます。WREDとDWREDは、転送速度を小さくすることによってドロップされるパケットに応答する、TCPのようなプロトコルで最も効果的です。

WREDおよびDWREDサービスの平均キュー サイズ計算に使用される指数を変更するには、このコマンドを使用します。クラス用に確保されるキューの平均キューサイズ計算の指数加重係数を設定する場合にも、このコマンドを使用できます。

（注） デフォルトの WRED または DWRED パラメータ値は、最適な使用可能データに基づきます。値を変更することでアプリケーションに利点があると判断した場合を除き、パラメータのデフォルト値を変更しないことを推奨します。

DWRED 機能はクラス ポリシーではサポートされません。

DWRED 機能は、RSP 7000 カード搭載 Cisco 7000 シリーズ ルータおよび VIP2-40 以降のインターフェイス プロセッサ搭載 Cisco 7500 シリーズ ルータでのみサポートされます。VIP のポート アダプタの集約ライン レートが DS3 を上回る場合は、VIP2-50 インターフェイス プロセッサを強く推奨します。OC-3 レートには VIP2-50 インターフェイス プロセッサが必要です。

DWRED を使用するには、まず分散型シスコ エクスプレス フォワーディング（dCEF）スイッチングをインターフェイスで有効にする必要があります。dCEF の詳細については、『Cisco IOS IP Switching Configuration Guide』および『Cisco IOS IP Switching Command Reference』を参照してください。

例

次に、重み係数が 10 のインターフェイスで WRED を設定する例を示します。

```
interface Hssi0/0/0
 description 45Mbps to R1
 ip address 10.200.14.250 255.255.255.252
 random-detect
 random-detect exponential-weighting-constant 10
```

次に、class1 という名前のクラスに対するポリシーの指定が含まれる、policy1 という名前のポリシーマップを設定する例を示します。輻輳が発生している間は、テール ドロップではなく、WRED パケット ドロップが使用されます。class1 のキューの平均キュー サイズ計算に使用される加重係数は 12 です。

```
! The following commands create the class map called class1:
class-map class1
 match input-interface FE0/1
! The following commands define policy1 to contain policy specification for class1:
policy-map policy1
 class class1
 bandwidth 1000
 random-detect
 random-detect exponential-weighting-constant 12
```

次に、int10 というトラフィック クラスのポリシーを設定して、指数加重係数を 12 に設定する例を示します。これは、トラフィック クラス int10 のキューの平均キュー サイズ計算に使用される加重係数です。トラフィック クラス int10 では、輻輳回避のためにテール ドロップではなく WRED パケットのドロップが使用されます。

```
policy-map policy12
 class int10
 bandwidth 2000
 random-detect exponential-weighting-constant 12
```

関連コマンド

Command	Description
bandwidth(policy-mapclass)	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。
exponential-weighting-constant	WRED パラメータ グループの平均キュー サイズ計算のための指数加重係数を設定します。
fair-queue(class-default)	デフォルト クラス ポリシーの一部として class-default クラスで使用するために予約するダイナミック キューの数を指定します。
precedence	VC バンドルまたは PVC バンドルに割り当てることができ、したがって、そのバンドルのすべてのメンバーに適用される、VC クラスまたは PVC クラスの precedence レベルを設定します。
precedence (WREDgroup)	特定の IP Precedence に対して WRED グループを設定します。
random-detectdscp	DSCP 値の最小および最大パケットしきい値を変更します。
random-detect(perVC)	per-VC WRED または per-VC DWRED をイネーブルにします。

Command	Description
random-detectprecedence	特定の IP Precedence の WRED パラメータと DWRED パラメータを設定します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

random-detect flow

（注） Cisco IOS Release 15.1(3)T では、**random-detectflow** コマンドは表示されません。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンドラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、今後のリリースで完全に削除されます。詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

フローベース重み付けランダム早期検出（WRED）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 **random-detectflow** コマンドを使用します。フローベース WRED を無効にするには、このコマンドの **no** 形式を使用します。

random-detect flow
no random-detect flow

構文の説明

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

フローベース WRED はデフォルトでは無効です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
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。このコマンドが非表示になりました。

使用上のガイドライン

random-detectflowaverage-depth-factor および **random-detectflowcount** コマンドを使用して、フローベース WRED のパラメータを詳細に設定する前に、このコマンドを使用してフローベース WRED を有効にする必要があります。

フローベース WRED を有効にする前に、WRED を有効にして、設定する必要があります。詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』を参照してください。

例

次の例では、シリアル インターフェイス 1 でフローベース WRED を有効にします。

```
interface Serial1
 random-detect
 random-detect flow
```

関連コマンド

Command	Description
random-detectdscp	DSCP値の最小および最大パケットしきい値を変更します。
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detectflowaverage-depth-factor	乗数を、フローベース WRED が有効な場合にフローの平均深度係数の決定に使用するために設定します。
random-detectflowcount	フローベース WRED のフロー カウントを設定します。
random-detectprecedence	特定の IP Precedence の WRED パラメータと DWRED パラメータを設定します。
showinterfaces	シリアル インターフェイスに固有の統計情報を表示します。
showqueue	特定のインターフェイスまたはVCのキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

random-detect flow average-depth-factor

（注） Cisco IOS Release 15.1(3)T では、**random-detectflowaverage-depth-factor** コマンドは表示されません。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンドラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、今後のリリースで完全に削除されます。詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

乗数を、フローベース重み付けランダム早期検出（WRED）の有効時にフローの平均深度係数の決定のために設定する場合は、インターフェイス コンフィギュレーション モードで **random-detectflowaverage-depth-factor** コマンドを使用します。現在のフローの平均深度係数値を削除するには、このコマンドの **no** 形式を使用します。

random-detect flow average-depth-factor *scaling-factor*
no random-detect flow average-depth-factor *scaling-factor*

構文の説明

scaling-factor	スケール係数は 1 から 16 までの番号を使用できます。

コマンド デフォルト

デフォルトの平均深度係数は 4 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
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。このコマンドが非表示になりました。

使用上のガイドライン

各フローで使用可能なバッファ数のスケーリング、および各アクティブ フローの出力キューで使用可能なパケット数の決定に、フローベース WRED が使用する必要があるスケール係数を指定するには、このコマンドを使用します。このスケール係数は、すべてのフローで共通です。測定したバッファ数の結果は、フローごとの制限になります。

このコマンドを使用せず、フローベース WRED が有効な場合、平均深度スケール係数のデフォルト値は 4 です。

フローは適応型ではないと見なされます。つまり、平均フロー深度と指定された乗数（スケール係数）をかけたものが、次のようにフロー深度より小さい場合、リソースを過剰に占有します。

average-flow-depth * (scaling factor) < flow-depth

このコマンドを使用する前に、**random-detectflow** コマンドを使用して、インターフェイスでフローベース WRED を有効にする必要があります。フローベース WRED を設定するには、**random-detectflowcount** コマンドも使用できます。

例

次の例では、シリアル インターフェイス 1 でフローベース WRED を有効にして、平均フロー深度のスケール係数を 8 に設定します。

```
interface Serial1
 random-detect
 random-detect flow
 random-detect flow average-depth-factor 8
```

関連コマンド

Command	Description
random-detectdscp	DSCP値の最小および最大パケットしきい値を変更します。
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detectflow	フローベース WRED をイネーブルにします。
random-detectflowcount	フローベース WRED のフロー カウントを設定します。
random-detectprecedence	特定の IP Precedence の WRED パラメータと DWRED パラメータを設定します。
showinterfaces	シリアル インターフェイスに固有の統計情報を表示します。
showqueue	特定のインターフェイスまたはVCのキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

random-detect flow count

（注） Cisco IOS Release 15.1(3)T では、**random-detectflowcount** コマンドは表示されません。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、今後のリリースで完全に削除されます。詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

フローベース重み付けランダム早期検出（WRED）にフロー カウントを設定するには、インターフェイス コンフィギュレーション モードで **random-detectflowcount** コマンドを使用します。現在のフロー カウント値を削除するには、このコマンドの **no** 形式を使用します。

random-detect flow count *number*
no random-detect flow count *number*

構文の説明

number	16 ～ 215（32768）の値を指定します。

コマンド デフォルト

256

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
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。このコマンドが非表示になりました。

使用上のガイドライン

このコマンドを使用する前に、**random-detectflow** コマンドを使用して、インターフェイスでフローベース WRED を有効にする必要があります。

例

次の例では、シリアル インターフェイス 1 でフローベース WRED を有効にして、フローしきい値定数を 16 に設定します。

```
interface Serial1
 random-detect
```

```
random-detect flow
random-detect flow count 16
```

関連コマンド

Command	Description
random-detectdscp	DSCP値の最小および最大パケットしきい値を変更します。
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detectflow	フローベース WRED をイネーブルにします。
random-detectprecedence	特定の IP Precedence の WRED パラメータと DWRED パラメータを設定します。
showinterfaces	シリアル インターフェイスに固有の統計情報を表示します。
showqueue	特定のインターフェイスまたはVCのキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

random-detect prec-based

（注） Cisco IOS Release 12.4(20)T では、**random-detectprec-based**コマンド **isreplacedbytherandom-detectprecedence-basedcommand.Seetherandom-detectprecedence-based** コマンド **formoreinformation.**

重み付けランダム早期検出（WRED）をパケットの precedence 値に基づくようにするには、**random-detectprec-based** コマンドをポリシーマップ 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。

random-detect prec-based
no random-detect prec-based

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

WRED はデフォルトでディセーブルになっています。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(28)S	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.4(20)T	このコマンドは、ポリシー マップ内では **random-detectprecedence-based** コマンドに置き換えられました。

使用上のガイドライン

random-detectprec-based コマンドでは、WRED はパケットの IP precedence 値に基づきます。

random-detectprecedence コマンドを設定する前に **random-detectprec-based** コマンドを使用します。

Cisco IOS Release 12.4(20)T 以降では、ポリシー マップを設定する場合、**random-detectprecedence** コマンドを使用します。

例

次に、パケットの precedence の値に基づいたランダム検出の例をします。

```
Router> enable
Router# configure terminal
Router(config)#

policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 80
```

```
Router(config-pmap-c)# random-detect precedence-based
Router(config-pmap-c)# random-detect precedence 2 500 ms 1000 ms
Router(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
random-detect	WRED または DWRED をイネーブルにします。
random-detectprecedence	特定の IP precedence に対する WRED パラメータと DWRED パラメータを設定します。クラス ポリシーの特定の IP precedence に対する WRED パラメータを、ポリシーマップで設定します。

random-detect precedence

（注） Cisco IOS Release 15.0(1)S および Cisco IOS Release 15.1(3)T のインターフェイス コンフィギュレーション モードでは、**random-detectprecedence** コマンドは表示されません。このコマンドは、Cisco IOS ソフトウェアで引き続き使用できますが、コマンド ラインで疑問符を入力しても、CLIインタラクティブ ヘルプに表示されません。このコマンドは今後のリリースで、インターフェイス コンフィギュレーション モードから完全に削除されます。つまり、適切な代替コマンド（または一連のコマンド）を使用する必要があります。代替コマンドのリストなど、詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

特定のIPプレシデンスに重み付けランダム早期検出（WRED）および分散WRED（DWRED）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 **random-detectprecedence** コマンドを使用します。ポリシー マップのクラス ポリシーの特定の IP プレシデンスに WRED パラメータを設定するには、QoS 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 **random-detectprecedence** コマンドを使用します。precedence のデフォルトに値を戻すには、このコマンドの **no** 形式を使用します。

random-detect precedence {*precedence*|**rsvp**} *min-threshold max-threshold mark-probability-denominator*
no random-detect precedence

構文の説明

precedence	IP precedence 番号。値の範囲は、0 ～ 7 です。RSP7000 インターフェイス プロセッサを搭載した Cisco 7000 シリーズ ルータおよび VIP2-40 インターフェイス プロセッサ（VIP2-50 インターフェイスプロセッサを強く推奨）を搭載したCisco 7500 シリーズルータについては、プレシデンス値の範囲が 0 ～ 7 になります。「使用上のガイドライン」セクションの表 1 を参照してください。
rsvp	リソース予約プロトコル（RSVP）トラフィックを示します。
min-threshold	パケット数での最小しきい値。この引数に指定できる値の範囲は、1 ～ 512000000 です。平均キューの長さが最小しきい値に達すると、WRED または DWRED では、指定された IP プレシデンスで一部のパケットがランダムにドロップされます。
max-threshold	パケット数での最大しきい値。この引数の値の範囲は、*min-threshold* 引数の最小値から 512000000 までです。平均キューの長さが最大しきい値を超えると、WRED またはDWRED では、指定された IP precedence の値ですべてのパケットがドロップされます。

mark-probability-denominator	平均キューの深さが最大しきい値の場合にドロップされたパケットの割合の分母。たとえば、分母が 512 の場合、平均キューが最大しきい値のときに、512 パケットごとに 1 パケットがドロップされます。値の範囲は、1 ～ 65536 です。デフォルトは 10 です。つまり、最大しきい値に達したときに、10 パケットにつき 1 つのパケットがドロップされます。

コマンド デフォルト

すべてのプレシデンスで、*mark-probability-denominator* のデフォルト値は 10 で、*max-threshold* 値は、インターフェイスの出力バッファリング容量と伝送速度で決まります。

デフォルトの *min-threshold* 値は precedence の値に応じて異なります。IP precedence 0 の *min-threshold* の値は、*max-threshold* の値の半分になります。残りの precedence 値は、*max-threshold* の値の半分から *max-threshold* の値までの間に、等間隔に配置されます。各 IP precedence のデフォルトの最小しきい値の一覧については、このコマンドの「使用上のガイドライン」のセクションにある表を参照してください。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

QoS ポリシー クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
12.4(20)T	モジュラ Quality of Service（QoS）CLI（MQC）を使用した階層型キューイング フレームワーク（HQF）のサポートが追加されました。 （注） QoS ポリシーマップ コンフィギュレーション モードでは、**random-detect prec-based** コマンドは、このコマンドによって置き換えられます。
15.0(1)S	このコマンドが変更されました。このコマンドがインターフェイス コンフィギュレーション モードで非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドがインターフェイス コンフィギュレーション モードで非表示になりました。
15.2(2)T	このコマンドが変更されました。最大しきい値と最小しきい値の範囲が変更されました。

リリース	変更箇所
Cisco IOS XE Release 3.6S	このコマンドが変更されました。Cisco ASR 903 ルータのサポートが追加されました。

使用上のガイドライン

WREDは輻輳回避メカニズムであり、輻輳が存在するときにパケットをランダムにドロップすることで、トラフィックを遅くします。DWRED は WRED に似ていますが、Route Switch Processor（RSP）ではなく、Versatile Interface Processor（VIP）を使用します。

インターフェイスで **random-detect** コマンドを設定すると、パケットの IP precedence に基づいて、パケットに対する優先処理が行われます。異なる precedence に対する処理を調節するには、**random-detectprecedence** コマンドを使用します。

WRED または DWRED でドロップするパケットを決定する際にプレシデンスを無視する場合は、各プレシデンスに同じパラメータでこのコマンドを入力します。最小しきい値および最大しきい値には、適切な値を設定します。

random-detectprecedence コマンドを使用してクラス ポリシー内の異なる precedence に対する処理を調節する場合、そのサービス ポリシーを適用するインターフェイスに WRED が設定されていないことを確認する必要があります。

（注） *min-threshold* 引数と *max-threshold* 引数の値の範囲は 1 ～ 512000000 ですが、指定可能な実際の値は設定するランダム検出のタイプに応じて異なります。たとえば、最大しきい値がキューの制限を超えることはできません。

次の表に、各 IP プレシデンスのデフォルト最小しきい値を示します。

表 *39* : デフォルト *WRED* および *DWRED* 最小しきい値

	最小しきい値（最大しきい値の分数）	
IP プレシデンス	WRED	DWRED
0	9/18	8/16
1	10/18	9/16
2	11/18	10/16
3	12/18	11/16
4	13/18	12/16
5	14/18	13/16
6	15/18	14/16
7	16/18	15/16

	最小しきい値（最大しきい値の分数）	
rsvp	17/18	—

（注） デフォルトの WRED または DWRED パラメータ値は、最適な使用可能データに基づきます。値を変更することでアプリケーションに利点があると判断した場合を除き、パラメータのデフォルト値を変更しないことを推奨します。

DWRED 機能は、RSP 7000 カード搭載 Cisco 7000 シリーズ ルータおよび VIP2-40 以降のインターフェイス プロセッサ搭載 Cisco 7500 シリーズ ルータでのみサポートされます。VIP のポート アダプタの集約ライン レートが DS3 を上回る場合は、VIP2-50 インターフェイス プロセッサを強く推奨します。OC-3 レートには VIP2-50 インターフェイス プロセッサが必要です。

DWRED を使用するには、まず分散型シスコ エクスプレス フォワーディング（dCEF）スイッチングをインターフェイスで有効にする必要があります。dCEF の詳細については、『*Cisco IOS IP Switching Configuration Guide*』および『*Cisco IOS IP Switching Command Reference*』を参照してください。

（注） DWRED 機能はクラス ポリシーではサポートされません。

例

次に、インターフェイスで WRED をイネーブルにし、さまざまな IP precedence にパラメータを指定する設定例を示します。

```
interface Hssi0/0/0
 description 45Mbps to R1
 ip address 10.200.14.250 255.255.255.252
 random-detect
 random-detect precedence 0 32 256 100
 random-detect precedence 1 64 256 100
 random-detect precedence 2 96 256 100
 random-detect precedence 3 120 256 100
 random-detect precedence 4 140 256 100
 random-detect precedence 5 170 256 100
 random-detect precedence 6 290 256 100
 random-detect precedence 7 210 256 100
 random-detect precedence rsvp 230 256 100
```

次に、policy10 という名前のポリシーマップ内の acl10 という名前のクラスのポリシーを設定する例を示します。クラス acl101 には、次のような特性があります。輻輳の発生時にこのクラスに最低 2000 Kb/s の帯域幅が提供され、平均キュー サイズの計算に重み係数 10 が使用されます。輻輳回避のために、テール ドロップではなく WRED パケットのドロップが使用されます。レベル 0 ～ 4 の IP precedence はリセットされます。

```
policy-map policy10
class acl10
 bandwidth 2000
```

```
random-detect
random-detect exponential-weighting-constant 10
random-detect precedence 0 32 256 100
random-detect precedence 1 64 256 100
random-detect precedence 2 96 256 100
random-detect precedence 3 120 256 100
random-detect precedence 4 140 256 100
```

関連コマンド

コマンド	説明
bandwidth(policy-mapclass)	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
fair-queue(class-default)	デフォルト クラス ポリシーの一部として class-default クラスで使用するために予約するダイナミック キューの数を指定します。
random-detect(perVC)	VC 単位 WRED または VC 単位 DWRED を有効にします。
random-detectdscp	DSCP 値の最小および最大パケットしきい値を変更します。
random-detectexponential-weighting-constant	平均キュー サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detectflowcount	フローベース WRED のフロー カウントを設定します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueuing	すべてまたは選択した設定済みキューイング戦略を表示します。

random-detect precedence（aggregate）

特定の IP プレシデンス値に集約重み付けランダム早期検出（WRED）パラメータを設定するには、 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 **random-detectprecedence**(aggregate) コマンドを使用します。集約 WRED プレシデンス値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。

random-detect precedence *sub-class-val1* [*sub-class-val2 sub-class-val3* **sub-class-val4**] *min-thresh max-thresh mark-prob*
no random-detect precedence *sub-class-val1* [*sub-class-val2 sub-class-val3 sub-class-val4*]

構文の説明

s *ub-class-val 1 sub-class-val 2* **s** *ub-class-val 3* **s** *ub-class-val 4*	次の WRED プロファイル パラメータ指定に対する IP プレシデンス値が適用されます。最大4つのサブクラス（IPプレシデンス値）が、コマンド ライン インターフェイス（CLI）エントリごとに指定できます。値の範囲は、0 ～ 7 です。
min-thresh	サブクラスの最小しきい値（パケット数）。有効な値は1～12288です。
max-thresh	サブクラスの最大しきい値（パケット数）を指定します。有効な値は、最小しきい値引数から 12288 までの範囲です。
mark-prob	平均キュー深度がサブクラスの最大しきい値に達した場合にドロップされるパケットの割合を示す分母を指定します。有効な値は 1 ～ 255 です。
Cisco10000SeriesRouter	次の WRED プロファイル パラメータ指定に対する IP プレシデンス値が適用されます。最大 8 つのサブクラス（IP precedence 値）を各 CLI エントリに指定できます。値の範囲は、0 ～ 7 です。
s *ub-class-val 1* [...[*subclass-val8*]]	
minimum-threshmin-thresh	キューで使用可能なパケットの最小数を指定します。平均キューの長さが最小しきい値に達すると、WRED では、指定された IP プレシデンス値で一部のパケットがランダムにドロップされます。有効な最小しきい値は 1 ～ 16384 です。
maximum-threshmax-thresh	キューで使用可能なパケットの最大数。平均キューの長さが最大しきい値を超えると、WRED は指定された IP プレシデンス値のすべてのパケットをドロップします。有効な最大しきい値の範囲は 1 ～ 16384 です。
mark-probabilitymark-prob	平均キュー深度が最大しきい値に達した場合にドロップされるパケットの割合を示す分母を指定します。たとえば、分母が 512 の場合、平均キューが最大しきい値のときに、512 パケットごとに 1 パケットがドロップされます。有効な値は 1 ～ 65535 です。

コマンド デフォルト

すべての優先レベルについて、デフォルトの mark-prob の値は 10 パケットです。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(17)SL	このコマンドが Cisco 10000 シリーズ ルータに追加されました。
12.2(18)SXE	このコマンドが導入されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、PRE3 用の Cisco 10000 シリーズ ルータに実装されました。

使用上のガイドライン

ATM インターフェイスの場合、集約 WRED 機能では ATM SPA カードが Cisco 7600 SIP-200 キャリア カードまたは Cisco 7600 SIP-400 キャリア カードにインストールされている必要があります。

ATM インターフェイスに WRED を設定するには、random-detect aggregate コマンドを使用する必要があります。標準 random-detect コマンドは ATM インターフェイスでサポートされなくなりました。

ポリシー マップ コンフィギュレーション内で、このコマンドと **random-detectaggregate** コマンドを使用します。

WRED パラメータを共有する IP precedence 値の各セットに対して、このコマンドを繰り返します。

ポリシー マップが定義された後で、ポリシー マップを VC レベルで割り当てる必要があります。

random-detectprecedence（集約）CLI で定義されたサブクラス（IP プレシデンス）値のセットは、単一のハードウェア WRED リソースに集約されます。これらのサブクラスの統計情報も、集約されます。

集約サブクラスの統計情報を表示するには、**showpolicy-mapinterface** コマンドを使用します。

Cisco 10000 シリーズ ルータ

次の表は、DSCP、IP プレシデンス、および廃棄クラスに基づいた WRED のデフォルト廃棄しきい値です。廃棄確率は、ルータが 10 パケットあたり 1 パケットをドロップすることを示します。

表 *40 : WRED* のデフォルト廃棄しきい値

DSCP、プレシデンス、および廃棄クラス値	最小しきい値（キュー サイズに対する割合）	最大しきい値（キューサイズに対する割合）	廃棄確率
すべての DSCP	1/4	1/2	1/10
0	1/4	1/2	1/10

DSCP、プレシデンス、および廃棄クラス値	最小しきい値（キュー サイズに対する割合）	最大しきい値（キューサイズに対する割合）	廃棄確率
1	9/32	1/2	1/10
2	5/16	1/2	1/10
3	11/32	1/2	1/10
4	3/8	1/2	1/10
5	13/32	1/2	1/10
6	7/16	1/2	1/10
7	15/32	1/2	1/10

PRE2 の場合、random-detect コマンドでキューのデフォルト プロファイルを指定します。PRE3 の場合、代わりに aggregate random-detect コマンドを使用して、WRED に集約パラメータを設定します。PRE3 でも PRE2 の random-detect コマンドを隠し CLI として使用できます。

PRE2 の場合、デフォルト プロファイルのアカウンティングはプレシデンスごとに行います。PRE3 の場合、デフォルト プロファイルのアカウンティングと設定はクラス マップごとに行います。

PRE2 の場合、明示的なしきい値設定をしないと、DSCP またはプレシデンス値のデフォルトしきい値は、プレシデンスごとに指定します。PRE3 の場合、デフォルトしきい値には WRED を設定しません。

PRE2 の場合、デフォルト プロファイル内の各プレシデンスのドロップ カウンタには、特定のプレシデンス値と一致するドロップ カウンタのみが含まれます。PRE2 にはデフォルト プロファイルのデフォルトしきい値があるため、CBQOSMIB にはデフォルトしきい値が表示されます。PRE3 の場合、デフォルト プロファイル内の各プレシデンスのドロップ カウンタには、デフォルト プロファイルの集約カウンタが含まれており、特定のプレシデンスに対応した個別のカウンタはありません。デフォルト プロファイルにしきい値を設定していない場合、PRE3 のデフォルト プロファイルでは、CBQOSMIB のデフォルトしきい値は表示されません。

例

Cisco 10000 シリーズ ルータ

次の例は、Cisco 10000 シリーズ ルータで IP プレシデンス ベース WRED を有効にします。この例では Class1 という名前のクラス マップを、IP プレシデンス 3、4、および 5 に基づいてトラフィックを分類するように設定します。IP プレシデンス 3、4、または 5 に一致するトラフィックは、Policy1 という名前のポリシー マップの Class1 という名前のクラスに割り当てられます。WRED ベースのパケット ドロップが Class1 に設定され、最小しきい値は 500、最大しきい値は 1500、および mark-probability-denominator は 200 が指定された IP プレシデンス 3 で判定されます。QoS ポリシーは、ポイントツーポイント ATM サブインターフェイス 1/0/0.1 の PVC 1/32 に適用されます。

```
Router(config)# class-map Class1
```

```
Router(config-cmap)# match ip precedence 3 4 5
Router(config-cmap)# exit
Router(config)# policy-map Policy1
Router(config-pmap)# class Class1
Router(config-pmap-c)# bandwidth 1000
Router(config-pmap-c)# random-detect prec-based
Router(config-pmap-c)# random-detect precedence 3 500 1500 200
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0
Router(config-if)# atm pxf queuing
Router(config-if)# interface atm 1/0/0.1 point-to-point
Router(config-subif)# pvc 1/32
Router(config-subif-atm-vc)# ubr 10000
Router(config-subif-atm-vc)# service-policy output policy1
```

関連コマンド

コマンド	説明
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
interface	インターフェイス タイプを設定し、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。
policy-map	1 つまたは複数のインターフェイスに付加してサービス ポリシーを指定するためのポリシー マップを作成します。
random-detectaggregate	集約 WRED をイネーブルにし、オプションで、デフォルト集約クラスに対するデフォルト WRED パラメータの値を指定します。このデフォルト クラスは、明示的に設定されていないすべてのサブクラスに使用されます。
service-policy	入力インターフェイスまたはVC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

random-detect-group

（注） Cisco IOS Release 15.0(1)S および Cisco IOS Release 15.1(3)T では、**random-detect-group** コマンドは表示されません。このコマンドはCisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、今後のリリースで完全に削除されます。詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

重み付けランダム早期検出（WRED）または分散WRED（DWRED）パラメータ グループを定義するには、グローバル コンフィギュレーション モードで **random-detect-group** コマンドを使用します。WRED またはDWRED パラメータ 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。

random-detect-group *group-name* [{**dscp-based**|**prec-based**}]
no random-detect-group *group-name* [{**dscp-based**|**prec-based**}]

構文の説明

group-name	WRED または DWRED のパラメータ グループの名前です。
dscp-based	（任意）パケットの廃棄確率を計算する場合、WRED で Diffserv コード ポイント（DSCP）の値を使用するよう、指定します。
prec-based	（任意）パケットの廃棄確率を計算する場合、WRED で IP precedence の値を使用するよう、指定します。

コマンド デフォルト

WRED または DWRED パラメータ グループは存在しません。

dscp-based キーワードまたは **prec-based** キーワードのいずれも使用しないことを選択した場合、WRED では、IP プレシデンス値（デフォルト方式）を使用して、パケットの廃棄確率が計算されます。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
11.1(22)CC	このコマンドが導入されました。
12.1(5)T	このコマンドが Cisco IOS Release 12.1(5)T に統合されました。差別化サービス（DiffServ）と相対的優先転送（AF）Per Hop Behavior（PHB）をサポートするためのキーワード、**dscp-based** および **prec-based** が追加されました。
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。

リリース	変更箇所
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。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。

使用上のガイドライン

WREDは輻輳回避メカニズムで、輻輳の発生時にランダムにパケットをドロップすることでトラフィックを低下させます。DWRED は WRED に類似していますが、Route Switch Processor（RSP）の代わりに Versatile Interface Processor（VIP）が使用されます。WRED と DWRED は、転送速度を下げることによってドロップされるパケットに応答する、TCP のようなプロトコルをトラフィックが使用する際に最も効果的です。

ルータで、WRED計算で使用するパラメータが自動的に定義されます。グループのこれらのパラメータを変更する場合は、**exponential-weighting-constant** コマンドまたは **precedence** コマンドを使用します。

パケットの廃棄確率を計算する 2 つの方式

このコマンドには、**dscp-based** と **prec-based** の 2 つのオプションの引数が含まれており、WRED がパケットの廃棄確率の計算に使用する方式が決定されます。

WRED で使用する方式を決める際には、次の点に注意してください。

- **dscp-based** キーワードを指定すると、WRED では DSCP 値（IP タイプ オブ サービス（ToS）バイトの最初の 6 ビット）を使用して廃棄確率が計算されます。
- **prec-based** キーワードを指定すると、WRED では IP プレシデンス値を使用して、廃棄確率が計算されます。
- **dscp-based** および **prec-based** キーワードは、どちらかを指定します。
- いずれの引数も指定されない場合、WRED では、IP precedence の値を使用して廃棄確率が計算されます（デフォルト方式）。

例

次の例では、sanjose という名前の WRED パラメータ グループを定義します。

```
random-detect-group sanjose
 precedence 0 32 256 100
 precedence 1 64 256 100
 precedence 2 96 256 100
 precedence 3 128 256 100
 precedence 4 160 256 100
 precedence 5 192 256 100
 precedence 6 224 256 100
 precedence 7 256 256 100
```

次に、DSCP 値 9 を使用して、WRED をイネーブルにする例を示します。DSCP 値 9 の最小しきい値は 20 で、最大しきい値は 50 です。この設定は、必要に応じて他の仮想回線（VC）に適用できます。

```
Router(config)# random-detect-group sanjose dscp-based
Router(cfg-red-grp)# dscp 9 20 50
Router(config-subif-vc)# random-detect attach sanjose
```

関連コマンド

Command	Description
dscp	DSCP 値の最小および最大パケットしきい値を変更します。
exponential-weighting-constant	WRED パラメータ グループの平均キュー サイズ計算のための指数加重係数を設定します。
precedence(WREDgroup)	特定の IP Precedence に対して WRED グループを設定します。
random-detect(perVC)	VC 単位 WRED または VC 単位 VIP 分散 WRED を有効にします。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。
showqueueinginterface	インターフェイスまたは VC のキューイングの統計情報を表示します。

rate

帯域幅プールのサイズを設定するには、Per-Flow Admission コンフィギュレーション モードで **rate** コマンドを使用します。帯域幅プールのサイズ設定を元に戻すには、このコマンドの **no** 形式を使用します。

rate{*kbps*|**percent** *percentage*}
no rate {*kbps*|**percent** *percentage*}

構文の説明

kbps	帯域幅プールのサイズ（kbps）を設定します。
percent	帯域幅プールのサイズを、出力クラスの帯域幅のパーセンテージとして設定します。
percentage	出力クラス帯域幅のパーセンテージを指定します。

コマンド デフォルト

レートが明示的に指定されない場合、クラス帯域幅プールのすべてで Per-Flow Admission が使用可能になります。

コマンド モード

Per-Flow Admission コンフィギュレーション モード（config-pmap-admit-cac）

コマンド履歴

リリース	変更箇所
15.4(2)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

rate コマンドは、帯域幅プールのサイズを設定します。出力では、クラスに帯域幅保証または優先順位保証が必要です。Per-Flow Admission レートは、アクティブ フローが存在しているときに、許可済みフローに影響を与える値には変更できません。

例

次の例に、**rate** コマンドの使用方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# policy-map test
Device(config-pmap-admit-cac)#flow idle-timeout 50
Device(config-pmap)# class af4
Device(config-pmap-c)# bandwidth 200
Device(config-pmap-c)# admit cac local
Device(config-pmap-admit-cac)# rate percent 80
```

関連コマンド

コマンド	説明
admit cac local	クラスに対して Per-Flow Admission を有効化し、Per-Flow Admission コンフィギュレーション モードを開始します。

rate-limit

専用アクセス レート（CAR）および分散 CAR（DCAR）ポリシーを設定するには、インターフェイス コンフィギュレーション モードで **rate-limit** コマンドを使用します。設定からレー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。

rate-limit {**input**|[**output** *acl-index* | **[rate-limit]** *rate-limit-acl-index* |**dscp***dscp-value* **qos-group** *qos-group-number*]}*burst-normal burst-max* **conform-action***conform-action* **exceed-action***exceed-action*
no rate-limit {**input**|[**output** *acl-index* | **[rate-limit]** *rate-limit-acl-index* |**dscp***dscp-value* **qos-group** *qos-group-number*]}*burst-normal burst-max* **conform-action***conform-action* **exceed-action***exceed-action*

構文の説明

input	この入力インターフェイスで受信されたパケットに、この CAR トラフィック ポリシーを適用します。
output	この出力インターフェイスで送信されたパケットに、この CAR トラフィック ポリシーを適用します。
bps	平均レート（ビット/秒（bps））です。値は 8 kbps ずつ増やす必要があります。値は 8000 ～ 2000000000 の数字です。
access-group	（任意）指定したアクセス リストに、この CAR トラフィック ポリシーを適用します。
acl-index	（任意）アクセス リストの番号。値の範囲は 1 ～ 2699 です。
rate-limit	（任意）アクセス リストはレート制限アクセス リストです。
rate-limit-acl-index	（任意）レート制限アクセス リストの番号。値の範囲は 0 ～ 99 です。
dscp	（任意）レート制限を、指定した DiffServ コード ポイント（DSCP）に一致するパケットに適用できます。
dscp-value	（任意）DSCP 番号。値の範囲は 0 ～ 63 です。
qos-group	（任意）レート制限を、指定した QoS グループ番号に一致するパケットに適用できます。値の範囲は 0 ～ 99 です。
qos-group-number	（任意）QoS グループ番号。値の範囲は 0 ～ 99 です。
burst-normal	バイト単位の通常バースト サイズ。最小値は 2000 で割った bps です。値は 1000 ～ 512000,000 の数字です。
burst-max	バイト単位の超過バースト サイズ。値は 2000 ～ 1024000000 の数字です。

conform-action *conform-action*	指定したレート制限に適合したパケットに対して実行するアクションです。次のいずれかのキーワードを指定します。 • **continue**：次の **rate-limit** コマンドを評価します。 • **drop**：パケットをドロップします。 • **set-dscp-continue**：DiffServ コード ポイント（DSCP）（0 ～ 63）を設定し、次の **rate-limit** コマンドを評価します。 • **set-dscp-transmit**：DSCP を送信し、パケットを送信します。 • **set-mpls-exp-imposition-continue**：インポジション中にマルチプロトコル ラベル スイッチング（MPLS）EXP ビット（0 ～ 7）を設定し、次の **rate-limit** コマンドを評価します。 • **set-mpls-exp-imposition-transmit**：インポジション中に MLPS EXP ビット（0 ～ 7）を設定し、パケットを送信します。 • **set-prec-continue**：IP プレシデンス（0 ～ 7）を設定し、次の **rate-limit** コマンドを評価します。 • **set-prec-transmit**：IP プレシデンス（0 ～ 7）を設定し、パケットを送信します。 • **set-qos-continue**：Quality of Service（QoS）グループ ID（1 ～ 99）を設定し、次の **rate-limit** コマンドを評価します。 • **set-qos-transmit**：QoS グループ ID（1 ～ 99）を設定し、パケットを送信します。 • **transmit**：パケットを送信します。

exceed-action *exceed-action*	指定したレート制限を超過したパケットに対して実行するアクションです。次のいずれかのキーワードを指定します。 • **continue**：次の **rate-limit** コマンドを評価します。 • **drop**：パケットをドロップします。 • **set-dscp-continue**：DSCP（0 ～ 63）を設定し、次の **rate-limit** コマンドを評価します。 • **set-dscp-transmit**：DSCP を送信し、パケットを送信します。 • **set-mpls-exp-imposition-continue**：インポジション中に MPLS EXP ビット（0 ～ 7）を設定し、次の **rate-limit** コマンドを評価します。 • **set-mpls-exp-imposition-transmit**：インポジション中に MLPS EXP ビット（0 ～ 7）を設定し、パケットを送信します。 • **set-prec-continue**：IP プレシデンス（0 ～ 7）を設定し、次の **rate-limit** コマンドを評価します。 • **set-prec-transmit**：IP プレシデンス（0 ～ 7）を設定し、パケットを送信します。 • **set-qos-continue**：QoS グループ ID（1 ～ 99）を設定し、次の **rate-limit** コマンドを評価します。 • **set-qos-transmit**：QoS グループ ID（1 ～ 99）を設定し、パケットを送信します。 • **transmit**：パケットを送信します。

コマンド デフォルト

CAR および DCAR は無効です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
11.1 CC	このコマンドが導入されました。
12.1(5)T	MPLS EXP フィールドの **conform** および **exceed** キーワードが追加されました。
12.2(4)T	このコマンドが Cisco MGX RPM-PR カードを持つ Cisco MGX 8850 スイッチおよび MGX 8950 スイッチに実装されました。
12.2(4)T2	このコマンドが Cisco 7500 シリーズ ルータに実装されました。
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。

リリース	変更箇所
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

インターフェイスに CAR ポリシーを設定するには、このコマンドを使用します。複数のポリシーを指定するには、ポリシーごとに 1 回ずつこのコマンドを入力します。

CAR と DCAR はインターフェイスまたはサブインターフェイスで設定できます。

CAR を使用したトラフィックのポリシング

CAR にはトラフィックをポリシングするためのレート制限機能があります。CAR を使用してトラフィックをポリシングする場合、通常および超過バーストパラメータには、次の値を推奨します。

通常バースト（バイト）=設定されたレート（1 秒あたりのビット数）X（1 バイト）/（8 ビット）X 1.5 秒

17,000,000 X（1 バイト）/（8 ビット）X 1.5 秒 = 3,187,500 バイト

超過バースト = 2 X 通常バースト

2 X 3,187,500 = 6,375,000 バイト

パラメータに記載された選択肢を使用すると、CAR が設定されたレートを達成していることが広範なテスト結果で示されています。バースト値が低すぎると、達成されるレートが設定されたレートよりかなり低くなる場合がよくあります。

CAR を使用したトラフィックのポリシングに関する詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Policing and Shaping Overview」の「Policing with CAR」セクションを参照してください。

例

次の例では、CAR の推奨バースト パラメータを使用します。

```
Router(config)# interface serial6/1/0
```

```
Router(config-if)#
rate-limitinputaccess-group11700000031875006375000conform-actiontransmitexceed-actiondrop
```

次の例では、レートは問題のあるアプリケーションによって制限されます。

- すべての World Wide Web トラフィックが送信されます。ただし、最初のレートポリシーに準拠する Web トラフィックの MPLS EXP フィールドは、5 に設定されます。準拠しないトラフィックについては、IP プレシデンスが 0（ベストエフォート）に設定されます。この例の次のコマンドを確認してください。

```
rate-limit input rate-limit access-group 101 20000000 24000 32000 conform-action
set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 0
access-list 101 permit tcp any any eq www
```

- 2 番目のレート ポリシーに準拠する場合、FTP トラフィックを MPLS EXP フィールド値に 5 を設定して送信します。FTP トラフィックがレート ポリシーを超過すると、FTP トラフィックはドロップされます。この例の次のコマンドを確認してください。

```
rate-limit input access-group 102 10000000 24000 32000
conform-action set-mpls-exp-transmit 5 exceed-action drop
access-list 102 permit tcp any any eq ftp
```

- 残りのすべてのトラフィックは、8 Mbps、通常バースト サイズは 1,500,000 バイト、超過バースト サイズは 3,000,000 バイトに制限されます。準拠するトラフィックは、MPLS EXP フィールドを 5 にして送信します。準拠しないトラフィックはドロップされます。この例の次のコマンドを確認してください。

```
rate-limit input 8000000 1500000 3000000 conform-action set-mpls-exp-transmit 5
exceed-action drop
```

2 つのアクセス リストは、CAR 機能で区別して処理できるように、Web トラフィックと FTP トラフィックを分類するために作成されます。

```
Router(config)# interface Hssi0/0/0
Router(config-if)# description 45Mbps to R2
Router(config-if)# rate-limit input rate-limit access-group 101 20000000 3750000 7500000
conform-action set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 0
Router(config-if)# rate-limit input access-group 102 10000000 1875000 3750000
conform-action set-mpls-exp-transmit 5 exceed-action drop
Router(config-if)# rate-limit input 8000000 1500000 3000000 conform-action
set-mpls-exp-transmit 5 exceed-action drop
Router(config-if)# ip address 10.1.1.1 255.255.255.252
!
Router(config-if)# access-list 101 permit tcp any any eq www
Router(config-if)# access-list 102 permit tcp any any eq ftp
```

次の例では、MPLS EXP フィールドを設定し、パケットを送信します。

```
Router(config)# interface FastEthernet1/1/0
Router(config-if)# rate-limit input 8000 1500 3000 access-group conform-action
set mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 5
```

次の例では、DSCP が 1 のパケットすべてにレート制限を適用します。

```
Router(config)# interface serial6/1/0
Router(config-if)# rate-limit output dscp 1 8000 1500 3000 conform-action transmit
exceed-action drop
```

関連コマンド

Command	Description
access-listrate-limit	CAR ポリシーで使用する場合のアクセス リストを設定します。
showaccess-listsrate-limit	レート制限アクセス リストに関する情報を表示します。
showinterfacesrate-limit	指定したインターフェイスの CAR に関する情報を表示します。

rcv-queue bandwidth

インターフェイス コンフィギュレーション コマンド モードでスケジューリング重みを使用して、入力（受信）WRR キューの帯域幅を定義するには、**rcv-queuebandwidth** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

rcv-queue bandwidth *weight-1 ... weight-n*
no rcv-queue bandwidth

構文の説明

weight-1 *...weight-n*	WRR 重みを指定します。有効値は 0 ～ 255 です。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- QoS が有効な場合 - 4：255
- QoS が無効な場合 - 255：1

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(17a)SX	このコマンドが Supervisor Engine 720 に導入されました。
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。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

このコマンドは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

このコマンドは、2q8t および 8q8t ポートだけでサポートされます。

設定できるキューの重みは最大で 7 つです。

例

次に、3 対 1 の帯域幅比率を割り当てる例を示します。

```
Router(config-if)# rcv-queue bandwidth 3 1
Router(config-if)#
```

関連コマンド

コマンド	説明
rcv-queuequeue-limit	完全プライオリティ キューと標準受信キューの間のサイズ比を設定します。
showqueueinginterface	キューイング情報を表示します。

rcv-queue cos-map

サービス クラス（CoS）値を標準受信キュー廃棄しきい値にマッピングするには、インターフェイス コンフィギュレーション モードで **rcv-queuecos-map** コマンドを使用します。マッピングを削除するには、このコマンドの **no** 形式を使用します。

rcv-queue cos-map *queue-id threshold-id cos-1 cos-n*
no rcv-queue cos-map *queue-id threshold-id*

構文の説明

queue-id	キュー ID。有効値は 1 です。
threshold-id	しきい値 ID。有効値は 1 ～ 4 です。
cos-1 *...cos-n*	CoS 値。有効値は、0 ～ 7 です。

コマンド デフォルト

デフォルト値を次の表に示します。

表 *41* : デフォルトの *CoS* に対する標準受信キューマップ

キュー	しきい値	cos-map	キュー	しきい値	cos-map
QoS がディセーブルの場合	QoS がイネーブルの場合				
1	1	0、1、2、3、4、5、6、7	1	1	0、1
1	2		1	2	2、3
1	3		1	3	4
1	4		1	4	6、7
2	1	5	2	1	5

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

リリース	変更箇所
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

cos-n 値は、モジュールおよびポート タイプによって定義されます。cos-n 値を入力する場合は、大きい値ほど高いプライオリティを示すことに注意してください。

このコマンドは、信頼されたポート上だけで使用してください。

例

次に、標準受信キューのしきい値 1 に CoS 値 0 および 1 をマッピングする例を示します。

```
Router (config-if)# rcv-queue cos-map 1 1 0 1
  cos-map configured on:  Gi1/1 Gi1/2
```

関連コマンド

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

rcv-queue queue-limit

絶対優先受信キューおよび標準受信キュー間のサイズ比を設定するには、インターフェイス コンフィギュレーション モードで **rcv-queuequeue-limit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

rcv-queue queue-limit *q-limit-1 q-limit-2*
no rcv-queue queue-limit

構文の説明

q-limit-1	標準キューの重み。有効値は 1 ～ 100% です。
q-limit-2	絶対優先キューの重み。有効値については、「使用上のガイドライン」セクションを参照してください。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- 80%（ロー プライオリティ）
- 20%（絶対優先）

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

1p1q8t 入力 LAN ポートを除き、有効な絶対優先の重み値は 1 ～ 100% です。1p1q8t 入力 LAN ポートでは、絶対優先キューの有効値は 3 ～ 100% です。

rcv-queuequeue-limit コマンドでは、ASIC ごとにポートを設定します。

ネットワークにおける完全優先トラフィックと標準トラフィックの配分（標準トラフィック 80%、完全優先トラフィック 20% など）を推定し、推定値をキューの重みに使用します。

例

次に、ギガビットイーサネットインターフェイス 1/2 に受信キューサイズ比を設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/2
Router(config-if)# rcv-queue queue-limit 75 15

Router(config-if)# end
```

関連コマンド

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

rcv-queue random-detect

特定の受信キューに最小しきい値と最大しきい値を指定するには、インターフェイス コンフィギュレーション モードで **rcv-queuerandom-detect** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

rcv-queue random-detect {**max-threshold**|**min-threshold**} *queue-id threshold-percent-1 threshold-percent-n*
no rcv-queue random-detect {**max-threshold**|**min-threshold**} *queue-id*

構文の説明

max-threshold	最大しきい値を指定します。
min-threshold	最小しきい値を指定します。
queue-id	キュー ID。有効値は 1 です。
threshold-percent-1 threshold-percent-n	しきい値の重み。有効値は 1 ～ 100% です。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- min-threshold：80%
- max-threshold：20%

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(17a)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

このコマンドは、1p1q8t および 8q8t ポートだけでサポートされます。

1p1q8t インターフェイスは、1 つの完全プライオリティ キューと、8 つのしきい値がある 1 つの標準キューを意味します。8q8tインターフェイスは、8つのしきい値がある8つの標準キューを意味します。完全プライオリティ キューのしきい値は設定できません。

しきい値には、それぞれ低および高しきい値があります。しきい値は受信キュー容量のパーセントです。

受信キューしきい値の設定の詳細については、『*Cisco 7600 Series Router Cisco IOS Software Configuration Guide*』の「QoS」章を参照してください。

例

次に、低プライオリティ受信キューのしきい値を設定する例を示します。

```
Router (config-if)# rcv-queue random-detect max-threshold 1 60 100
```

関連コマンド

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

rcv-queue threshold

1p1q4t および 1p1q0t インターフェイスの標準受信キューに廃棄しきい値パーセンテージを設定するには、インターフェイス コンフィギュレーション モードで **rcv-queuethreshold** コマンドを使用します。しきい値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。

rcv-queue threshold *queue-id threshold-percent-1 threshold-percent-n*
no rcv-queue threshold

構文の説明

queue-id	キュー ID。有効値は 1 です。
threshold- percent-1 ...threshold- percent-n	しきい値 ID。有効値は 1 ～ 100% です。

コマンド デフォルト

1p1q4t および 1p1q0t のデフォルト設定は、次のとおりです。

- Quality of service（QoS）では、サービス クラス（CoS）が 5 のすべてのトラフィックが絶対優先キューに割り当てられます。
- QoS はその他のすべてのトラフィックを標準キューに割り当てます。

1q4t のデフォルト設定では、QoS はすべてのトラフィックを標準キューに割り当てます。

QoS がイネーブルの場合は、次のデフォルトのしきい値が適用されます。

- 1p1q4t インターフェイスの廃棄しきい値のデフォルト設定は、次のとおりです。
  - CoS が 0、1、2、3、4、6、または 7 のフレームは、標準受信キューに入ります。
  - 標準受信キュー廃棄しきい値が 1 の場合、受信キュー バッファが 50% 以上満たされると、Cisco 7600 シリーズ ルータは CoS 0 または 1 の着信フレームを廃棄します。
  - 標準受信キュー廃棄しきい値が 2 の場合、受信キュー バッファが 60% 以上満たされると、Cisco 7600 シリーズ ルータは CoS 2 または 3 の着信フレームを廃棄します。
  - 標準受信キュー廃棄しきい値が 3 の場合、受信キュー バッファが 80% 以上満たされると、Cisco 7600 シリーズ ルータは CoS 4 の着信フレームを廃棄します。
  - 標準受信キュー廃棄しきい値が 4 の場合、受信キュー バッファが 100% 満たされると、Cisco 7600 シリーズ ルータは CoS 6 または 7 の着信フレームを廃棄します。
  - CoS 5 のフレームは、絶対優先受信キュー（キュー 2）に送られます。絶対優先受信キュー バッファが 100% 満たされた場合のみ、Cisco 7600 シリーズ ルータは着信フレームを廃棄します。
- 1p1q0t インターフェイスの廃棄しきい値のデフォルト設定は、次のとおりです。
  - CoS が 0、1、2、3、4、6、または 7 のフレームは、標準受信キューに入ります。受信キュー バッファが 100% 満たされると、Cisco 7600 シリーズ ルータは着信フレームを廃棄します。

- CoS 5 のフレームは、絶対優先受信キュー（キュー 2）に送られます。絶対優先受信キュー バッファが 100% 満たされた場合のみ、Cisco 7600 シリーズ ルータは着信フレームを廃棄します。

（注） 100% のしきい値は、実際は、ブリッジ プロトコル データ ユニット（BPDU）トラフィックを処理できるように、モジュールによって 98% に変更されます。BPDU しきい値は、出荷時に 100% に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

queue-id 値は、常に 1 です。

10 という値は、バッファが 10% 満たされている場合のしきい値を意味します。

しきい値 4 は常に 100% に設定してください。

受信しきい値が有効なのは、信頼状態が trust cos のポート上だけです。

1q4t の受信キュー テールドロップしきい値パーセンテージを設定するには、**wrr-queuethreshold** コマンドを使用します。

例

次に、ギガビット イーサネット インターフェイス 1/1 に受信キュー廃棄しきい値を設定する例を示します。

```
Router(config-if)# rcv-queue threshold 1 60 75 85 100
```

関連コマンド

コマンド	説明
showqueueinginterface	キューイング情報を表示します。
wrr-queuethreshold	1q4t および 2q2t インターフェイス上の標準受信キューおよび標準送信キューの廃棄しきい値パーセントを設定します。

recoverable-loss

Enhanced Compressed Real-Time Transport Protocol（ECRTP）を有効にするには、IPHC-profile コンフィギュレーション モードで **recoverable-loss** コマンドを使用します。ECRTP を無効にするには、このコマンドの **no** 形式を使用します。

recoverable-loss {**dynamic***packet-drops*}
no recoverable-loss

構文の説明

dynamic	動的回復可能損失の計算が使用されることを示します。
packet-drops	連続するパケット破棄の最大数です。範囲は 1 ～ 8 です。

コマンド デフォルト

ECRTP は無効です。

コマンド モード

IPHC プロファイル コンフィギュレーション（config-iphcp）

コマンド履歴

リリース	変更箇所
12.4(9)T	このコマンドが導入されました。
12.4(11)T	フレーム リレー カプセル化のサポートが追加されました。

使用上のガイドライン

recoverable-loss コマンドは、ECRTP 機能に含まれます。

ECRPT の機能

ECRTP は、コンプレッサがデコンプレッサのコンテキスト情報を更新する方法を管理することで、破損を減らします。コンプレッサは、更新されたコンテキスト情報を定期的に送信して、コンプレッサとデコンプレッサ間の同期を維持します。更新を繰り返すと、パケット損失によるコンテキスト破損の確率が最小化されます。

コンプレッサとデコンプレッサ間でコンテキスト情報を動的に（**dynamic** キーワードを指定）、または一定数のパケットがドロップされたときに（*packet-drops* 引数を使用）同期できます。

パケット ドロップ数はホスト間のリンクの品質を示します。パケット ドロップ数が少ないほど、ホスト間のリンクの品質は高くなります。

パケット ドロップ値は、各コンテキストで個別に保持されるため、すべてのコンテキストで同じである必要はありません。

（注） *packet-drops* 引数でパケット ドロップ数を指定する場合、**recoverable-loss** コマンドによって ECRTP が自動的に有効になります。

IPHC プロファイルでの使用目的

recoverable-loss は IP ヘッダー圧縮（IPHC）プロファイル内で使用するコマンドです。IPHC プロファイルは、ネットワーク上でヘッダー圧縮を有効にして設定するために使用されます。IPHC プロファイルを使用してヘッダー圧縮を設定する詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、リリース 12.4T の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

例

次に、profile2 という名前の IPHC プロファイルを設定する例を示します。この例では、ECRTP を連続パケット ドロップ数の最大値に 5 を指定して有効にします。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# recoverable-loss 5
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
iphc-profile	IPHCプロファイルを作成します。

redirect interface

特定クラス内のパケットを、指定したインターフェイスにリダイレクトするようにトラフィック クラスを設定するには、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 redirect interface コマンドを使用します。パケットがリダイレクトされないようにするには、このコマンドの no 形式を使用します。

redirect interface *interface* **type number**
no redirect interface interface type number

構文の説明

interface type number	パケットをリダイレクトする先のインターフェイスのタイプと番号です。

コマンド デフォルト

このコマンドを指定しない場合、パケットはインターフェイスにリダイレクトされません。

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.2(18)ZYA1	このコマンドが導入されました。

使用上のガイドライン

パケットを定義済みインターフェイスにリダイレクトするには、このコマンドを使用します。drop コマンドや copy interface コマンドではなく、log コマンドを使用して redirect interface コマンドを設定することもできます。スタック クラスのサービス ポリシーを使用して、このコマンドを構成することはできません。パケットは、次のインターフェイスにのみにリダイレクトできます。

- Ethernet
- ファスト イーサネット
- ギガビット イーサネット
- Ten Gigabit Ethernet

例

次の例では、cmtest というトラフィック クラスを作成し、pmtest というポリシー マップで使用できるように設定しています。ポリシー マップ（サービス ポリシー）は、FastEthernet インターフェイス 4/15 に適用されます。cmtest 内のすべてのパケットは、FastEthernet インターフェイス 4/18 にリダイレクトされます。

```
Router(config)# policy-map type access-control pmtest
Router(config-pmap)# class cmtest
Router(config-pmap-c)# redirect interface FastEthernet 4/18
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
```

```
Router(config)# interface FastEthernet 4/18
Router(config-if)# service-policy input pmtest
```

関連コマンド

コマンド	説明
log	ポリシーマップ クラス コンフィギュレーション モードまたはクラス マップ コンフィギュレーション モードでログ メッセージを生成します。
showclass-map	すべてのクラス マップおよびその一致基準を表示します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

refresh max-period

フルヘッダー リフレッシュが発生する間に送信するパケット数を設定するには、IPHC-profile コンフィギュレーション モードで **refreshmax-period** コマンドを使用します。パケットのデフォルト数を使用するには、このコマンドの **no** 形式を使用します。

refresh max-period {*number-of-packets*|**infinite**}
no refresh max-period

構文の説明

number-of-packets	フルヘッダー リフレッシュが発生する間に送信するパケット数。範囲は 0 ～ 65535 です。デフォルトは 256 です。
infinite	フルヘッダー リフレッシュが発生する間に送信するパケット数は無制限です。

コマンド デフォルト

フルヘッダー リフレッシュが発生する間に送信するパケット数は 256 です。

コマンド モード

IPHC 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	変更箇所
12.4(9)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

フルヘッダー リフレッシュが発生する間に送信する非 TCP パケット数を設定するには、**refreshmax-period** コマンドを使用します。**refreshmax-period** コマンドで、フルヘッダー リフレッシュが発生する間に送信するパケット数を無制限に指定することもできます。送信されたパケット数を無制限にするには、**infinite** キーワードを使用します。

前提条件

refreshmax-period コマンドを使用する前に、**non-tcp** コマンドを使用して、非 TCP ヘッダー圧縮を有効にする必要があります。

IPHC プロファイルでの使用目的

refreshmax-period コマンドは、IPHC プロファイルの一部として使用することを目的としています。IPHC プロファイルは、ネットワークでのヘッダー圧縮を有効および設定するために使用されます。IPHC プロファイルを使用してヘッダー圧縮を設定する詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、リリース 12.4T の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

例

profile2 という IPHC プロファイルの例を、次に示します。この例では、フルヘッダー リフレッシュの発生までに送信するパケット数は 700 パケットです。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# refresh max-period 700
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
iphc-profile	IPHC プロファイルを作成します。
non-tcp	IPHC プロファイルの非 TCP ヘッダー圧縮を有効にします。

refresh max-time

フルヘッダー リフレッシュ発生までの待機時間を設定するには、IPHC-profile コンフィギュレーション モードで **refreshmax-time** コマンドを使用します。デフォルト時間を使用するには、このコマンドの **no** 形式を使用します。

refresh max-time {秒|**infinite**}
no refresh max-time

構文の説明

秒	フルヘッダー リフレッシュ発生までの待機時間（秒）。範囲は 0 ～ 65535 です。デフォルトは 5 です。
infinite	フルヘッダー リフレッシュ間の時間が無制限です。

コマンド デフォルト

フルヘッダー リフレッシュ発生までの待機時間は 5 秒に設定されます。

コマンド モード

IPHC 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	変更箇所
12.4(9)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

フルヘッダー リフレッシュ発生までの最大待機時間を設定するには、**refreshmax-time** コマンドを使用します。**refreshmax-time** コマンドでは、フルヘッダー リフレッシュ発生までの待機時間を無制限に指定することもできます。フルヘッダーリフレッシュ発生までの待機時間を無制限に指定するには、 **infinite** キーワードを使用します。

前提条件

refreshmax-time コマンドを使用する前に、**non-tcp** コマンドを使用して、非 TCP ヘッダー圧縮を有効にする必要があります。

IPHC プロファイルでの使用目的

refreshmax-time コマンドは、IPHC プロファイルの一部として使用することを目的としています。IPHC プロファイルは、ネットワークでのヘッダー圧縮を有効および設定するために使用されます。IPHC プロファイルを使用してヘッダー圧縮を設定する詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、リリース 12.4T の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

例

profile2 という IPHC プロファイルの例を、次に示します。この例では、フルヘッダー リフレッシュ発生までの最大待機時間を 500 秒にします。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# refresh max-time 500
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
iphc-profile	IPHC プロファイルを作成します。
non-tcp	IPHC プロファイルの非 TCP ヘッダー圧縮を有効にします。

refresh rtp

Real-time Transport Protocol（RTP）ヘッダー圧縮でコンテキスト リフレッシュの発生を有効にするには、IPHC-profile コンフィギュレーション モードで **refreshrtp** コマンドを使用します。RTP ヘッダー圧縮でのコンテキスト リフレッシュの発生を無効にするには、このコマンドの **no** 形式を使用します。

refresh rtp
no refresh rtp

構文の説明

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

RTP ヘッダー圧縮でのコンテキスト リフレッシュの発生は無効です。

コマンド モード

IPHC 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	変更箇所
12.4(9)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

RTP ヘッダー圧縮でコンテキスト リフレッシュの発生を有効にするには、**refreshrtp** コマンドを使用します。コンテキストとは、コンプレッサがヘッダーの圧縮に使用し、デコンプレッサがヘッダーの圧縮解除に使用する状態です。コンテキストは、送信された最終ヘッダーの非圧縮バージョンであり、パケットの圧縮と圧縮解除に使用する情報が含まれます。

前提条件

refreshrtp コマンドを使用する前に、**rtp** コマンドを使用して、RTP ヘッダー圧縮を有効にする必要があります。

IPHC プロファイルでの使用目的

refreshrtp は IP ヘッダー圧縮（IPHC）プロファイル内で使用するコマンドです。IPHC プロファイルは、ネットワークでのヘッダー圧縮を有効および設定するために使用されます。IPHC プロファイルを使用してヘッダー圧縮を設定する詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、リリース 12.4T の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

例

profile2 という IPHC プロファイルの例を、次に示します。この例では、RTP ヘッダー圧縮でコンテキスト リフレッシュの発生を有効にするために、**refreshrtp** コマンドを使用します。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
```

```
Router(config-iphcp)# rtp
Router(config-iphcp)# refresh rtp
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
iphc-profile	IPHC プロファイルを作成します。
rtp	IPHC プロファイル内の RTP ヘッダー圧縮を有効にします。

rtp

IP ヘッダー圧縮（IPHC）プロファイル内で Real-time Transport Protocol（RTP）ヘッダー圧縮を有効にするには、IPHC-profile コンフィギュレーション モードで **rtp** コマンドを使用します。IPHC プロファイル内で RTP ヘッダー圧縮を無効にするには、このコマンドの **no** 形式を使用します。

rtp
no rtp

構文の説明

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

RTP ヘッダー圧縮は有効です。

コマンド モード

IPHC 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	変更箇所
12.4(9)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

rtp コマンドでは、RTP ヘッダー圧縮が有効になり、非 TCP ヘッダー圧縮が自動的に有効になります（**non-tcp** コマンドを使用した場合と同様）。

IPHC プロファイルでの使用目的

rtp は IP ヘッダー圧縮（IPHC）プロファイル内で使用するコマンドです。IPHC プロファイルは、ネットワーク上でヘッダー圧縮を有効にして設定するために使用されます。IPHC プロファイルを使用したヘッダー圧縮の設定の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、Release 12.4T の「Header Compression」モジュールと「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

例

次に、profile2 という名前の IPHC プロファイルを設定する例を示します。この例では、RTP ヘッダー圧縮が設定されます。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# rtp
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
iphc-profile	IPHC プロファイルを作成します。

コマンド	説明
non-tcp	IPHC プロファイルの非 TCP ヘッダー圧縮を有効にします。

send qdm message から show atm bundle svc statistics

- sdm prefer enable_portchannel_qos_multiple_active （1097 ページ）
- sdm prefer disable_portchannel_qos_multiple_active （1098 ページ）
- send qdm message （1099 ページ）
- service-group （1101 ページ）
- service-policy （1102 ページ）
- service-policy（クラスマップ） （1114 ページ）
- service-policy（コントロール プレーン） （1116 ページ）
- service-policy（ポリシーマップ クラス） （1119 ページ）
- service-policy（サービス グループ） （1122 ページ）
- service-policy type qos （1123 ページ）
- set atm-clp （1124 ページ）
- set cos （1126 ページ）
- set cos cos-inner（ポリシーマップ コンフィギュレーション） （1131 ページ）
- set cos-inner （1134 ページ）
- set cos-inner cos （1136 ページ）
- set discard-class （1138 ページ）
- set dscp （1139 ページ）
- set fr-de （1143 ページ）
- set ip dscp （1145 ページ）
- set ip dscp（ポリシー マップ コンフィギュレーション） （1146 ページ）
- set ip dscp tunnel （1149 ページ）
- set ip precedence（ポリシー マップ コンフィギュレーション） （1152 ページ）
- set ip precedence（ポリシー マップ） （1155 ページ）
- set ip precedence（ルートマップ） （1156 ページ）
- set ip precedence tunnel （1159 ページ）
- set ip tos（ルートマップ） （1161 ページ）
- set precedence （1164 ページ）
- set qos-group （1168 ページ）

- set vlan inner （1172 ページ）
- shape （1173 ページ）
- shape (percent) （1175 ページ）
- shape（policy-map クラス） （1179 ページ）
- shape adaptive （1186 ページ）
- shape fecn-adapt （1188 ページ）
- shape max-buffers （1190 ページ）
- show access-lists rate-limit （1192 ページ）
- show atm bundle （1194 ページ）
- show atm bundle stat （1196 ページ）
- show atm bundle svc （1198 ページ）
- show atm bundle svc stat （1200 ページ）

sdm prefer enable_portchannel_qos_multiple_active

ポートチャネル アクティブ/アクティブ モードを有効にするには、グローバル コンフィギュレーション モードで **sdm prefer enable_portchannel_qos_multiple_active** コマンドを使用します。

sdm prefer enable_portchannel_qos_multiple_active

構文の説明

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

sdm テンプレートは、デフォルトでは無効になっています。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
XE 3.18.1 SP	このコマンドのサポートが ASR 900 シリーズ ルータに追加されました。

使用上のガイドライン

ポートチャネル アクティブ/アクティブ モードを作成するには、テンプレートを有効にする必要があります。**sdm prefer enable_portchannel_qos_multiple_active** コマンドを有効にすると、デバイスが再起動します。正常にリブートしたら、**show sdm prefer current** コマンドを使用して設定を検証します。

例

次の例は、ポートチャネル アクティブ/アクティブ モードを有効にする方法を示しています。

```
enable
configure terminal
sdm prefer enable_portchannel_qos_multiple_active
end
```

関連コマンド

コマンド	説明
show sdm prefer current	ポートチャネルアクティブ/アクティブ モードを有効にした後で設定を検証します。
show etherchannel summary	ポートチャネル概要の詳細を検証します。
show policy-map interface brief	ポートチャネルインターフェイスでアタッチしたポリシーマップを検証します。

sdm prefer disable_portchannel_qos_multiple_active

ポートチャネル アクティブ/アクティブ モードを無効にするには、グローバル コンフィギュレーション モードで **sdm prefer disable_portchannel_qos_multiple_active** コマンドを使用します。

sdm prefer disable_portchannel_qos_multiple_active

構文の説明

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

sdm テンプレートは、デフォルトでは無効になっています。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
XE 3.18.1 SP	このコマンドのサポートが ASR 900 シリーズ ルータに追加されました。

使用上のガイドライン

ポートチャネル アクティブ/アクティブ モードを作成するには、テンプレートを有効にする必要があります。

例

次の例は、ポートチャネル アクティブ/アクティブ モードを無効にする方法を示しています。

```
enable
configure terminal
sdm prefer disable_portchannel_qos_multiple_active
end
```

関連コマンド

コマンド	説明
show sdm prefer current	ポートチャネルアクティブ/アクティブモードを有効にした後で設定を検証します。
show etherchannel summary	ポートチャネル概要の詳細を検証します。
show policy-map interface brief	ポートチャネルインターフェイスでアタッチしたポリシーマップを検証します。

send qdm message

すべての Quality Device Manager（QDM）クライアントにテキスト メッセージを送信するには、EXEC モードで **sendqdmmessage** コマンドを使用します。

send qdm [**client** *client-id*] **message** *message-text*

構文の説明

client	（任意）メッセージを受信する QDM クライアントを指定します。
client-id	（任意）テキスト メッセージを受信するクライアントの QDM ID を指定します。
message	メッセージ送信を指定します。
message-text	メッセージの実際のテキストです。

コマンド デフォルト

テキスト メッセージは送信されません。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.1(1)E	このコマンドが導入されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
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。

使用上のガイドライン

特定の QDM クライアントにメッセージを送信するには、**sendqdm** コマンドを使用します。たとえば、**sendqdmclient9messagehello** コマンドを入力すると、クライアント ID 9 に「hello」というメッセージを送信します。

メッセージをすべての QDM クライアントに送信するには、**sendqdmmessage***message-text* コマンドを使用します。たとえば、**sendqdmmessagehello** コマンドを入力すると、すべてのオープンな QDM クライアントに「hello」というメッセージを送信します。

例

次の例では、クライアント ID 12 に「how are you?」というテキスト メッセージを送信します。

```
send qdm client 12 message how are you?
```

次の例では、ルータに接続されているすべての QDM クライアントに「how is everybody?」というテキスト メッセージを送信します。

```
send qdm message how is everybody?
```

関連コマンド

コマンド	説明
showqdmstatus	接続済みQDMクライアントの状態を表示します。

service-group

サービス グループを作成するには、グローバル コンフィギュレーション モードで service-group コマンドを使用します。サービス グループを削除するには、このコマンドの **no** 形式を使用します。

service-group service-group-identifier
no service-group service-group-identifier

構文の説明

service-group-identifier	サービス グループ番号。有効なエントリは 1 からルータでサポート可能な最大グループ数までの範囲の番号です。詳細については、疑問符（?）オンライン ヘルプ機能を使用し、「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

サービス グループは作成されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.2(33)SRE	このコマンドが導入されました。

使用上のガイドライン

ルータでサポートされる最大サービス グループ数は、システム起動時にルータによって決定されます。Cisco 7600 シリーズ ルータの場合、*service-group-identifier* 引数の有効なエントリの範囲は、1 ～ 32768 です。

例

次の例では、サービス グループ 750 が作成されます。

```
Router> enable
Router# configure terminal
Router(config)# service-group 750
Router(config)# end
```

service-policy

入力インターフェイス、仮想回線（VC）、出力インターフェイス、またはインターフェイスか VC のサービス ポリシーとして使用される VC に、ポリシー マップを適用するには、適切な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。入力インターフェイス、出力インターフェイス、入力 VC、出力 VC からサービス ポリシーを削除するには、このコマンドの **no** 形式を使用します。

service-policy [**type access-control**] {**input**|**output**} *policy-map-name*
no service-policy [**type access-control**] {**input**|**output**} *policy-map-name*

Cisco 10000 シリーズおよび Cisco 7600 シリーズ ルータ
service-policy [{**history**|{**input**|**output**} *policy-map-name*|**type control** *control-policy-name*}]
no service-policy [{**history**|{**input**|**output**} *policy-map-name*|**type control** *control-policy-name*}]

インターフェイス テンプレート コンフィギュレーション
service-policy [**access-control**] {**input**|**output**|**type control subcriber** }*policy-map-name*
no service-policy [**access-control**] {**input**|**output**|**type control subcriber** }*policy-map-name*

構文の説明

typeaccess-control	（任意）該当するプロトコルスタックで検索する完全一致パターンを決定します。
input	指定されたポリシー マップを入力インターフェイスまたは入力 VC に対応付けます。
output	指定されたポリシー マップを出力インターフェイスまたは出力 VC に対応付けます。
policy-map-name	適用されるサービス ポリシー マップ（**policy-map** コマンドを使用して作成）の名前。この名前には最大 40 文字までの英数字を指定できます。
history	（任意）Quality of Service（QoS）メトリックの履歴を保持します。
type control *control-policy-name*	（任意）コンテキストに適用するクラスベース ポリシー言語（CPL）制御ポリシー マップを作成します。
type control subscriber *policy-map-name*	インターフェイスに加入者制御ポリシーを適用します。

コマンド デフォルト

サービス ポリシーは指定されていません。コントロール ポリシーは、コンテキストには適用されません。ポリシー マップは適用されません。

コマンド モード

ATM VC バンドル コンフィギュレーション（config-atm-bundle）

ATM PVP コンフィギュレーション（config-if-atm-l2trans-pvp）

ATM VC コンフィギュレーション モード（config-if-atm-vc）

イーサネット サービス コンフィギュレーション（config-if-srv）

グローバル コンフィギュレーション（config）

インターフェイス コンフィギュレーション（config-if）

スタティック マップ クラス コンフィギュレーション（config-map-class）

ATM PVC-in-range コンフィギュレーション（cfg-if-atm-range-pvc）

サブインターフェイス コンフィギュレーション（config-subif）

テンプレート コンフィギュレーション（config-template）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。
12.0(7)S	このコマンドが、Cisco IOS Release 12.0(7)S に統合されました。
12.0(17)SL	このコマンドが Cisco 10000 シリーズ ルータに実装されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(2)T	このコマンドは、フレーム リレー VC で低遅延キューイング（LLQ）をイネーブルにするよう、変更されました。
12.2(14)SX	このコマンドのサポートが Cisco 7600 シリーズ ルータに実装されました。出力ポリシー マップのサポートが追加されました。
12.2(15)BX	このコマンドが ESR-PRE2 に実装されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。
12.4(2)T	このコマンドが変更されました。サブインターフェイス コンフィギュレーション モードと ATM PVC-in-range コンフィギュレーション モードのサポートが追加され、ATM VC のポリシー マップ機能が ATM VC 範囲に拡張されました。
12.4(4)T	**type stack** および **type control** キーワードが追加され、Flexible Packet Matching（FPM）がサポートされました。
12.2(28)SB	このコマンドが Cisco IOS Release 12.2(28)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。

リリース	変更箇所
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.3(7)XI2	このコマンドが変更され、Cisco 10000 シリーズ ルータと Cisco 7200 シリーズ ルータの ATM VC に対応したサブインターフェイス コンフィギュレーション モードと ATM PVC-in-range コンフィギュレーション モードがサポートされるようになりました。
12.2(18)ZY	**type stack** および **type control** キーワードが、Catalyst 6500 シリーズの Programmable Intelligent Services Accelerator（PISA）が搭載されているスイッチの Cisco IOS Release 12.2(18)ZY に統合されました。
12.2(33)SRC	このコマンドのサポートが Cisco 7600 シリーズ ルータで拡張されました。
12.2(33)SB	このコマンドが変更されました。PRE3 用と PRE4 用の Cisco 10000 シリーズ ルータに実装されました。
Cisco IOS XE リリース 2.3	このコマンドは、ATM PVP コンフィギュレーション モードをサポートするよう、変更されました。
12.4(18e)	このコマンドが変更され、同じインターフェイスにレガシー トラフィック シェーピングと Cisco モジュラ QoS CLI（MQC）シェーピングを同時に設定することはできなくなりました。
Cisco IOS XE リリース 3.3S	このコマンドが変更され、イーサネット サービス コンフィギュレーション モードがサポートされるようになりました。
Cisco IOS XE リリース 3.5S	このコマンドが変更されました。**service-policy input** または **service-policy output** コマンドを設定しようとすると、エラーが表示されるのは、**ip subscriber interface** コマンドがインターフェイスに設定済みの場合です。
15.2(1)S	このコマンドが変更され、同時非キューイング ポリシーをサブインターフェイスで有効にできるようになりました。
15.2(2)E	このコマンドが、Cisco IOS リリース 15.2(2)E に統合されました。このコマンドは、テンプレート コンフィギュレーション モードでサポートされます。
Cisco IOS XE Release 3.6E	このコマンドが Cisco IOS XE Release 3.6E に統合されました。このコマンドは、テンプレート コンフィギュレーション モードでサポートされます。

使用上のガイドライン

次の表に、コマンドの用途別のコンフィギュレーション モードを示します。

表 *42 :* コマンド用途別のコンフィギュレーション モード

Application	モード
独立型 VC	ATM VC サブモード
ATM VC バンドル メンバー	ATM VC バンドル コンフィギュレーション
ATM PVC の範囲	サブインターフェイス コンフィギュレーション
PVC 範囲内の個別の PVC	ATM PVC-in-range コンフィギュレーション
フレーム リレー VC	スタティック マップ クラス コンフィギュレーション
イーサネット サービス、イーサネット VC（EVC）	イーサネット サービス コンフィギュレーション
インターフェイス テンプレート（Interface Template）	テンプレート コンフィギュレーション

1 つまたは複数のインターフェイスや、1 つまたは複数の VC に、1 つのポリシー マップを付加し、これらのインターフェイスまたは VC にサービス ポリシーを指定できます。

クラスベース WFQ（CBWFQ）。ポリシー マップに含まれるクラス ポリシーは、そのクラスのクラス マップの一致基準を満たすパケットに適用されます。

インターフェイスまたは ATM VC にポリシー マップを適用するには、ポリシー マップに含まれるクラスに設定されている最小帯域幅の集約値が、インターフェイス帯域幅または VC に割り当てられている帯域幅の 75%（Cisco 10008 ルータでは 99%）以下である必要があります。

フレーム リレー（プライオリティ キューイング [PQ]/CBWFQ）の低遅延キューイング（LLQ）を有効にするには、まずインターフェイス コンフィギュレーション モードで **frame-relay traffic-shaping** コマンドを使用して、インターフェイスでフレーム リレー トラフィック シェーピング（FRTS）を有効にする必要があります。次に、スタティック マップ クラス コンフィギュレーション モードで **service-policy** コマンドを使用して、出力サービス ポリシーをフレーム リレー VC に適用します。

インターフェイスまたは ATM VC にポリシー マップを適用するには、ポリシー マップに含まれるクラスに設定されている最小帯域幅の集約値が、インターフェイス帯域幅または VC に割り当てられている帯域幅の 75% 以下である必要があります。フレーム リレー VC の場合、割り当てられた帯域幅の合計量が、VC に設定された最小の認定情報レート（CIR）を超えない（**frame-relay voice bandwidth** または **frame-relay ip rtp priority** スタティック マップ クラス コンフィギュレーション モード コマンドで予約した帯域幅を超えない）ようにします。これらの値が設定されていない場合、最小 CIR のデフォルト値は CIR の半分になります。

物理インターフェイスでの CBWFQ は、インターフェイスがデフォルトのキューイング モードにある場合のみ設定可能です。E1（2.048 Mbps）以下のシリアル インターフェイスでは、重み付け均等化キューイング（WFQ）がデフォルトで使用されます。その他のインターフェイスでは、ファーストイン ファーストアウト（FIFO）がデフォルトで使用されます。物理インター

フェイスで CBWFQ をイネーブルにすると、デフォルトのインターフェイス キューイング方式が上書きされます。ATM 相手先固定接続（PVC）で CBWFQ をイネーブルにしても、デフォルトのキューイング方式は無効になりません。

CBWFQ に対応したサービス ポリシーをインターフェイスに適用する場合、均等化キューイング、カスタム キューイング、プライオリティ キューイング、重み付けランダム早期検出（WRED）などの高度なキューイングに関連するコマンドは、モジュラ Quality of Service CLI（MQC）で使用できます。ただし、ポリシーマップをインターフェイスから削除するまでは、これらの機能を直接インターフェイスに設定できません。

（注） Cisco IOS Release 12.4(18e) 以降は、トラフィック シェープ レートおよび MQC シェーピングを同時に同じインターフェイスに設定することはできません。サービス ポリシーを適用する前に、インターフェイスに設定されたトラフィック シェープ レートを削除する必要があります。たとえば、**traffic-shape rate** コマンドがすでに有効になっているときに **service-policy** {**input** | **output**} *policy-map-name* コマンドを入力しようとすると、このメッセージが表示されます

```
Remove traffic-shape rate configured on the interface before attaching the service-policy.
```

MQC シェーパーが最初に適用された場合、レガシー **traffic-shape rate** コマンドを同じインターフェイスに入力すると、コマンドが拒否され、エラー メッセージが表示されます。

インターフェイスまたは VC に適用したポリシーマップを変更して、このマップに含まれるいずれかのクラスの帯域幅を変更できます。適用済みポリシーマップに加えた帯域幅変更は、ポリシーマップに含まれるすべてのクラスの帯域幅（変更されたクラス帯域幅を含む）量の集約値が、インターフェイス帯域幅または VC 帯域幅の 75% 以下である場合のみ、有効です。新しい集約帯域幅量がインターフェイス帯域幅または VC 帯域幅の 75% を超える場合、ポリシーマップは変更されません。

サービス クラス（CoS）ビットを設定する **service-policy** コマンドをイーサネット インターフェイスに適用すると、8021.Q または Inter-Switch Link（ISL）トランキングが動作するサブインターフェイスが存在している限り、このポリシーはアクティブです。ただし、リロード時に次のエラー メッセージが表示されて、設定からサービス ポリシーが削除されます。

```
Process "set" action associated with class-map voip failed: Set cos supported only with
 IEEE 802.1Q/ISL interfaces.
```

（注） **service-policy input** および **service-policy output** コマンドは、**ip subscriber interface** コマンドがインターフェイスに設定済みの場合、設定できません。これらのコマンドを両方設定することはできません。

同時非キューイング QoS ポリシー

Cisco IOS Release 15.2(1)S 以降は、ATM サブインターフェイスおよび ATM PVC、またはフレームリレー（FR）サブインターフェイスおよびデータリンク接続識別子（DLCI）に同時非キューイング QoS ポリシーを設定できます。ただし、階層型キューイング フレームワーク層競合が

発生するため、同時キューイング ポリシーは引き続き使用できません。同時キューイング ポリシーを設定しようとすると、ポリシーが拒否され、ルータにエラー メッセージが表示されます。

（注） 同じサブインターフェイスに PVC または DLCI ポリシーとサブインターフェイス ポリシーの両方を適用する場合、PVC または DLCI のポリシーが優先され、サブインターフェイス ポリシーは無効になります。

Cisco 10000 シリーズ ルータの使用上のガイドライン

Cisco 10000 シリーズ ルータでは、未指定ビット レート（UBR）VC への CBWFQ ポリシーの適用はサポートされていません。

インターフェイスまたは VC にポリシー マップを適用するには、ポリシー マップに含まれるクラスに設定されている最小帯域幅の集約値が、インターフェイス帯域幅または VC に割り当てられている帯域幅の 99% 以下である必要があります。クラスに割り当てられている帯域幅の合計が使用可能な帯域幅の 99% を超えている場合にポリシー マップをインターフェイスに適用しようとすると、ルータのログに警告メッセージが記録され、要求された帯域幅がクラスのすべてには割り当てられません。ポリシーマップが他のインターフェイスにすでに適用されている場合、そのインターフェイスから削除されます。

帯域幅の合計は、物理インターフェイスの ATM 層の速度（レート）です。ルータは、指定した最小帯域幅をインターフェイス速度の 1/255（ESR–PRE1）または 1/65,535（ESR–PRE2）の至近の倍数に変換します。1/255 または 1/65,535 の倍数ではない値を要求すると、ルータによって最も近い倍数が選択されます。

帯域幅のパーセンテージは、インターフェイスの帯域幅に基づきます。階層型ポリシーでは、帯域幅のパーセンテージは至近の親シェープ レートに基づきます。

デフォルトでは、最小帯域幅保証キューにはライン レートで 32 パケット以上、256 バイトのパケットの最大 50 ミリ秒のバッファがあります。

Cisco IOS Release 12.0(22)S 以降の場合、Cisco 10000 シリーズ ルータでフレーム リレーの LLQ（プライオリティ キューイング（PQ）/CBWFQ）を有効にするには、まずポリシー マップを作成した後、**priority** コマンドを使用して、定義済みのトラフィック クラスに優先順位を割り当てます。たとえば、次の設定例では 8000 kb/s 保証帯域幅のプライオリティ キューを設定します。この例では、「map1」という名前のポリシーマップのビジネス クラスはプライオリティ キューとして設定されます。map1 ポリシーには 48 kb/s 最低帯域保証の非ビジネス クラスも含まれます。map1 ポリシーは、発信方向のシリアル インターフェイス 2/0/0 に適用されます。

```
class-map Business
 match ip precedence 3
policy-map map1
 class Business
 priority
 police 8000
 class Non-Business
 bandwidth 48
interface serial 2/0/0
```

```
frame-relay encapsulation
service-policy output map1
```

PRE2 では、**service-policy** コマンドを使用して、QoS ポリシーを ATM サブインターフェイスまたは PVC に適用します。ただし、PRE3 では、PVC のみに QoS ポリシーを適用できます。

Cisco 7600 シリーズ ルータ

output キーワードは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

EtherChannel のメンバーであるポートに、サービス ポリシーを付加しないでください。

CLI を使用すると、OC-12 ATM オプティカル サービス モジュール（OSM）の WAN ポートおよびチャネライズド OSM の WAN ポートにポリシー フィーチャ カード（PFC）ベースの QoS を設定できますが、PFC ベースの QoS はこれらの OSM の WAN ポートではサポートされていません。OSM は、Supervisor Engine 32 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

PFC QoS は、VLAN インターフェイス上だけで **output** キーワード（任意）をサポートします。VLAN インターフェイスには、入力ポリシー マップおよび出力ポリシー マップの両方を適用できます。

Cisco 10000 シリーズ ルータの制御ポリシー マップ

コンテキストに適用して、制御ポリシー マップをアクティブ化します。制御ポリシー マップは次のタイプのコンテキスト（優先順位で表示）の 1 つ以上に適用できます。

1. グローバル
2. インターフェイス
3. サブインターフェイス
4. Virtual template
5. VC クラス
6. PVC

一般的に、より限定的なコンテキストに適用される制御ポリシーマップが、より汎用的なコンテキストに適用されるポリシーマップよりも優先されます。リストでは、コンテキストのタイプに優先順位で番号を付けています。たとえば、相手先固定接続（PVC）に適用される制御ポリシー マップは、インターフェイスに適用される制御ポリシー マップよりも優先されます。

コンテキストでホストされるすべてのセッションに制御ポリシーが適用されます。特定のコンテキストに適用できる制御ポリシー マップは 1 つだけです。

service-policy コマンドの省略形

Cisco IOS Release 12.2(33)SB 以降では、ルータで **service-policy** コマンドの省略形（ser）は使用できません。ルータでこのコマンドを使用するには、コマンド名 **service-** を入力する必要があ

ります。たとえば、**service-policy** コマンドの省略形を使用すると、次のエラー メッセージが表示されます。

```
interface GigabitEthernet1/1/0
 ser out ?
% Unrecognized command
 ser ?
% Unrecognized command
```

次の例に示すように、このコマンドを **service-** の後にスペースを入れて入力すると、ルータはコマンドを **service-policy** と解析します。疑問符を入力すると、ルータは **service-policy** コマンドのコマンド オプションを表示します。

```
service- ?
input Assign policy-map to the input of an interface
output Assign policy-map to the output of an interface
type Configure CPL Service Policy
```

Cisco IOS Release 12.2(33)SB より前のリリースでは、ルータで **service-policy** コマンドの省略形が使用できます。たとえば、次のコマンドが使用できます。

```
interface GigabitEthernet1/1/0
 ser out test
```

例

次に、ポリシー マップをファスト イーサネット インターフェイスに適用する例を示します。

```
interface fastethernet 5/20
 service-policy input pmap1
```

次の例では、「policy9」という名前のサービス ポリシー マップを出力シリアル インターフェイス 1 の DLCI 100 に適用し、フレーム リレーの LLQ を有効にします。

```
interface Serial1/0.1 point-to-point
 frame-relay interface-dlci 100
 class fragment
 map-class frame-relay fragment
 service-policy output policy9
```

次の例では、「policy9」という名前のサービス ポリシー マップを入力シリアル インターフェイス 1 に適用します。

```
interface Serial1
 service-policy input policy9
```

次の例では、「policy9」という名前のサービス ポリシーマップを「cisco」という名前の入力 PVC に適用します。

```
pvc cisco 0/34
service-policy input policy9
vbr-nt 5000 3000 500
precedence 4-7
```

次の例では、「policy9」という名前のポリシーを出力シリアル インターフェイス 1 に適用して、このインターフェイスにサービス ポリシーを指定し、CBWFQ を有効にします。

```
interface serial1
 service-policy output policy9
```

次の例では、「policy9」という名前のサービス ポリシーマップを「cisco」という名前の出力 PVC に適用します。

```
pvc cisco 0/5
service-policy output policy9
vbr-nt 4000 2000 500
precedence 2-3
```

Cisco 10000 シリーズ ルータの設定例

次の例では、「userpolicy」という名前のサービス ポリシーを発信パケット用シリアル サブインターフェイス 1/0/0.1 の DLCI 100 に適用します。

```
interface serial 1/0/0.1 point-to-point
 frame-relay interface-dlci 100
 service-policy output userpolicy
```

（注） この方法でポリシーを DLCI に適用するには、Cisco IOS Release 12.0(22)S 以降が動作している必要があります。Cisco IOS Release 12.0(22)S より前のリリースが動作している場合、前述の「「policy9」という名前のサービス ポリシー マップを出力シリアル インターフェイス 1 の DLCI 100 に適用し、フレーム リレーの LLQ を有効にします」の設定例に示すように、レガシー フレーム リレー コマンドを使用してサービス ポリシーを適用します。

次の例では、「map2」という名前の QoS サービス ポリシーを着信トラフィック用 ATM サブインターフェイス 3/0/0.1 の PVC 0/101 に適用します。

```
interface atm 3/0/0
 atm pxf queueing
interface atm 3/0/0.1
 pvc 0/101
 service-policy input map2
```

（注） **atm pxf queueing** コマンドは PRE3 または PRE4 でサポートされていません。

次の例では、「myQoS」という名前のサービスポリシーを着信トラフィック用物理ギガビット イーサネット インターフェイス 1/0/0 に適用します。VLAN 4（ギガビット イーサネット サブインターフェイス 1/0/0.3 に設定）は、物理ギガビット イーサネット インターフェイス 1/0/0 のサービス ポリシーを継承します。

```
interface GigabitEthernet 1/0/0
 service-policy input myQoS
interface GigabitEthernet 1/0/0.3
 encapsulation dot1q 4
```

次の例では、「policy1」という名前のポリシー マップを「virtual-template1」という名前のすべての着信トラフィック用仮想テンプレートに適用します。この例では、仮想テンプレート設定にはChallenge Handshake Authentication Protocol（CHAP）認証およびPPP 認証とアカウンティングも含まれます。

```
interface virtual-template1
 ip unnumbered Loopback1
 no peer default ip address
 ppp authentication chap vpn1
 ppp authorization vpn1
 ppp accounting vpn1
 service-policy input policy1
```

次の例では、「voice」という名前のサービス ポリシー マップを、3 つの PVC 合計の PVC 範囲内の ATM VC 2/0/0 に適用し、サブインターフェイス コンフィギュレーション モードを有効にします。このモードで、ポイントツーポイント サブインターフェイスが範囲内の各PVCに作成されます。この範囲内に作成された各PVCには、音声サービス ポリシーを適用します。

```
configure terminal
 interface atm 2/0/0
 range pvc 1/50 1/52
 service-policy input voice
```

次の例では、「voice」という名前のサービス ポリシー マップを、PVC 範囲内の ATM VC 2/0/0 に適用します。この範囲内に作成されたすべてのVCに音声サービス ポリシーを適用します。例外はPVC 1/51 で、この範囲内で別のPVCとして設定され、「data」という名前の別のサービス ポリシーがATM PVC-in-rangeコンフィギュレーション モードで適用されます。

```
configure terminal
 interface atm 2/0/0
 range pvc 1/50 1/52
 service-policy input voice
 pvc-in-range 1/51
 service-policy input data
```

次の例では、「PREMIUM-SERVICE」という名前のサービス グループを設定し、「PREMIUM-MARK-IN」という名前の入力ポリシーと「PREMIUM-OUT」という名前の出力ポリシーをこのサービス グループに適用します。

```
policy-map type service PREMIUM-SERVICE
 service-policy input PREMIUM-MARK-IN
 service-policy output PREMIUM-OUT
```

次の例では、同時非キューイング ポリシーをサポートしているポリシーマップおよびインターフェイス設定を表示します。

```
Policy-map p-map
```

```
class c-map
set mpls experimental imposition 4

interface ATM1/0/0.1 multipoint
no atm enable-ilmi-trap
xconnect 10.1.1.1 100001 encapsulation mpls
service-policy input p-map
pvc 1/41 l2transport
no epd
!
pvc 1/42 l2transport
no epd
!
pvc 1/43 l2transport
no epd
interface ATM1/0/0.101 multipoint
no atm enable-ilmi-trap
pvc 9/41 l2transport
xconnect 10.1.1.1 1001011 encapsulation mpls
service-policy input p-map
!
pvc 10/41 l2transport
xconnect 10.1.1.1 1001012 encapsulation mpls
!
```

次の例では、同時非キューイング QoS ポリシーを ATM サブインターフェイスと ATM PVC に適用します。

```
interface atm 1/0/0.101
pvc 9/41
service-policy input p-map
```

次の例では、インターフェイステンプレートの組み込み自動設定ポリシーマップを有効にします。

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# service-policy type control subscriber BUILTIN_AUTOCONF_POLICY

Device(config-template)# end
```

関連コマンド

コマンド	説明
class-map	QoS クラスマップ コンフィギュレーション モードにアクセスし、QoS クラス マップを設定します。
frame-relay ip rtp priority	UDP 宛先ポートの範囲内の RTP パケット フローセットについて、フレーム リレー PVC に絶対優先キューを予約します。
frame-relay traffic-shaping	フレーム リレー インターフェイスのすべての PVC と SVC に、トラフィック シェーピングと仮想回線単位キューイングを両方有効にします。
frame-relay voice bandwidth	特定の DLCI の音声トラフィック用に予約する帯域幅量を指定します。

コマンド	説明
ip subscriber interface	ISG IP インターフェイス セッションを作成します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
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与えます。
show policy-map	指定されたサービス ポリシーマップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
show policy-map interface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。
traffic-shape rate	インターフェイスの発信トラフィックにトラフィック シェーピングを有効にします。

service-policy（クラスマップ）

ポリシー マップをクラスに適用するには、クラスマップ コンフィギュレーション モードで **service-policy** コマンドを使用します。クラスからサービス ポリシーを削除するには、このコマンドの **no** 形式を使用します。

service-policy *policy-map*
no service-policy

構文の説明

policy-map	適用されるサービス ポリシー マップ（**policy-map** コマンドを使用して作成）の名前。名前には最大 40 文字までの英数字を指定できます。

コマンド デフォルト

サービス ポリシーは指定されていません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(2)T	このコマンドが導入されました。
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。

使用上のガイドライン

1 つまたは複数のクラスに 1 つのポリシー マップを付加し、これらのクラスにサービス ポリシーを指定できます。このコマンドは、出力インターフェイスだけで使用可能であると見なされます。

例

次の例では、cust1-classes、cust2-classes、cust-policy の 3 つのポリシー マップが定義されます。ポリシー マップ cust1-classes と cust2-classes には、gold、silver、bronze の 3 つのクラスが定義されます。

cust1-classes では、帯域幅の 50% を使用するよう、gold が設定されます。silver は、帯域幅の 20% を使用するよう設定され、bronze は帯域幅の 15% を使用するよう設定されます。

cust2-classes では、帯域幅の 30% を使用するよう、gold が設定されます。silver は、帯域幅の 15% を使用するよう設定され、bronze は帯域幅の 10% を使用するよう設定されます。

ポリシー マップ cust-policy では、384 kbps の平均レート シェーピングが指定され、cust1-classes という名前のサービス ポリシーが cust1-classes という名前のポリシー マッ

プに割り当てられます。ポリシー マップ cust-policy では、512 kbps のピーク レート シェーピングが指定され、cust2-classes という名前のサービス ポリシーが cust2-classes という名前のポリシー マップに割り当てられます。

cust1-classes に対してクラスを設定するには、次のコマンドを使用します。

```
Router(config)# policy-map cust1-classes
Router(config-pmap)# class gold
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class silver
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap-c)# exit
Router(config-pmap)# class bronze
Router(config-pmap-c)# bandwidth percent 15
```

cust2 に対してクラスを設定するには、次のコマンドを使用します。

```
Router(config)# policy-map cust2-classes
Router(config-pmap)# class gold
Router(config-pmap-c)# bandwidth percent 30
Router(config-pmap-c)# exit
Router(config-pmap)# class silver
Router(config-pmap-c)# bandwidth percent 15
Router(config-pmap-c)# exit
Router(config-pmap)# class bronze
Router(config-pmap-c)# bandwidth percent 10
```

cust1-classes、cust2-classes、および QoS 機能でカスタマー ポリシーを定義するには、次のコマンドを使用します。

```
Router(config)# policy-map cust-policy
Router(config-pmap)# class cust1
Router(config-pmap-c)# shape average 38400
Router(config-pmap-c)# service-policy cust1-classes
Router(config-pmap-c)# exit
Router(config-pmap)# class cust2
Router(config-pmap-c)# shape peak 51200
Router(config-pmap-c)# service-policy cust2-classes
Router(config-pmap-c)# interface Serial 3/2
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# exit
Router(config)# interface serial0/0
Router(config-if)# service out cust-policy
```

関連コマンド

コマンド	説明
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。

service-policy（コントロール プレーン）

集約または分散コントロール プレーン サービスのコントロール プレーンにポリシー マップを適用するには、コントロール プレーン 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。コントロール プレーンからサービス ポリシーを削除するには、このコマンドの **no** 形式を使用します。

service-policy {**input**|**output**} *policy-map-name*
no service-policy {**input**|**output**} *policy-map-name*

構文の説明

input	コントロールプレーンに着信するパケットに指定のサービス ポリシーを適用します。
output	指定したサービス ポリシーをコントロールプレーンを出るパケットに適用して、ルータでパケットを自動的に廃棄できるようにします。
policy-map-name	追加するサービス ポリシーマップの名前（**policy-map** コマンドを使用して作成）。名前には最大 40 文字までの英数字を指定できます。

コマンド デフォルト

サービス ポリシーは指定されていません。

コマンド モード

コントロール プレーン コンフィギュレーション（config-cp）

コマンド履歴

リリース	変更箇所
12.2(18)S	このコマンドが導入されました。
12.3(4)T	このコマンドが、Cisco IOS Release 12.3(4)T に統合されました。**output** キーワードのサポートが追加されました。
12.0(29)S	このコマンドが、Cisco IOS Release 12.0(29)S に統合されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
12.2(25)S	**output** キーワードのサポートが、Cisco IOS Release 12.2(25)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
Cisco IOS XE Release 2.2	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

control-plane コマンドを入力後、**service-policy** コマンドを使用して、Quality of Service（QoS）ポリシーを設定します。このポリシーは集約または分散コントロール プレーン サービスのコ

ントロール プレーン インターフェイスに適用されて、プロセス レベルに入るパケットの数やレートを制御します。

service-policyoutput*policy-map-name* コマンドを使用して、コントロール プレーン トラフィックに出力ポリシングを設定する場合、ルータは自動的にパケットを廃棄します。出力ポリシングは次のリリースでサポートされます。

- サポートされるのは次のリリースのみです。
  - Cisco IOS Release 12.2(25)S およびそれ以降の Cisco IOS 12.2S リリース。
  - Cisco IOS Release 12.3(4)T およびそれ以降の Cisco IOS 12.3T リリース。
  - Cisco IOS Release 12.2(18)SXD1 およびそれ以降の Cisco IOS 12.2SX リリース。
  - Cisco IOS XE Release 2.2 およびそれ以降の Cisco IOS XE リリース。
- 分散コントロール プレーン サービスに QoS ポリシーを適用する場合はサポートされません。
- Cisco 6500 ルータ、Cisco 7500 シリーズ、および Cisco 10720 インターネット ルータでは、サポートされません。

service-policyoutput コマンドで出力ポリシングを設定し、サイレント モードで実行すると、適用された QoS ポリシーに基づいて、コントロール プレーンから出て行くパケットが自動的に廃棄されます。サイレント モードでは、Cisco IOS ソフトウェアが動作しているルータは、システム メッセージを送信せずに動作できます。コントロール プレーンから出て行くパケットが出力ポリシングで廃棄されても、エラー メッセージを受け取ることはありません。

サイレント モードでは、Cisco IOS ソフトウェアが動作しているルータは、システム メッセージを送信せずに動作できます。ルータ宛のパケットが何らかの理由で廃棄された場合も、ユーザはエラー メッセージを受信しません。エラー メッセージを生成しないイベントは次のとおりです。

- ルータが待ち受けていないポートにトラフィックが送信されている場合
- 要求の形式に誤りがあるために正規のアドレスとポートへの接続が拒否される場合

例

次の例では、送信元アドレス 10.1.1.1 および 10.1.1.2 の信頼できるホストを設定し、Telnet パケットをコントロール プレーンに無制限に転送する方法を示します。残りのすべての Telnet パケットは、指定レートでポリシングされるようにします。

```
! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet

! Allow
10.1.1.2
 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet

! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class-map “telnet-class.”
Router(config)# class-map telnet-class
```

```
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-policy
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control plane service for the active route processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-policy
Router(config-cp)# end
```

次に、送信元アドレス 10.0.0.0 および 10.0.0.2 の信頼できるネットワークは Internet Control Message Protocol（ICMP）ポート到達不能応答を無制限に受信し、残りのすべての ICMP ポート到達不能応答を廃棄できるように設定する例を示します。

```
! Allow 10.0.0.0 trusted network traffic.
Router(config)# access-list 141 deny icmp host
10.0.0.0

255.255.255.224
 any port-unreachable

! Allow 10.0.0.2 trusted network traffic.
Router(config)# access-list 141 deny icmp host
10.0.0.2 255.255.255.224
 any port-unreachable

! Rate-limit all other ICMP traffic.
Router(config)# access-list 141 permit icmp any any port-unreachable
Router(config)# class-map icmp-class

Router(config-cmap)# match access-group 141
Router(config-cmap)# exit
Router(config)# policy-map control-plane-out-policy
! Drop all traffic that matches the class "icmp-class."
Router(config-pmap)# class icmp-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# control-plane
! Define aggregate control plane service for the active route processor.
Router(config-cp)# service-policy output control-plane-out-policy
Router(config-cp)# end
```

関連コマンド

コマンド	説明
control-plane	コントロール プレーン コンフィギュレーション モードで、コントロール プレーン宛てのトラフィックをポリシングする QoS ポリシーを適用します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
showpolicy-mapcontrol-plane	コントロール プレーンにアタッチされたポリシー マップのあるクラス、またはすべてのクラスの設定を表示します。

service-policy（ポリシーマップ クラス）

ポリシー マップ内で QoS ポリシーとしてサービス ポリシー（階層型サービス ポリシー）を使用するには、ポリシーマップ クラス コンフィギュレーション モードで **service-policy** コマンドを使用します。ポリシー マップ内で QoS ポリシーとして特定のサービス 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 *policy-map-name*
no service-policy *policy-map-name*

構文の説明

policy-map-name	QoS ポリシーとして使用される事前定義済みのポリシー マップの名前を指定します。名前には最大 40 文字までの英数字を指定できます。

コマンド デフォルト

サービス ポリシーは使用されません。

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.1(2)E	このコマンドが導入されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
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。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

このコマンドは、ポリシー マップ コンフィギュレーション モードで階層サービス ポリシーの作成に使用されます。

このコマンドは、インターフェイス コンフィギュレーション モードで使用する **service-policy** {**input**|**output**}*policy-map-name* コマンドとは異なります。
service-policy{**input**|**output**}*policy-map-name* の用途は、インターフェイスへのサービス ポリシーの適用です。

子ポリシーは、**service-policy** コマンドを使用して新しいサービス ポリシーに関連付けられている、事前定義済みのサービス ポリシーです。既存のサービス ポリシーを使用する新しいサービス ポリシーが親ポリシーです。

このコマンドには、次の制限があります。

- **priority** コマンドは、親ポリシーと子ポリシーのいずれかで使用できますが、両方のポリシーで同時に使用することはできません。
- **shape** コマンドは、親ポリシーと子ポリシーのいずれかで使用できますが、サブインターフェイスの両方のポリシーで同時に使用することはできません。
- **fair-queue** コマンドは、親ポリシーで定義できません。
- 子ポリシーで **bandwidth** コマンドを使用する場合、**bandwidth** コマンドを親ポリシーでも使用する必要があります。デフォルト クラスを使用するポリシーが 1 つの例外となります。

例

次に、parent という名前のサービス ポリシーで、階層サービス ポリシーを作成する例を示します。

```
Router(config)# policy-map child
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# service-policy child
```

Versatile Interface Processor（VIP）対応 Cisco 7500 シリーズ ルータの FRF.11 と FRF.12 設定は、設定時に階層型サービス ポリシーが必要なことがよくあります。FRF.11 と FRF.12 の階層型サービス ポリシーには次の要素が必要です。

1. Voice over Frame Relay（VoFR）プロトコルのみを一致基準として使用するトラフィック クラス。
2. **priority** コマンドを使用した低遅延キューイング（LLQ）をすべての VoFR プロトコル トラフィックに保証するトラフィック ポリシー。
3. シェーピング パラメータが定義され、要素 2 に示す要素が含まれるトラフィック ポリシー。

要素 3 は、**service-policy** コマンドで設定する、階層型サービス ポリシーを使用した場合のみ実現可能です。

次の例では、要素 1 はトラフィック クラス frf で、要素 2 はトラフィック ポリシー llq で、要素 3 はトラフィック ポリシー lq-shape で設定されます。

```
Router(config)#

class-map frf
Router(config-cmap)# match protocol vofr
Router(config-cmap)
#
exit
Router(config)#
```

```
policy-map llq
Router(config-pmap)#

class frf
Router(config-pmap-c)# priority 2000
Router(config-pmap-c)#

exit
Router(config-pmap)# exit
Router(config)# policy-map llq-shape
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 1000 128000
Router(config-pmap-c)#

service-policy llq
```

FRF.11 と FRF.12 の階層型サービス ポリシーを使用する最後の手順は、マップクラス コンフィギュレーション モードで実行します。次の例では、トラフィック ポリシー llq-shape をマップ クラス frag に適用します。

```
Router(config)#

map-class frame-relay frag
Router(config-map-class)# frame-relay fragment 40
Router(config-map-class)# service-policy llq-shape
```

関連コマンド

コマンド	説明
bandwidth(policy-mapclass)	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。
fair-queue	トラフィック クラスでの使用のために確保されるキューの番号を指定します。
policy-map	設定するサービス ポリシーの名前を指定します。
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与えます。
service-policy	インターフェイスに付加するサービス ポリシーの名前を指定します。
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。
showpolicy-map	指定されたサービス ポリシーマップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

service-policy（サービス グループ）

ポリシー マップをサービス グループに適用するには、サービス グループ 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。サービス グループからポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

service-policy {**input**|**output**} *policy-map-name*
no service-policy {**input**|**output**} *policy-map-name*

構文の説明

input	ポリシー マップを入力方向のサービス グループに適用します。
output	ポリシー マップを出力方向のサービス グループに適用します。
policy-map-name	ポリシーマップ名です。既存のポリシーマップの名前を入力します。

コマンド デフォルト

ポリシー マップは、サービス グループに適用されません。

コマンド モード

サービス グループ コンフィギュレーション（config-service-group）

コマンド履歴

リリース	変更箇所
12.2(33)SRE	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 マップがすでに存在し、サービス レベル契約（SLA）で指定されているプロビジョニングに基づいてサービス グループに適用する Quality of Service（QoS）機能が含まれている必要があります。ポリシー マップを作成して設定するには、モジュラ QoS コマンドライン インターフェイス（CLI）（MQC）を使用します。MQC の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』を参照してください。

例

次の例では、3-customer-in という名前のポリシー マップがサービス グループ 1 に適用されます。

```
Router> enable

Router# configure terminal

Router(config)# service-group 1

Router(config-service-group)# service-policy input 3-customer-in

Router(config-service-group)# end
```

service-policy type qos

Quality of Service（QoS）ポリシー マップをアイデンティティに適用するには、アイデンティティ ポリシー コンフィギュレーション モードで **service-policytypeqos** コマンドを使用します。QoS ポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

service-policy type qos {**input**|**output**} *policy-map-name*
no service-policy type qos {**input**|**output**} *policy-map-name*

構文の説明

input	入力 QoS ポリシー マップを指定します。
output	出力 QoS ポリシー マップを指定します。
policy-map-name	ポリシー マップの名前。

コマンド デフォルト

QoS ポリシー マップは、アイデンティティに適用されません。

コマンド モード

アイデンティティ ポリシー コンフィギュレーション（config-identity-policy）

コマンド履歴

リリース	変更箇所
12.2(33)SXI	このコマンドが導入されました。

使用上のガイドライン

input および **output** キーワードは、ポリシー マップが適用される方向を示します。

policy-map-name 引数の値は、**policy-map***policy-map-name* グローバル コンフィギュレーション コマンドを使用して、スイッチに設定された QoS ポリシー マップを表します。

例

次の例では、入力 QoS ポリシー マップをアイデンティティに適用します。

```
Router(config)# identity policy policy1
Router(config-identity-policy)# service-policy type qos input my-in-policy
```

関連コマンド

コマンド	説明
identitypolicy	アイデンティティ ポリシーを作成します。
policy-map	ポリシー マップを作成、または変更します。
showepmsessionip	セッションがアクティブな場合、インターフェイスの設定とポリシーを表示します。

set atm-clp

ポリシーマップの設定時にATMセル損失率優先度（CLP）ビットを設定するには、**setatm-clp** コマンドをポリシーマップ クラス コンフィギュレーション モードで使用します。特定の ATM CLP ビット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。

set atm-clp
no set atm-clp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

マルチプロトコル ラベル スイッチング（MPLS）対応の ATM ネットワークを介して送信する際に、Cisco ルータによって IP パケットが ATM セルに変換される場合、ATM CLP ビットは Cisco ルータ インターフェイスによって自動的に 0 に設定されます。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.1(5)T	このコマンドが導入されました。
12.2(4)T	このコマンドが Cisco MGX RPM-PR カードを持つ Cisco MGX 8850 スイッチおよび MGX 8950 スイッチに実装されました。
12.2(4)T2	このコマンドが Cisco 7500 シリーズ ルータに実装されました。
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。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
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

このコマンドを無効にするには、**noservice-policy** コマンドを使用して、インターフェイスからサービス ポリシーを削除します。

setatm-clp コマンドは、拡張 ATM ポート アダプタ（PA-A3）、T1 ポート 8 点付きの ATM IMA ポート アダプタ（PA-A3-8T1IMA）、E1 ポート 8 点付きの ATM IMA ポート アダプタ（PA-A3-8E1IMA）のいずれかをサポートするプラットフォームでのみ動作します。詳細については、使用しているルータのドキュメントを参照してください。

setatm-clp コマンドが含まれるポリシー マップは、出力ポリシーとしてのみ適用できます。**setatm-clp** コマンドでは、ルータから発信されるパケットはサポートされません。ATM セット CLP ビット Quality of Service（QoS）を含むポリシー マップは、PPP over X（PPPoX）セッショ

ンに適用できません。このポリシー マップは、**setatm-clp** コマンドを指定しない場合のみ適用できます。

例

次の例では、ポリシー マップで **setatm-clp** コマンドを使用して、CLP ビットを設定します。

```
Router(config)#
class-map ip-precedence
Router(config-cmap)#
match ip precedence 0 1
Router(config-cmap)#
exit
Router(config)#
policy-map atm-clp-set
Router(config-pmap)#
class ip-precedence
Router(config-pmap-c)#
set atm-clp
Router(config-pmap-c)#
exit
Router(config-pmap)#
exit
Router(config)#
interface atm 1/0/0.1
Router(config-if)#
service-policy output policy1
```

関連コマンド

Command	Description
class	マップ クラスを、指定したデータリンク接続識別子に関連付けます。
class-map	クラス マップを設定します。
interface	インターフェイスを作成します。
match ip precedence	一致基準として使用する IP プレシデンス値を指定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
service-policy	ポリシーマップを入力インターフェイス、仮想回線（VC）、出力インターフェイス、またはインターフェイスや VC のサービス ポリシーとして使用する VC に適用します。
showatmpvc	すべての ATM PVC およびトラフィック情報を表示します。
showpolicy-map	インターフェイスのポリシー マップについての情報を表示します。

set cos

発信パケットのレイヤ 2 サービス クラス（CoS）値を設定するには、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 **setcos** コマンドを使用します。特定の CoS 値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。

set cos {*cos-value*|*from-field* [**table** *table-map-name*]}
no set cos {*cos-value*|*from-field* [**table** *table-map-name*]}

Cisco CMTS、および 10000 シリーズ ルータ
set cos *cos-value*

構文の説明

cos-value	0 ～ 7 の特定の IEEE 802.1Q CoS 値です。
from-field	パケットの CoS 値の設定に使用される特定のパケットマーキング カテゴリです。パケットマーキング値のマッピングと変換のためにテーブル マップを使用している場合、これが「map from」パケットマーキング カテゴリを確立します。パケットマーキング カテゴリ キーワードは次のとおりです。 • **precedence** • **dscp**
table	（任意）指定のテーブル マップに設定された値が CoS 値の設定に使用されることを示します。
table-map-name	（任意）CoS 値の指定に使用されるテーブル マップ名です。テーブル マップ名には、最大 64 の英数字を使用できます。

コマンド デフォルト

発信パケットには CoS 値は設定されていません。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(5)T	このコマンドが導入されました。
12.2(13)T	このコマンドは、拡張パケット マーキングで、マッピング テーブル（テーブル マップ）を使用して packet-marking の値を変換し、送信できるよう、変更されました。
12.0(16)BX	このコマンドは、ESR-PRE2 用の Cisco 10000 シリーズ ルータに実装されました。
12.0(31)S	このコマンドが、Cisco IOS Release 12.0(31)S に統合されました。
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。

リリース	変更箇所
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
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。
12.2(33)SCF	このコマンドが、Cisco IOS リリース 12.2(33)SCF に統合されました。
3.2SE	このコマンドが、Cisco IOS XE リリース 3.2SE に統合されました。

使用上のガイドライン

CoS パケット マーキングは、シスコ エクスプレス フォワーディングのスイッチング パスでのみサポートされます。

setcos コマンドは、スイッチに送信中のパケットにマーキングをする場合に、ルータで使用する必要があります。スイッチは、CoS 値のマーキングを含む レイヤ 2 ヘッダー情報を利用できます。

setcos コマンドは、インターフェイスの出力方向に対応付けられたサービス ポリシーでのみ使用できます。インターフェイスが受信するパケットは、CoS 値で設定できません。

matchcos および **setcos** コマンドは同時に使用すると、ルータとスイッチは CoS マーキング ベースの Quality of Service（QoS）の相互運用と提供ができます。

スイッチにより、CoS 値がすでに一致および設定できるため、CoS 値の一致によってレベル 2 とレベル 3 のマッピングを設定できます。ユーザ定義 QoS サービスを区別するようマーク付けする必要があるパケットが、ルータから出てスイッチに入る場合、スイッチではレイヤ 2 ヘッダーを処理できるため、ルータによりパケットの CoS 値を設定する必要があります。

拡張パケット マーキング機能でのこのコマンドの使用

このコマンドを拡張パケット マーキング機能の一部として使用すると、CoS 値のマッピングと設定に使用される「from-field」パケットマーキング カテゴリを指定できます。「from-field」パケットマーキング カテゴリは次のとおりです。

- Precedence
- Diffserv コード ポイント（DSCP）

「from-field」カテゴリを指定しても **table** キーワードと適用可能な *table-map-name* 引数を指定していない場合、デフォルト アクションとは「from-field」カテゴリに関連付けられた値を CoS 値としてコピーすることです。たとえば、**setcosprecedence** コマンドを設定する場合、プレシデンス値がコピーされ、CoS 値として使用されます。

DSCP マーキング カテゴリに対して同じことを行うことができます。つまり、**setcosdscp** コマンドを設定できます。この場合、DSCP 値がコピーされ、CoS 値として使用されます。

（注） **setcosdscp** コマンドを設定する場合、DSCP フィールドの最初の *3* ビット（クラス セレクタ ビット）のみが使用されます。

例

次の例では、異なるタイプのトラフィックに異なる CoS 値を割り当てるために、「cos-set」という名前のポリシー マップが作成されます。この例では、「voice」および「video-data」という名前のクラス マップがすでに作成されているものと想定しています。

```
Router(config)#
policy-map cos-set
Router(config-pmap)#
class voice
Router(config-pmap-c)#
set cos 1
Router(config-pmap-c)#
exit
Router(config-pmap)#
class video-data
Router(config-pmap-c)#
set cos 2
Router(config-pmap-c)#
end
```

拡張パケット マーキングの例

次の例では、「policy-cos」という名前のポリシー マップが作成され、「table-map1」という名前のテーブル マップで定義されている値が使用されます。「table-map1」というテーブル マップは、**table-map** (value mapping) コマンドで前に作成されたものです。**table-map** (value mapping) コマンドの詳細については、**table-map** (value mapping) コマンド ページを参照してください。

この例では、CoS 値の設定は「table-map1」に定義されているプレシデンス値に基づいています。

```
Router(config)#
policy-map policy-cos
```

```
Router(config-pmap)#

class class-default

Router(config-pmap-c)#

set cos precedence table table-map1
Router(config-pmap-c)#

end
```

Cisco CMTS ルータ：例

次の例では、802.1p ドメインにサービス クラスを設定します。

```
Router(config)# policy-map cos7
Router(config-pmap)# class cos7
Router(config-pmap-c)# set cos 2
Router(config-pmap-c)# end
```

（注） QoS ポリシーマップ コンフィギュレーション モードでサービス ポリシーを作成し、インターフェイスまたは ATM 仮想回線（VC）にサービス ポリシーを適用する場合、**setcos** コマンドを使用します。サービス ポリシーの適用についての詳細は、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Modular Quality of Service Command-Line Interface Overview」の章を参照してください。

関連コマンド

コマンド	説明
matchcos	レイヤ 2 CoS マーキングに基づいて、パケットを一致させます。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
service-policy	入力インターフェイスまたはVC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
setdscp	ToS バイトにレイヤ 3 DSCP 値を設定することにより、パケットにマーク付けします。
setprecedence	パケット ヘッダーに precedence 値を設定します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapclass	指定されたポリシーマップの指定されたクラスの設定を表示します。

コマンド	説明
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

set cos cos-inner（ポリシーマップ コンフィギュレーション）

QinQ-translated 発信パケットのトランク VLAN タグで 802.1Q プライオリティ ビットに、内部カスタマーエッジ VLAN タグからのプライオリティの値を設定するには、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 **setcoscos-inner** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

set cos cos-inner
no set cos cos-inner

構文の説明

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

P ビットが、外部プロバイダー エッジ VLAN タグからコピーされます。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(18)SXD	このコマンドのサポートが Supervisor Engine 720 に追加されました。
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。

使用上のガイドライン

このコマンドがサポートされるのは、Optical Service Module（OSM）-2+4GE-WAN+ OSM モジュール搭載の Cisco 7600 シリーズ ルータのギガビット イーサネット WAN インターフェイスのみです。

OSM は、Supervisor Engine 32 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

802.1P プライオリティ ビットは、QoS 処理の目的で VLAN タグで使用されます。

ルータにより二重タグ付き QinQ パケットが宛先インターフェイスにコピーされる場合、デフォルトで、外部（プロバイダー）VLAN タグからの P ビットが使用されます。内部（カスタマー）VLAN タグ内の P ビットを保持するには、**setcoscos-inner** コマンドを使用します。

setcoscos-inner コマンドを有効にするには、**mlsqostrust** コマンドを使用して、適切なインターフェイスまたはサブインターフェイスを信頼されたインターフェイスとして設定する必要があります。これ以外の場合、インターフェイスまたはサブインターフェイスはデフォルトで信頼されない状態になり、**setcoscos-inner** コマンドによって外部 VLAN タグにコピーできるようになるまで、レイヤ 2 インターフェイスでは着信パケットの P ビットがゼロに設定されます。

setcoscos-inner コマンドは、内部（カスタマー）VLAN で設定されているサブインターフェイスのみでサポートされています。**setcoscos-inner** コマンドは、**bridge-domain** (subinterface configuration) コマンドの **out-range** キーワードを使用するサブインターフェイス、または

bridge-domain (subinterface configuration) コマンドのいずれの形式でも設定されていないサブインターフェイスでは、サポートされません。

メインインターフェイスに適用されるポリシーに **setcoscos-inner** コマンドを設定する場合、この動作が維持されます。**setcoscos-inner** コマンドによって、特定の内部 VLAN で設定されたサブインターフェイスは影響を受けますが、VLAN で設定されていないサブインターフェイスや **out-range** キーワードで設定されているサブインターフェイスは影響を受けません。

例

次に、内部 VLAN タグからの P ビットが使用されている音声トラフィックに対して、ポリシー マップを設定する例を示します。

```
Router(config-cmap)# set cos cos-inner
```

次に、デフォルト ポリシー マップ クラスを設定し、そのデフォルト値をリセットする例を示します。

```
Router(config-cmap)# no set cos cos-inner
```

次に、**bridge-domain(subinterfaceconfiguration)** コマンドで設定されているサブインターフェイスにポリシーを適用しようとすると表示されるシステム メッセージの例を示します。

```
Router(config-if)# bridge-vlan 32 dot1q-tunnel out-range

Router(config-if)# service-policy output cos1

%bridge-vlan 32 does not have any inner-vlan configured. 'set cos cos-inner' is not
supported
```

関連コマンド

コマンド	説明
bridge-domain(subinterfaceconfiguration)	PVC を指定された vlan-id にバインドします。
classmap	QoS クラス マップ コンフィギュレーション モードにアクセスして QoS クラス マップを設定します。
modedot1q-in-dot1qaccess-gateway	ギガビット イーサネット WAN インターフェイスをイネーブルにして、Q-in-Q VLAN 変換に関してゲートウェイとして動作するようにします。
policy-map	QoS ポリシーマップを設定するための QoS ポリシーマップ コンフィギュレーション モードにアクセスします。
service-policy	ポリシーマップをインターフェイスに付加します。
setindscp(policy-mapconfiguration)	ToS バイトに IP DSCP を設定することにより、パケットにマーク付けします。
setipprecedence(policy-mapconfiguration)	IP ヘッダーに優先順位を設定します。

コマンド	説明
showcwanqinq	Q-in-Q 変換で使用される内部、外部、およびトランク VLAN を表示します。
showcwanqinqbridge-domain	QinQ 変換が行われるギガビット イーサネット WAN で使用されるプロバイダー エッジ VLAN ID を表示するか、または、特定のプロバイダー エッジ VLAN で使用されるカスタマー エッジ VLAN を表示します。
showcwanqinqinterface	1 つまたはすべてのギガビット イーサネット WAN インターフェイスおよびポート チャネル インターフェイス上の IEEE 802.1Q-in-802.1Q（Q-in-Q）変換のインターフェイス統計を表示します。
showpolicy-map	ポリシー マップ情報を表示します。
showpolicy-mapinterface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

set cos-inner

ブリッジ フレームで内部サービス クラス フィールドにマーク付けするには、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 **setcos-inner** コマンドを使用します。内部 CoS フィールドのマーキングを削除するには、このコマンドの **no** 形式を使用します。

set cos-inner *cos-value*
no set cos-inner *cos-value*

構文の説明

cos-value	IEEE 802.1q CoS の値は、0 ～ -7 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

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(33)SRA	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 Cisco IOS Release 12.2(33)SRA に導入され、拡張 FlexWAN モジュールでマルチポイント ブリッジング（MPB）機能を使用する場合と、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 で SPA の MPB 機能を使用する場合に、内部 CoS 値のマーキングがサポートされるようになりました。

このコマンドは、Cisco 7600 SIP-600 ではサポートされていません。

Cisco 7600 SIP-200 では、同じインターフェイスへ、このコマンドと **setcos** コマンドを使用することはサポートされていません。

Cisco 7600 シリーズ ルータで SIP によってサポートされる QoS とマーキング コマンドの形式の詳細については、『*Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide*』を参照してください。

例

次に、VLAN 100 で一致するすべてのトラフィックをクラス「vlan-inner-100」にフィルタリングする QoS クラスを設定する例を示します。この設定では、「vlan-inner-100」クラスに属するトラフィックに内部 CoS 値として 3 をマークするポリシーマップ（この名前も「vlan-inner-100」）の定義を示します。内部 CoS 値のマーキングはブリッジング機能でのみサポートされるため、設定には、**bridge-domain** コマンドを使用して VLAN 100 にトラフィックがブリッジ処理されているシリアル SPA インターフェイスへ、出力ポリシーとして適用中のサービス ポリシーも表示されます。

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
```

```
Router(config-pmap)# class vlan-inner-100
Router(config-pmap-c)# set cos-inner 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/0/0
Router(config-if)# no ip address
Router(config_if)# encapsulation ppp
Router(config-if)# bridge-domain 100 dot1q
Router(config-if)# service-policy output vlan-inner-100
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# end
```

関連コマンド

コマンド	説明
bridge-domain	RFC 1483 ATM ブリッジングまたは RFC 1490 フレーム リレー ブリッジングで、ブリッジ処理される仮想 LAN（VLAN）の、ATM 相手先固定接続（PVC）またはフレーム リレーのデータリンク接続識別子（DLCI）へのマップを、イネーブルにします。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
policy-map	1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
service-policy	ポリシー マップを入力インターフェイスまたは仮想回線（VC）（もしくは出力インターフェイスまたは VC）に付加して、そのインターフェイスまたは VC のサービス ポリシーとして使用します。

set cos-inner cos

外部 COS を二重タグ付きパケットの内部 COS にコピーするには、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 **setcos-innercos** コマンドを使用します。二重タグ付きパケットの内部 COS にコピーされた外部 COS 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-inner cos *cos-value*
no set cos-inner cos *cos-value*

構文の説明

cos-value	IEEE 802.1q CoS の値は、0 ～ -7 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

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(33)SRB	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 Cisco IOS Release 12.2(33)SRB に追加されました。このコマンドは、EVC サービス インスタンスに適用されているポリシーに限定されます。

分類のため、内部タグと外部タグへの参照は、回線上で見えるフレームにされます。つまり、それぞれ存在する場合、入力フレームでは、タグは "rewrite" の前にあり、出力フレームでは、タグは "rewrite" の後にあります。

マーキングのため、入力での外部 COS へのリファレンスは DBUS-COS に対して、出力へのリファレンスはフレームの最初のタグの COS に対して、それぞれ行われます。また、出力では、外部 COS と内部 COS へのリファレンスは、フレーム内のそれに対して行われます。

例

次に、外部 COS 3 と 4 で一致が行われ、外部 COS が内部 COS に対してコピーされる例を示します。

```
Router(config)# class-map cos3_4
Router(config-cmap)# match cos 3 4
Router(config)# policy-map mark-it-in
Router(config-pmap)# class cos3_4
Router(config-pmap-c)# set cos-inner cos
```

関連コマンド

コマンド	説明
bridge-domain	RFC 1483 ATM ブリッジングまたは RFC 1490 フレーム リレー ブリッジングで、ブリッジ処理される仮想 LAN（VLAN）の、ATM 相手先固定接続（PVC）またはフレーム リレーのデータリンク接続識別子（DLCI）へのマップを、イネーブルにします。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
service-policy	ポリシー マップを入力インターフェイスまたは仮想回線（VC）（もしくは出力インターフェイスまたは VC）に付加して、そのインターフェイスまたは VC のサービス ポリシーとして使用します。

set discard-class

廃棄クラス値でパケットをマーク付けするには、QoS ポリシーマップ コンフィギュレーション モードで **setdiscard-class** コマンドを使用します。パケットの廃棄クラス値の変更を防ぐには、このコマンドの **no** 形式を使用します。

set discard-class *value*
no set discard-class *value*

構文の説明

value	ドロップするトラフィックに対して、Per-Hop Behavior（PHB）を指定します。値により、トラフィックのタイプのプライオリティが設定されます。有効値の範囲は 0 ～ 7 です。

コマンド デフォルト

このコマンドを入力しない場合、パケットの廃棄クラス値は 0 に設定されます。

コマンド モード

QoS ポリシー マップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。
12.3(7)XI	このコマンドは、ESR-PRE2 用の Cisco 10000 シリーズ ルータに実装されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。

使用上のガイドライン

廃棄クラス値により、PHB の廃棄部分が示されます。DiffServ トンネリング パイプ モードでのみ **setdiscard-class** コマンドを使用します。廃棄クラスは、入力 PHB マーキングを使用して出力インターフェイスのパケットが分類される場合にだけ必要です。

このコマンドを使用すると、輻輳の場合にドロップされるトラフィックのタイプも指定できます。

Cisco 10000 シリーズ ルータ

このコマンドは、ESR-PRE2 でのみサポートされます。

例

次に、トラフィックが廃棄クラス値 2 に設定される例を示します。

```
set discard-class 2
```

関連コマンド

コマンド	説明
matchdiscard-class	特定の廃棄クラスのパケットを照合します。
random-detectdiscard-class-based	WRED の基礎をパケットのクラス廃棄値にします。

set dscp

タイプ オブ サービス（ToS）バイトに Differentiated Services Code Point（DSCP; DiffServ コードポイント）値を設定してパケットをマークするには、QoS 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 **setdscp** コマンドを使用します。以前に設定した 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。

set dscp {*dscp-value*|*from-field* [**table** *table-map-name*]}
no set dscp {*dscp-value*|*from-field* [**table** *table-map-name*]}

構文の説明

dscp-value	DSCP 値を設定する番号。指定できる範囲は 0 ～ 63 です。 次の予約キーワードは、数値の代わりに指定できます。 • **EF**（完全優先転送） • **AF11**（相対的優先転送クラス AF11） • **AF12**（相対的優先転送クラス AF12）
from-field	パケットの DSCP 値の設定に使用される特定のパケットマーキング カテゴリです。パケットマーキング カテゴリ キーワードは次のとおりです。 • **cos** • **qos-group** （注） パケットマーキング値のマッピングと変換のためにテーブル マップを使用している場合、これが「map from」パケットマーキング カテゴリを確立します。
table	（任意）指定したテーブル マップに設定した値は DSCP 値の設定に使用することを示します。 • このキーワードは、*from-field* 引数とともに使用します。
table-map-name	（任意）DSCP 値の指定に使用されるテーブルマップの名前。この名前には最大 64 文字までの英数字を指定できます。 • この引数は、**table** キーワードとともに使用します。

コマンド デフォルト

ToS バイトの DSCP 値は設定されません。

コマンド モード

QoS ポリシー クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。**setipdscp** コマンドを置き換えます
12.0(28)S	このコマンドが変更されました。このコマンドの IPv6 でのサポートが、Cisco 12000 シリーズ インターネット ルータに追加されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。

使用上のガイドライン

DSCP ビットを設定すると、他の Quality of Service（QoS）機能がビット設定で動作するようになります。

相互に排他的な DSCP と precedence

setdscp コマンドと **setprecedence** コマンドを同時に使用して、同じパケットをマークすることはできません。2 つの値（DSCP および precedence）は相互に排他的です。パケットにはどちらか一方の値を設定でき、両方を設定することはできません。

Precedence の値とキューイング

マーキングされたトラフィックには、ネットワークによってプライオリティ（または緊急処理のタイプ）が設定されます。通常は、ネットワーク エッジ（または管理ドメイン）で Precedence 値を設定します。データは、precedence に従ってキューイングされます。重み付け均等化キューイング（WFQ）で、輻輳ポイントでの優先順位の高いトラフィックの処理を高速化できます。Weighted Random Early Detection（WRED; 重み付けランダム早期検出）により、輻輳時の優先順位の高いトラフィックの損失率を他のトラフィックより確実に小さくできます。

「from-field」パケットマーキング カテゴリの使用

このコマンドを、拡張パケット マーキング機能の一部として使用すると、DSCP 値のマッピングと設定に使用される「from-field」パケットマーキング カテゴリを指定できます。「from-field」パケットマーキング カテゴリは次のとおりです。

- サービス クラス（CoS）
- QoS group

「from-field」カテゴリを指定しても、**table** キーワードと適用可能な *table-map-name* 引数を指定していない場合、デフォルト アクションとは「from-field」カテゴリに関連付けられた値を DSCP 値としてコピーすることです。たとえば、**setdscpcos** コマンドを設定する場合、CoS 値がコピーされ、DSCP 値として使用されます。

（注） CoS フィールドは 3 ビット フィールドで、DSCP フィールドは 6 ビット フィールドです。**setdscpcos** コマンドを設定する場合、CoS フィールドの 3 ビットのみが使用されます。

setdscpqos-group コマンドを設定する場合、QoS グループ値がコピーされ、DSCP 値として使用されます。

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。このため、**setdscpqos-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。

- QoS グループの値が両方の値の範囲（たとえば、44）にある場合、packet-marking 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）、packet-marking 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。

IPv6 環境での DSCP 値の設定

このコマンドを IPv6 環境で使用すると、デフォルトで IPv4 パケットと IPv6 パケットの両方が照合されます。ただし、この機能によって設定される実際のパケットは、この機能を含むクラス マップの一致基準に合致するパケットのみです。

IPv6 パケットのみへの DSCP 値の設定

IPv6 値のみの DSCP 値を設定するには、**matchprotocolipv6** コマンドも使用する必要があります。このコマンドがない場合、precedence 一致では、デフォルトで、IPv4 パケットと IPv6 パケットの両方で一致が発生します。

IPv4 パケットのみへの DSCP 値の設定

IPv4 値のみの DSCP 値を設定するには、適切な **matchip** コマンドを使用する必要があります。このコマンドを使用しないと、他の一致基準に応じて、クラス マップが IPv6 パケットと IPv4 パケットの両方に合致し、DSCP 値が両方のタイプのパケットで機能することがあります。

例

パケットマーキング値とテーブル マップ

次の例では、「policy1」という名前のポリシー マップが、「table-map1」という名前のテーブル マップで定義されたパケットマーキング値を使用するために作成されます。テーブル マップは、**table-map** (value mapping) コマンドで前に作成されたものです。**table-map** (value mapping) コマンドの詳細については、**table-map** (value mapping) コマンド ページを参照してください。

この例では、「table-map1」という名前のテーブル マップで定義されている CoS の値に従って、DSCP の値が設定されます。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set dscp cos table table-map1
Router(config-pmap-c)#end
```

QoS ポリシーマップ コンフィギュレーション モードでサービス ポリシーを作成すると、**setdscp** コマンドが適用されます。このサービス ポリシーは、まだ、インターフェイスには付加されていません。インターフェイスへのサービス ポリシーの適用についての詳細は、『*Quality of Service Solutions Configuration Guide*』の「Modular Quality of Service Command-Line Interface」セクションを参照してください。

関連コマンド

コマンド	説明
matchipdscp	1 つまたは複数の DSCP 値、AF 値、および CS 値を一致基準として指定します。
matchprotocol	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。
policy-map	1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたはVCに、そのインターフェイスまたはVCのサービス ポリシーとして使用するポリシー マップを対応付けます。
setcos	発信パケットのレイヤ 2 CoS 値を設定します。
setprecedence	パケット ヘッダーに precedence 値を設定します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapclass	指定されたポリシー マップの指定されたクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。
showtable-map	指定されたテーブルマップまたはすべてのテーブルマップの設定を表示します。
table-map(valuemapping)	1 つの packet-marking 値を別の値にマッピングおよび変換するための、マッピング テーブルを作成します。

set fr-de

インターフェイスから出るすべてのトラフィックについて、フレーム リレー フレームのアドレス フィールドの廃棄適性（DE）ビットの設定を 1 に変更するには、ポリシーマップ クラス コマンドで **setfr-de** コマンドを使用します。DE ビット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。

set fr-de
no set fr-de

構文の説明

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

DE ビットは、通常、0 に設定されます。このコマンドにより、DE ビット設定が 1 に変更されます。

コマンド モード

ポリシー マップ クラス

コマンド履歴

リリース	変更箇所
12.2(2)T	このコマンドが導入されました。
12.2(31)SB2	このコマンドが Cisco IOS Release 12.2(31)SB2 に統合され、Cisco 10000 シリーズ ルータの PRE3 に実装されました。

使用上のガイドライン

トラフィック ポリシーでこのコマンドを無効にするには、このトラフィック ポリシーのポリシーマップ クラス コンフィギュレーション モードで、**nosetfr-de** コマンドを使用します。

DE ビットがすでに 1 に設定されている場合、フレームは変更されません。

例

次の例では、トラフィック ポリシーで **setfr-de** コマンドを使用して、DE ビットを設定します。ルータにより、ip-precedence クラスに属す発信パケットの DE ビットが設定されます。

```
Router(config)#
class-map ip-precedence
Router(config-cmap)#
match ip precedence 0 1
Router(config-cmap)#
exit
Router(config)#
policy-map set-de
Router(config-pmap)#
class ip-precedence
Router(config-pmap-c)#
set fr-de
Router(config-pmap-c)#
exit
Router(config-pmap)#
```

```
exit
Router(config)# interface serial 1/0/0
Router(config-if)# no ip address
Router(config-if)# encapsulation frame-relay
Router(config-if)#
interface serial 1/0/0.1
Router(config-subif)# ip address 10.1.1.1 255.255.255.252
Router(config-subif)# no ip directed-broadcast
Router(config-subif)#
service-policy output set-de
```

関連コマンド

コマンド	説明
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。

set ip dscp

setipdscp コマンドは set dscp コマンドによって置き換えられます。詳細については、set dscp コマンドを参照してください。

set ip dscp（ポリシー マップ コンフィギュレーション）

タイプ オブ サービス（ToS）バイトに IP Diffserv コード ポイント（DSCP）値を設定してパケットをマークするには、ポリシーマップ コンフィギュレーション モードで **setipdscp** コマンドを使用します。前に設定された IP DSCP の値を削除するには、このコマンドの **no** 形式を使用します。

set ip dscp *ip-dscp-value*
no set ip dscp *ip-dscp-value*

構文の説明

ip-dscp-value	IP DSCP の値。有効値の範囲は 0 ～ 63 です。詳細については、「使用上のガイドライン」を参照してください。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

ポリシー マップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。
15.1(2)SNH	このコマンドが、Cisco ASR 901 シリーズの集約サービス ルータに実装されました。

使用上のガイドライン

ip-dscp-value には数値ではなく、予約済みキーワード **EF**（完全優先転送）、**AF11**（相対的優先転送クラス AF11）、および **AF12**（相対的優先転送クラス AF12）を使用します。

IP DSCP ビットがオンに設定されると、他の Quality of Service（QoS）機能はビット設定で動作できます。

setipprecedence (policy-map configuration) コマンドを使用して IP プレシデンスでのパケットのマーキングができない場合は、**setipdscp** コマンドを使用して同じパケットを IP DSCP 値でマーキングします。

マーキングされたトラフィックには、ネットワークによってプライオリティ（または緊急処理のタイプ）が設定されます。通常は、ネットワーク エッジ（または管理ドメイン）で IP Precedence 値を設定します。データは、precedence に従ってキューイングされます。Weighted Fair Queueing（WFQ）は、輻輳ポイントで優先順位の高いトラフィックの処理を高速化できます。Weighted Random Early Detection（WRED）により、トラフィック輻輳時の優先順位の高いトラフィックの損失率を他のトラフィックより確実に小さくできます。

QoS ポリシーマップ コンフィギュレーション モードでサービス ポリシーを作成すると、**setipprecedence** (policy-map configuration) コマンドが適用されます。このサービス ポリシーは、インターフェイスにも、ATM 仮想回線にも、付加されていません。インターフェイスへのサービス ポリシーの適用については、**service-policy** コマンドを参照してください。

ポリシー マップ クラス アクションを設定する場合には、次の点に注意してください。

- ハードウェア スイッチド トラフィックの場合、ポリシー フィーチャ カード（PFC）QoS では、**bandwidth**、**priority**、**queue-limit**、または **random-detect** ポリシーマップ コマンドはサポートされません。これらのコマンドはソフトウェアでスイッチングされるトラフィックに使用できるので、設定が可能です。
- PFC QoS では、**setmpls** または **setqos-group** ポリシーマップ クラス コマンドはサポートされません。
- PFC QoS でサポートされるのは、**setipdscp** および **setipprecedence** ポリシーマップ クラス コマンドです（『*Cisco 7600 Series Router Cisco IOS Software Configuration Guide*』の「Configuring Policy Map Class Marking」セクションを参照）。
- ポリシー マップ クラスでは、次の 3 つのすべてを実行することはできません。
  - **setipdscp** または **setipprecedence** (policy-map configuration) コマンドを使用してトラフィックをマークする
  - 信頼状態の設定
  - ポリシングの設定

ポリシーマップ クラスで、**setipdscp** または **setipprecedence** (policy-map configuration) コマンドを使用してトラフィックをマークするか、次のいずれかまたは両方を実行します。

-
  - 信頼状態の設定
  - ポリシングの設定

例

次に、policy1 という名前のポリシー マップで IP DSCP ToS バイトを 8 に設定する例を示します。

```
Router(config)#
policy-map policy1
Router(config-cmap)#
class class1
Router(config-cmap)#
set ip dscp 8
```

一致基準の class1 を満たすすべてのパケットが、IP DSCP 値の 8 で設定されます。パケットが IP DSCP 値の 8 にマーク付けされる方法は、ネットワーク設定によって決定されます。

次に、ネットワーク エッジで音声パケットを示す設定の実行後、音声パケットに対する低遅延処理が提供されるよう、すべての中間ルータが設定される例を示します。

```
Router(config)# class-map voice
Router(config-cmap)# match ip dscp ef
Router(config)# policy qos-policy
Router(config-cmap)# class voice
Router(config-cmap)# priority 24
```

関連コマンド

コマンド	説明
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。
service-policy	ポリシー マップをインターフェイスに付加します。
showpolicy-map	ポリシー マップ情報を表示します。
showpolicy-mapinterface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

set ip dscp tunnel

トンネル マーキングのため、レイヤ 2 Tunnel Protocol Version 3（L2TPv3）または Generic Routing Encapsulation（GRE）トンネル型パケットのトンネル ヘッダーで、Differentiated Services Code Point（DSCP; DiffServ コード ポイント）の値を設定するには、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 **setipdscp tunnel** 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。

set ip dscp tunnel *dscp-value*
no set ip dscp tunnel *dscp-value*

構文の説明

dscp-value	トンネル ヘッダーの値を識別する 0 ～ 63 の数。次の予約キーワードは、数値の代わりに指定できます。 • **EF**（完全優先転送） • **AF11**（相対的優先転送クラス AF11）

コマンド デフォルト

DSCP の値は設定されていません。

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(28)S	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。
12.4(15)T2	このコマンドが Cisco IOS Release 12.4(15)T2 に統合され、GRE トンネル型パケットのマーキングに対するサポートが含められました。 （注） このリリースでは、GRE トンネル型パケットのマーキングは、Cisco MGX ルート プロセッサ モジュール（RPM-XF）に搭載されているプラットフォームでのみ、サポートされます。
12.2(33)SB	GRE トンネル型パケットのマーキングのサポートが含められ、Cisco 7300 シリーズ ルータのサポートが追加されました。
Cisco IOS XE リリース 3.5S	このコマンドが Cisco IOS XE Release 3.5S に統合され、Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

L2TPv3（または GRE）トンネル マーキングと **ip tos** コマンドは、同時に設定できます。ただし、モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）（L2TPv3 または GRE）トンネル マーキングの優先順位は **ip tos** コマンドの優先順位より高く、これは、トンネル マーキングによってトンネル パケットの IP ヘッダーに対して常に再書き込みが行われ、ip tos コマンドによって設定された値が上書きされることを意味します。これらのコマンドを同時に使用した場合の適用の順序は次のとおりです。

1. **setipdscptunnel** または **setipprecedencetunnel**（L2TPv3 または GRE トンネル マーキング）
2. **iptosreflect**
3. **iptos** *tos-value*

L2TPv3（または GRE）トンネル マーキングだけを設定し、 **ip tos** コマンドで設定されたすべてのピアを L2TPv3（または GRE）トンネル マーキングに再設定することを推奨します。

（注） Cisco IOS Release 12.4(15)T2 では、GRE トンネル型パケットのマーキングは、Cisco RPM-XF に搭載されているプラットフォームでのみ、サポートされます。

例

次の例では、トンネル マーキング コンフィギュレーションで **setipdscptunnel** コマンドを使用します。この例では、「class-cl」という名前のクラス マップが、DSCP 値設定に基づいてトラフィックを照合するように設定されています。また、「policy1」という名前のポリシー マップ（**setipdscptunnel** コマンドが設定済み）が作成されています。

```
Router> enable
Router# configure terminal
Router(config)# class-map class-c1
Router(config-cmap)# match ip dscp 0
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class tunnel
Router(config-pmap-c)# set ip dscp tunnel 5
Router(config-pmap-c)# end
```

（注） この場合も、ポリシー マップは、**service-policy** コマンドを使用してインターフェイスまたは ATM PVC に適用する必要があります。トンネル マーキング ポリシーは、サービス プロバイダー エッジ（SPE）ルータの入力物理インターフェイス上の入力ポリシーとして、または、トンネルインターフェイス上のイーグレス ポリシーとして適用できます。インターフェイスまたは ATM PVC へのポリシー マップの適用についての詳細は、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Applying QoS Features Using the MQC」モジュールを参照してください。

関連コマンド

コマンド	説明
iptos	IP トラフィックの ToS レベルを指定します。
setipprecedencetunnel	L2TPv3 または GRE トンネル型パケットのヘッダーで、precedence 値を設定します。

setipprecedence（ポリシーマップコンフィギュレーション）

IP ヘッダーでプレシデンス値を設定するには、ポリシーマップ コンフィギュレーション モードで **setippprecedence** コマンドを使用します。現在の設定のプレシデンス値を変更しない場合は、このコマンドの **no** 形式を使用します。

set ip precedence *ip-precedence-value*
no set ip precedence

構文の説明

ip-precedence-value	IP ヘッダーの precedence ビットの値。有効値の範囲は 0 ～ 7 です。次の表は、値の定義リストです。

コマンド デフォルト

このコマンドはデフォルトでは無効になっています。

コマンド モード

ポリシー マップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。
15.1(2)SNH	このコマンドが、Cisco ASR 901 シリーズの集約サービス ルータに実装されました。

使用上のガイドライン

次の表は、IP ヘッダーのプレシデンス値の値定義です。重要度のより小さいものから大きいものへの順序で表示します。

表 *43 : IP* プレシデンス値の定義

値	定義
	routine
	priority
	immediate
	flash
	flash-override

値	定義
	critical
	internet
	network

IP precedence ビットがオンに設定されると、Weighted Fair Queueing（WFQ）や Weighted Random Early Detection（WRED）などの他の Quality of Service（QoS）機能は、ビット設定で動作します。

ネットワーク プライオリティ（または緊急処理の一部のタイプ）により、ネットワークのダウンストリームのポイントで、WFQ と WRED の適用を介してトラフィックをマーク付けできます。通常は、ネットワーク エッジ（または管理ドメイン）で IP Precedence 値を設定します。データは、precedenceに従ってキューイングされます。WFQ は、輻輳ポイントで特定の優先トラフィックの処理を高速化できます。WRED により、トラフィック輻輳時の特定の優先トラフィックの損失率を他のトラフィックより確実に小さくできます。

ポリシーマップ コンフィギュレーション モードでサービス ポリシーを作成すると、**setipprecedence** コマンドが適用されます。このサービス ポリシーは、インターフェイスにも、ATM 仮想回線にも、付加されていません。インターフェイスへのサービス ポリシーの適用については、**service-policy** コマンドを参照してください。

例

次に、class1 という名前のクラス マップで一致基準を満たすパケットの IP precedence を 5 に設定する例を示します。

```
Router(config)#
policy-map policy1
Router(config-pmap)#
class class1
Router(config-pmap-c)#
set ip precedence 5
```

一致基準の class1 を満たすすべてのパケットが、IP DSCP 値の 5 で設定されます。パケットが IP-precedence 値の 5 にマーク付けされる方法は、ネットワーク設定によって決定されます。

関連コマンド

コマンド	説明
policy-map	QoS ポリシーマップを設定するための QoS ポリシーマップ コンフィギュレーション モードにアクセスします。
service-policy	ポリシー マップをインターフェイスに付加します。
showpolicy-map	ポリシー マップ情報を表示します。

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

set ip precedence（ポリシー マップ）

setipprecedence (policy-map) コマンドは、set precedence コマンドによって置き換えられます。詳細については、set precedence コマンドを参照してください。

set ip precedence（ルートマップ）

IP ヘッダーでプレシデンス値（およびオプションの IP 番号または IP 名）を設定するには、ルートマップ コンフィギュレーション モードで **setipprecedence** コマンドを使用します。プレシデンス値を変更しない場合は、このコマンドの **no** 形式を使用します。

set ip precedence [{*numbername*}]
no set ip precedence

構文の説明

number *name*	（任意）IP ヘッダーで precedence ビットを設定する番号または名前。*number* 引数と対応する *name* 引数の値は、重要度のより小さいものから大きいものへの順序で、次の表に示します。

コマンド デフォルト

無効

コマンド モード

ルート マップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
11.0	このコマンドが導入されました。
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。

使用上のガイドライン

次の表に、IP ヘッダーのプレシデンス値の *number* 引数と、対応する *name* 引数の値を示します。重要度のより小さいものから大きいものへの順序で表示します。

表 *44 : IP* プレシデンスの番号と名前

番号（Number）	名前（Name）
0	**routine**
1	**priority**
2	**immediate**
3	**flash**
4	**flash-override**
5	**critical**

番号（Number）	名前（Name）
6	**internet**
7	**network**

precedence は、番号または対応する名前を使用して設定できます。IP precedence ビットがオンに設定されると、Weighted Fair Queueing（WFQ）や Weighted Random Early Detection（WRED）などの他の Quality of Service（QoS）機能は、ビット設定で動作します。

ネットワークにより、プライオリティ（または緊急処理の一部のタイプ）が付与され、ネットワークのダウンストリームのポイントで、WFQ と WRED の適用を介してトラフィックがマーク付けされます。通常は、ネットワーク エッジ（または管理ドメイン）で IP Precedence 値を設定します。データは、precedence に従ってキューイングされます。WFQ は、輻輳ポイントで特定の優先トラフィックの処理を高速化できます。WRED により、輻輳時の特定の優先トラフィックの損失率を他のトラフィックより確実に小さくできます。

routine や **priority** などの引数からプレシデンス値へのマッピングは、一部のインスタンスだけに効力があります。つまり、precedence ビットの使用はまだ発展途上にあります。precedence 値の意味は、その値を使用する他の機能をイネーブルにすることで定義できます。シスコから使用可能なハイエンド インターネット QoS の場合、IP Precedence を使用すると、ネットワーク内の処理の良し悪しが数字的に対応する必要がないサービス クラスを確立できます。

route-map (IP) グローバル コンフィギュレーション コマンドを **match** および **set** ルートマップ コンフィギュレーション コマンドとともに使用して、ルーティング プロトコル間のルートの再配布またはポリシー ルーティングの条件を定義します。各 **route-map** コマンドには、**match** および **set** コマンドの関連リストがあります。**match** コマンドにより、現在の **route-map** コマンドで使用可能な再配分またはポリシー ルーティングでの、一致基準が指定されます。**set** コマンドによってセット アクションを指定します。**match** コマンドで適用する基準を満足する場合は、特定の再配布またはポリシー ルーティング アクションが実行されます。**noroute-map** コマンドでルート マップを削除します。

set ルートマップ コンフィギュレーション コマンドは、ルート マップのすべての一致基準が満たされたときに実行される再配布セット アクションを指定します。

例

次に、ルート マップ一致に渡されるパケットの IP Precedence を 5（critical）に設定する例を示します。

```
interface serial 0
 ip policy route-map texas
route-map texas
match length 68 128
set ip precedence 5
```

関連コマンド

Command	Description
fair-queue(WFQ)	インターフェイスに対する WFQ を有効にします。

Command	Description
ippolicyroute-map	インターフェイスでポリシー ルーティングに使用するルートマップを特定します。
random-detectdscp	DSCP 値の最小および最大パケットしきい値を変更します。
sendqdmmessage	CAR および DCAR ポリシーを設定します。
route-map(IP)	あるルーティング プロトコルから別のルーティング プロトコルへルートを再配布する条件を定義するか、ポリシー ルーティングをイネーブルにします。
traffic-shapeadaptive	BECN 信号の受信時に使用可能な帯域幅を推定するように、フレーム リレー サブインターフェイスを設定します。
traffic-shapefecn-adapt	FECN ビット（BECN ビットを設定した TEST RESPONSE メッセージで設定）が設定されたメッセージに返信します。
traffic-shapegroup	インターフェイス上でアウトバウンド トラフィック専用のアクセス リストに基づくトラフィック シェーピングをイネーブルにします。
traffic-shaperate	インターフェイスの発信トラフィックにトラフィック シェーピングを有効にします。

set ip precedence tunnel

トンネル マーキングのため、レイヤ 2 Tunnel Protocol Version 3（L2TPv3）または Generic Routing Encapsulation（GRE）トンネル型パケットのヘッダーで、プレシデンス値を設定するには、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 **setipprecedencetunnel** 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。

set ip precedence tunnel *precedence-value*
no set ip precedence tunnel *precedence-value*

構文の説明

precedence-value	トンネル ヘッダーの precedence 値を識別する 0 ～ 7 の数。

コマンド デフォルト

precedence の値は設定されていません。

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(28)S	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。
12.4(15)T2	このコマンドが Cisco IOS Release 12.4(15)T2 に統合され、GRE トンネル型パケットのマーキングに対するサポートが含められました。 （注） このリリースでは、GRE トンネル型パケットのマーキングは、Cisco MGX ルート プロセッサ モジュール（RPM-XF）に搭載されているプラットフォームでのみ、サポートされます。
12.2(33)SB	GRE トンネル型パケットのマーキングのサポートが含められ、Cisco 7300 シリーズ ルータのサポートが追加されました。
Cisco IOS XE リリース 3.5S	このコマンドが Cisco IOS XE Release 3.5S に統合され、Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

L2TPv3（または GRE）トンネル マーキングと **ip tos** コマンドは、同時に設定できます。ただし、モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）（L2TPv3 または GRE）トンネル マーキングの優先順位は **ip tos** コマンドの優先順位より高く、これは、トンネル マーキングによってトンネル パケットの IP ヘッダーに対して常に再書き込みが行われ、ip tos コマンドによって設定された値が上書きされることを意味します。これらのコマンドを同時に使用した場合の適用の順序は次のとおりです。

1. **setipdscptunnel** または **setipprecedencetunnel**（L2TPv3 または GRE トンネル マーキング）
2. **iptosreflect**
3. **iptos** *tos-value*

L2TPv3（または GRE）トンネル マーキングだけを設定し、 **ip tos** コマンドで設定されたすべてのピアを L2TPv3（または GRE）トンネル マーキングに再設定することを推奨します。

（注） Cisco IOS Release 12.4(15)T2 では、GRE トンネル型パケットのマーキングは、Cisco RPM-XF に搭載されているプラットフォームでのみ、サポートされます。

例

次の例では、トンネル マーキング コンフィギュレーションで **setipprecedencetunnel** コマンドを使用します。この例では、「MATCH_PREC」という名前のクラスマップが、プレシデンス値に基づいてトラフィックを照合するように設定されています。また、「TUNNEL_MARKING」という名前のポリシー マップ（**setipprecedencetunnel** コマンドが設定済み）が作成されています。

```
Router> enable
Router# configure terminal
Router(config)# class-map match-any MATCH_PREC
Router(config-cmap)# match ip precedence 0
Router(config-cmap)# exit
Router(config)# policy-map TUNNEL_MARKING
Router(config-pmap)# class MATCH_PREC
Router(config-pmap-c)# set ip precedence tunnel 3
Router(config-pmap-c)# end
```

（注） この場合でも、**service-policy** コマンドを使用して、インターフェイスまたはATM PVC にポリシーマップを適用する必要があります。トンネルマーキングポリシーは、サービス プロバイダー エッジ（SPE）ルータの入力物理インターフェイス上の入力ポリシーとして、または、トンネルインターフェイス上のイーグレスポリシーとして適用できます。インターフェイスまたは ATM PVC へのポリシー マップの適用についての詳細は、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Applying QoS Features Using the MQC」モジュールを参照してください。

関連コマンド

コマンド	説明
iptos	TN3270 サーバで、IP トラフィックの ToS レベルを指定します。
setipdscptunnel	L2TPv3 トンネル型パケットのヘッダーで、DSCP 値を設定します。

set ip tos（ルートマップ）

IP パケットのヘッダーでタイプ オブ サービス（ToS）ビットを設定するには、ルートマップ コンフィギュレーション モードで **setiptos** コマンドを使用します。ToS ビットを変更しない場合は、このコマンドの **no** 形式を使用します。

set ip tos [{*tos-bit-value*|**max-reliability**|**max-throughput**|**min-delay**|**min-monetary-cost**|**normal**}]
no set ip tos

構文の説明

tos-bit-value	（任意）IP ヘッダーで ToS ビットを設定する 0 ～ 15 の値（番号）。詳細については、次の表を参照してください。
max-reliability	（任意）最大信頼度の ToS ビットを 2 に設定します。
max-throughput	（任意）最大スループットの ToS ビットを 4 に設定します。
min-delay	（任意）最小遅延の ToS ビットを 8 に設定します。
min-monetary-cost	（任意）最小貨幣コストの ToS ビットを 1 に設定します。
normal	（任意）通常の ToS ビットを 0 に設定します。

コマンド デフォルト

無効

コマンド モード

ルート マップ コンフィギュレーション

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
12.4T	このコマンドが Cisco IOS Release 12.4T に統合されました。
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。

使用上のガイドライン

このコマンドを使用すると、ToS バイト ヘッダーの 4 つのビットを設定できます。次の表に、2 進数での 4 つのビットの形式を示します。

表 *45 : ToS* ビットと説明

T3	T2	T1	T0	説明
0	0	0	0	0 通常フォワーディング
0	0	0	1	1 最小貨幣コスト
0	0	1	0	2 最大信頼度
0	1	0	0	4 最大スループット
1	0	0	0	8 最小遅延

T3 ビットにより、遅延が設定されます。T3 を 0 に設定すると、通常遅延、1 に設定すると、低遅延になります。

T2 ビットにより、スループットが設定されます。このビット を 0 に設定すると、通常スループット、1 に設定すると、最小スループットになります。同様に、T1 ビットと T0 ビットにより、それぞれ、信頼度とコストが設定されます。したがって、たとえば、次の要件でパケットを設定するとします。

最小遅延 T3 = 1

通常スループット T2 = 0

通常信頼度 T1 = 0

最小貨幣コスト T0 = 1

この場合、ToS を 9 に設定します。これは、2 進数形式で 1001 になります。

route-map (IP) グローバル コンフィギュレーション コマンドを **match** および **set** (route-map) コンフィギュレーション コマンドとともに使用して、ルーティング プロトコル間のルートの再配布またはポリシー ルーティングの条件を定義します。各 **route-map** コマンドには、**match** および **set** コマンドの関連リストがあります。**match** コマンドにより、現在の route-map コマンドで使用可能な再配分またはポリシー ルーティングでの、一致基準が指定されます。**set** コマンドによってセット アクションを指定します。match コマンドで適用する基準を満足する場合は、特定の再配布またはポリシー ルーティング アクションが実行されます。**noroute-map** コマンドでルート マップを削除します。

set (route-map) コマンドは、ルート マップのすべての一致基準が満たされたときに実行される再配布セット アクションを指定します。

例

次に、ルートマップ照合に渡されるパケットの IP ToS ビットを 8 に設定する例を示します。

```
interface serial 0
 ip policy route-map texas
!
route-map texas
```

```
  match length 68 128
  set ip tos 8
!
```

関連コマンド

Command	Description
ippolicyroute-map	インターフェイスでポリシールーティングに使用するルートマップを特定します。
route-map(IP)	あるルーティングプロトコルから別のルーティングプロトコルへルートを再配布する条件を定義するか、ポリシー ルーティングをイネーブルにします。

set precedence

パケットヘッダーでプレシデンス値を設定するには、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 **setprecedence** コマンドを使用します。プレシデンス値を削除するには、このコマンドの **no** 形式を使用します。

Cisco 10000 シリーズ ルータ以外でサポートされるプラットフォーム
set precedence {*precedence-value*|*from-field* [**table** *table-map-name*]}
no set precedence {*precedence-value*|*from-field* [**table** *table-map-name*]}

Cisco 10000 シリーズ ルータ
set precedence {*precedence-value*}
no setprecedence {*precedence-value*}

構文の説明

precedence-value	パケット ヘッダーに precedence ビットを設定する 0 ～ 7 の数字です。
from-field	パケットの precedence 値の設定に使用される特定のパケットマーキング カテゴリです。パケットマーキング値のマッピングと変換のためにテーブルマップを使用している場合、この引数値がパケットマーキング カテゴリからマップを確立します。パケットマーキング カテゴリ キーワードは次のとおりです。 • **cos** • **qos-group**
table	（任意）指定のテーブル マップに設定された値が precedence 値の設定に使用されることを示します。
table-map-name	（任意）サービス クラス（CoS）値に基づいて precedence 値を指定するのに使用されるテーブル マップ名です。この名前には最大 64 文字までの英数字を指定できます。

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

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。**setipprecedence** コマンドは、このコマンドに置き換えられます。
12.0(28)S	このコマンドの IPv6 でのサポートが、Cisco 12000 シリーズ インターネット ルータに追加されました。
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。

リリース	変更箇所
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

コマンドの互換性

古いコンフィギュレーションを含むCisco IOS Release 12.2(13)Tからのイメージでルータをロードすると、**setipprecedence** コマンドはまだ認識されます。ただし、**setprecedence** コマンドが **setipprecedence** の代わりに使用されます。

setprecedence コマンドと **setdscp** コマンドを同時に使用して、同じパケットをマークすることはできません。Diffserv コード ポイント（DSCP）と precedence の 2 つの値は、相互に排他的です。パケットにはどちらか一方の値を設定でき、両方を設定することはできません。

ビット設定

precedence ビットがオンに設定されると、Weighted Fair Queueing（WFQ）や Weighted Random Early Detection（WRED）などの他の Quality of Service（QoS）機能は、ビット設定で動作します。

precedence 値

ネットワークにより、プライオリティ（または緊急処理の一部のタイプ）が付与され、ネットワークのダウンストリームのポイントで、WFQ と WRED の適用を介してトラフィックがマーク付けされます。通常は、ネットワーク エッジ（または管理ドメイン）で Precedence 値を設定します。データは、指定された precedence に従ってキューイングされます。WFQ は、輻輳ポイントで特定の優先トラフィックの処理を高速化できます。WREDにより、輻輳時の特定の優先トラフィックの損失率を他のトラフィックより確実に小さくできます。

拡張パケット マーキング機能でのこのコマンドの使用

このコマンドを、拡張パケット マーキング機能の一部として使用すると、プレシデンス値のマッピングと設定に使用されるパケット マーキング カテゴリ「from-field」を指定できます。「from-field」パケットマーキング カテゴリは次のとおりです。

- CoS
- QoS group

「from-field」カテゴリを指定しても、**table** キーワードと適用可能な *table-map-name* 引数を指定していない場合、デフォルト アクションは、「from-field」カテゴリに関連付けられた値をプレシデンス値としてコピーすることです。たとえば、**setprecedencecos** コマンドを設定する場合、CoS 値がコピーされ、プレシデンス値として使用されます。

QoS グループマーキング カテゴリに対して同じことを行うことができます。つまり、**setprecedenceqos-group** コマンドを設定できます。この場合、QoS グループ値がコピーされ、プレシデンス値として使用されます。

precedence の有効値の範囲は 0 ～ 7 の数字です。QoS グループの有効値の範囲は 0 ～ 99 です。このため、**setprecedenceqos-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。

- QoS グループの値が両方の値の範囲（たとえば、6）にある場合、packet-marking 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 precedence の範囲を超える場合（たとえば、10）、packet-marking 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。

IPv6 環境での precedence 値

このコマンドを IPv6 環境で使用する場合、IPv4 および IPv6 パケットの両方に値を設定できます。ただし、この機能によって設定される実際のパケットは、この機能を含むクラスマップの一致基準に合致するパケットのみです。

IPv6 パケットのみに対する precedence 値の設定

IPv6 パケットのみにプレシデンス値を設定するには、このアクションにパケットを分類しているクラス マップで **matchprotocolipv6** コマンドも使用する必要があります。**matchprotocolipv6** コマンドを使用しないと、他の一致基準に応じて、クラス マップが IPv6 パケットと IPv4 パケットの両方を分類し、**setprecedence** コマンドが両方のタイプのパケットで機能します。

IPv4 パケットのみに対する precedence 値の設定

IPv4 パケットのみにプレシデンス値を設定するには、**matchipprecedence** や **matchipdscp** コマンドのように、**ip** キーワードを指定したコマンドを使用するか、クラス マップ内に他のコマンドとともに **matchprotocolip** コマンドを追加します。**ip** キーワードを追加しない場合は、他の一致基準に応じて、クラス マップが IPv6 パケットと IPv4 パケットの両方を照合し、**setprecedence** または **setdscp** コマンドが両方のタイプのパケットで機能します。

例

次の例では、policy-cos というポリシー マップが、table-map1 というテーブル マップで定義された値を使用するために作成されます。「table-map1」テーブル マップは、**table-map** (value mapping) コマンドで前に作成されたものです。**table-map** (value mapping) コマンドの詳細については、**table-map** (value mapping) コマンド ページを参照してください。

この例では、table-map1 に定義されている CoS の値に従って、precedence の値が設定されます。

```
Router(config)# policy-map policy-cos
Router(config-pmap)# class class-default
Router(config-pmap-c)# set precedence cos table table-map1
Router(config-pmap-c)# end
```

QoS ポリシーマップ コンフィギュレーション モードでサービス ポリシーを作成すると、**setprecedence** コマンドが適用されます。このサービス ポリシーは、インターフェイスにも、ATM 仮想回線にも、付加されていません。インターフェイスへのサービス ポリシーの適用については、『*Quality of Service Solutions Configuration Guide*』の「Modular Quality of Service Command-Line Interface Overview」の章を参照してください。

関連コマンド

Command	Description
matchdscp	特定の IP DSCP 値を一致基準として識別します。
matchprecedence	IP precedence 値を一致基準として識別します。
matchprotocol	指定されたプロトコルに基づいて、クラスマップの一致基準を設定します。
policy-map	1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたはVCに、そのインターフェイスまたはVCのサービス ポリシーとして使用するポリシー マップを対応付けます。
setcos	発信パケットのレイヤ 2 CoS 値を設定します。
setdscp	ToS バイトにレイヤ 3 DSCP 値を設定することにより、パケットにマーク付けします。
setqos-group	後からパケットの分類に使用できるグループ ID を設定します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。
showtable-map	指定されたテーブルマップまたはすべてのテーブルマップの設定を表示します。
table-map(valuemapping)	1 つの packet-marking 値を別の値にマッピングおよび変換するための、マッピング テーブルを作成します。

set qos-group

あとでパケットの分類に使用できるサービス品質（QoS）グループ識別子（ID）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 **set qos-group** コマンドを使用します。グループ ID を削除するには、このコマンドの **no** 形式を使用します。

Cisco 10000 シリーズ ルータ以外でサポートされるプラットフォーム
set qos-group {*group-id*|*from-field* [**table** *table-map-name*]}
no set qos-group {*group-id*|*from-field* [**table** *table-map-name*]}

Cisco 10000 シリーズ ルータ
set qos-group *group-id*
no set qos-group *group-id*

構文の説明

group-id	グループ ID 番号の範囲は 0 ～ 99 です。
from-field	パケットの QoS グループ値を設定するために使用される、特定の packet-marking のカテゴリ。パケットマーキング値のマッピングと変換のためにテーブルマップを使用している場合、これが「map from」パケットマーキング カテゴリを確立します。パケットマーキング カテゴリ キーワードは次のとおりです。 • **cos**：QoS グループ値が、パケットのオリジナル 802.1P サービス クラス（CoS）フィールドから設定されることを指定します。 • **precedence**：QoS グループ値が、パケットのオリジナル IP プレシデンス フィールドから設定されることを指定します。 • **dscp**：QoS グループ値が、パケットのオリジナル Diffserv コードポイント（DSCP）フィールドから設定されることを指定します。 • **mplsexptopmost**：QoS グループ値が、パケットのオリジナル最上位 MPLS EXP フィールドから設定されることを指定します。
table *table-map-name*	（任意）*from-field* 引数との組み合わせで使用されます。*table-map-name* によって指定されたテーブル マップに設定されている値が、QoS グループ値の設定に使用されることを示します。

コマンド デフォルト

グループ ID は指定されていません。

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。

リリース	変更箇所
12.0(17)SL	このコマンドが Cisco 10000 シリーズ ルータに追加されました。
12.2(13)T	このコマンドは、**random-detect discard-class-based** コマンドとともに使用でき、拡張パケットマーキング機能に合わせて変更されました。マッピングテーブル（テーブルマップ）を使用して、packet-marking の値を変換し、送信できます。
12.2(18)SXE	このコマンドが Cisco IOS 12.2(18)SXE に統合され、**cos** キーワードが追加されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。
15.1(2)SNH	このコマンドが、Cisco ASR 901 シリーズの集約サービス ルータに実装されました。
15.2(2)E	このコマンドが変更されました。

使用上のガイドライン

set qos-group コマンドでは、グループ ID をパケットと関連付けできます。後でグループ ID を使用して、プレフィックス、自律システム、コミュニティ ストリングに基づいて、パケットを QoS グループに分類できます。

QoS グループと廃棄クラスは、入力 Per-Hop Behavior マーキング（PHB）を使用して出力インターフェイスのパケットが分類される場合に必要です。

拡張パケット マーキング機能でのこのコマンドの使用

このコマンドを、拡張パケット マーキング機能の一部として使用すると、プレシデンス値のマッピングと設定に使用されるパケット マーキング カテゴリ「from-field」を指定できます。

「from-field」カテゴリを指定しても、**table** キーワードと適用可能な *table-map-name* 引数を指定していない場合、デフォルト アクションは、「from-field」カテゴリに関連付けられた値をプレシデンス値としてコピーすることです。たとえば、**set qos-grouppprecedence** を入力すると、プレシデンス 値がコピーされ、QoS グループ値として使用されます。

パケットは、ルータ内で処理中の間だけ、QoS グループ値でマーク付けされます。パケットが出力インターフェイスを介して送信されるとき、QoS グループ値はパケットのヘッダーに含まれません。ただし、QoS グループ値を使用すると、パケットのヘッダーに含まれるレイヤ 2 またはレイヤ 3 フィールド（MPLS EXP、CoS、DSCP フィールドなど）の値を設定できます。

（注） **set qos-group cos** および **set qos-group precedence** コマンドは、**mls qos trust cos** および **mls qos trust prec** コマンドと同等です。

ヒント　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 ポリシーを適用するまでは、**set qos-group** コマンドを適用できません。サービス ポリシーの適用については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Modular Quality of Service Command-Line Interface Overview」の章を参照してください。

例

次に、class1 という名前のクラス マップの一致基準を満たすすべてのパケットの QoS を 1 に設定する例を示します。これらのパケットは、QoS グループ ID に基づいてレートが制限されます。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set qos-group 1
Router(config-pmap-c)# end
```

次に、パケットのオリジナル 802.1P CoS 値に基づいて、QoS グループ値を設定する例を示します。

```
Router(config)# policy map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set qos-group cos
Router(config-pmap-c)# end
```

拡張パケット マーキングの例

次に、table-map1 という名前のテーブルマップで定義される値に基づいて、QoS グループ値を設定する例を示します。このテーブルマップは、policy1 という名前のポリシーマップで設定されます。ポリシー マップ policy1 により、table-map1 に定義されている値に従って QoS 値が変換され、送信されます。

この例では、table-map1 に定義されている precedence の値に従って、QoS グループの値が設定されます。

```
Router(config)# policy map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set qos-group precedence table table-map1
Router(config-pmap-c)# end
```

関連コマンド

コマンド	説明
matchinputvlan	特定の VLAN ID を持つ着信パケットに一致するクラス マップを設定します。
matchqos-group	一致基準として特定の QoS グループ値を指定します。

コマンド	説明
mlsqostrust	保存する必要があるパケットの着信QoSフィールドを決めるために、インターフェイスの信頼状態を設定します。
policy-map	1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
service-policy	入力インターフェイスまたはVC、あるいは出力インターフェイスまたはVCに、そのインターフェイスまたはVCのサービス ポリシーとして使用するポリシー マップを対応付けます。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定のPVCに対するサービス ポリシーのクラスを表示します。

set vlan inner

相手先固定接続（PVC）のブリッジされたパケットを特定の仮想 LAN 識別子（VLAN ID）でマークするには、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 **setvlaninner** 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。

set vlan inner *vlan-number*
no set vlan inner *vlan-number*

構文の説明

vlan-number	VLAN を識別する番号。範囲は 1 ～ 4094 です。

コマンド デフォルト

bridge-dot1qencap コマンドによる設定に基づいて、ブリッジされたパケットはデフォルトの VLAN ID でマークされます。

コマンド モード

ポリシーマップ クラス コンフィギュレーション モード（config-pmap-c）

コマンド履歴

リリース	変更箇所
15.1(2)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

複数の VLAN は単一 PVC で使用できますが、Address Resolution Protocol（ARP）パケットなど、ローカルで生成されたパケットは、クラスのデフォルト VLAN ID のみで送信されます。**setvlaninner** コマンドは、クラスのデフォルト内で適用する必要があります。

例

次の例では、802.1Q タグのブリッジされたパケットについて、内部 VLAN ID を 2 にマークします。

```
Router(config)# policy-map egress-policy
Router(config-pmap)# class egress
Router(config-pmap-c)# set vlan inner 2
```

関連コマンド

コマンド	説明
bridge-dot1qencap	ATM xDSL リンク経由の ATM PVC に VLAN ID を追加します。

shape

平均レート トラフィック シェーピングまたはピーク レート トラフィック シェーピングを指定するには、クラスマップ コンフィギュレーション モードで **shape** コマンドを使用します。トラフィック シェーピングを削除するには、このコマンドの **no** 形式を使用します。

shape {**average**|**peak**} *cir* [*bc*] [*be*]
no shape {**average**|**peak**} *cir* [*bc*] [*be*]

構文の説明

average	平均レート シェーピングを指定します。
peak	ピーク レート シェーピングを指定します。
cir	認定情報レート（CIR）（1秒あたりのビット数（bps））。
bc	（任意）認定バースト サイズ（バイト）。
be	（任意）超過バースト サイズ（バイト）。

コマンド デフォルト

平均またはピークのトラフィック シェーピングは指定されません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
12.1(2)T	このコマンドが導入されました。
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(1)T	このコマンドが変更されました。cir 引数に使用できる値が変更されました。値は 8,000 ～ 1,000,000,000 bps である必要があります。

使用上のガイドライン

トラフィック シェーピングは、データの転送レートを制限します。特に設定された送信レートに加え、ジェネリック トラフィック シェーピング（GTS）を使用して、輻輳レベルに基づいた派生送信レートを指定できます。

平均レート シェーピングとピーク レート シェーピングの、2つのタイプのトラフィック シェーピングを指定できます。平均レート シェーピングの送信レートは、CIR に制限されます。CIR を使用すると、送信中のトラフィックの平均量が、ネットワークで想定されているレートに準拠します。

ピーク レート シェーピングでは、CIR を超えるトラフィックを送信するようルータを設定します。ピーク レートを決める場合、ルータでは、次の式が使用されます。

peak rate = CIR(1 + Be / Bc)

引数の説明

- Be は超過バースト サイズです。
- Bc は認定バースト サイズです。

ピーク レート シェーピングを使用すると、平均レート シェーピングより大きいバーストがルータで許可されます。ただし、ピーク レート シェーピングを使用すると、ネットワークが輻輳状態の場合、CIR（デルタ値）を超えて送信されるトラフィックはドロップされる場合があります。

ネットワークで（準備されている CIR を超える）追加帯域幅が使用可能な場合、アプリケーションまたはクラスでは、まれに、パケットの損失が発生することがあり、この場合、余分な帯域幅をピーク レート シェーピングを使用して利用できます。しかし、ネットワーク輻輳が発生した場合には、しばしばパケットがドロップされます。ネットワークに送信されるトラフィックは、プロビジョニングされたネットワーク CIR に厳密に従わなければなりません。

例

次に、256 kbps の帯域幅を保証する平均レート シェーピングの設定例を示します。

```
shape average 256000
```

次に、ピーク レート シェーピングを設定して 300 kbps の帯域幅を保証する一方で、インターフェイスで十分な帯域幅が利用できる場合に最大 512 kbps のスループットを許可する例を示します。

```
bandwidth 300
shape peak 512000
```

関連コマンド

コマンド	説明
bandwidth	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
shapemax-buffers	シェーピング キューに認められるバッファの最大数を指定します。

shape (percent)

インターフェイスで使用可能な帯域幅のパーセンテージに基づいて、平均レート トラフィック シェーピングまたはピーク レート トラフィック シェーピングを指定するには、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 **shape** コマンドを使用します。トラフィック シェーピングを削除するには、このコマンドの **no** 形式を使用します。

shape {**average**|**peak**} **percent** *percentage* [*sustained-burst-in-msec* **ms**] [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**]
no shape {**average**|**peak**} **percent** *percentage* [*sustained-burst-in-msec* **ms**] [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**]

構文の説明

average	平均レート トラフィック シェーピングを指定します。
peak	ピーク レート トラフィック シェーピングを指定します。
percent	平均レート トラフィック シェーピングまたはピーク レート トラフィック シェーピングのいずれかで使用される帯域幅の割合を指定します。
percentage	帯域幅の割合（%）を指定します。有効値の範囲は 1 ～ 100 です。
sustained-burst-in-msec	（任意）ポリシング トラフィックの最初のトークン バケットによって使用される平均バースト サイズ。有効値の範囲は 4 ～ 200 です。
ms	（任意）バーストの値がミリ秒（ms）単位で指定されていることを示します。
be	（任意）ポリシング トラフィックの 2 番目のトークン バケットによって使用される超過バースト（be）サイズ。
excess-burst-in-msec	（任意）be サイズをミリ秒単位で指定します。有効値の範囲は 0 ～ 200 です。
bc	（任意）ポリシング トラフィックの最初のトークン バケットによって使用される認定バースト（bc）サイズ。
committed-burst-in-msec	（任意）bc 値をミリ秒単位で指定します。有効な範囲は 1 ～ 2000 の数字です。

コマンド デフォルト

bc と be のデフォルト値は 4 ms です。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.1(2)T	このコマンドが導入されました。

リリース	変更箇所
12.2(13)T	このコマンドは、パーセントベース ポリシング機能とシェーピング機能のために、変更されました。
12.0(28)S	このコマンドが Cisco IOS Release 12.0(28)S に統合されました。
12.2(18)SXE	このコマンドが Cisco IOS Release 12.2(18)SXE に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

認定情報レート

このコマンドは、インターフェイスの利用可能な帯域幅に基づいて認定情報レート（CIR）を計算します。ポリシーマップがインターフェイスに付加されている場合、ビット/秒（bps）単位での同等のCIRの値が、インターフェイスの帯域幅と、このコマンドで入力された割合（%）の値で計算されます。これにより、**showpolicy-mapinterface** コマンドを使用して、計算された CIR bps 値を確認できます。

計算された CIR bps レートは、8000 ～ 154,400,000 bps の範囲にある必要があります。レートが 8000 bps を下回る場合は、対応するポリシーマップはインターフェイスに適用できません。インターフェイス帯域幅が変化した（たとえば、さらに追加されるなど）場合、CIR bps 値は集成された帯域幅の値に基づいて再計算されます。ポリシーマップがインターフェイスに付加された後に CIR 割合が変更された場合は、CIR bps 値が再計算されます。

ミリ秒単位での適合バースト サイズと最大バースト サイズ

また、このコマンドでは、適合バースト サイズとピーク バースト サイズの値をミリ秒単位で指定することもできます。帯域幅を割合として計算する場合は、適合バーストサイズとピークバースト サイズをミリ秒単位で指定する必要があります。

トラフィック シェーピング収束率は、トラフィック パターンおよびタイム スライス（Tc）パラメータによって異なり、設定された bc から直接影響を受けます。設定された Tc および平均レートは、持続間隔あたりのビット数の計算に使用されます。したがって、シェープ レートの実施を確実にするために、Tc を 10 ms より大きくする bc を使用します。

階層型ポリシー マップ

shape (percent) コマンドを「子」（階層型）ポリシー マップで使用することは、Cisco 7500、Cisco 7200、およびそれより下位のシリーズ ルータではサポートされません。したがって、これらのルータでは、階層型ポリシー マップで使用するように **shape** (percent) コマンドを設定することはできません。

帯域幅を計算するには

shape (percent) コマンドは、しばしば **bandwidth** コマンドと **priority** コマンドとの組み合わせで使用されます。**bandwidth** コマンドと **priority** コマンドを使用すると、エンティティ（たと

えば、物理インターフェイスなど）で使用可能な帯域幅の合計量を計算できます。**bandwidth** コマンドと **priority** コマンドを使用して、エンティティで使用可能な帯域幅の合計量を計算する場合は、次の注意事項に従ってください。

- エンティティが物理インターフェイスの場合、合計帯域幅は、物理インターフェイス上の帯域幅です。
- エンティティが整形 ATM 相手先固定接続（PVC）の場合、合計帯域幅は、次のように計算されます。
  - 可変ビット レート（VBR）の仮想回線（VC）の場合、計算には、平均セル レート（SCR）が使用されます。
  - 使用可能ビット レート（ABR）の VC の場合、計算には、最小セル レート（MCR）が使用されます。

帯域割り当ての詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Congestion Management Overview」の章を参照してください。

（注） このコマンドと **shapeadaptive** コマンドは同時には使用できません。

例

次に、帯域幅の割合に基づいた平均シェーピング レートを使用するトラフィック シェーピングの設定例を示します。この例では、帯域幅の 25% が指定されています。さらに、オプションの be 値と bc 値（それぞれ、100 ms と 400 ms）が指定されています。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# shape average percent 25 20 ms be 100 ms bc 400 ms
Router(config-pmap-c)# end
```

ポリシー マップとクラス マップの設定後、ポリシー マップは次の例に示すように、インターフェイスにアタッチされます。

```
Router> enable
Router# configure terminal
Router(config)#

interface serial4/0
Router(config-if)#

service-policy input policy1
Router(config-if)# end
```

関連コマンド

コマンド	説明
bandwidth	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。

コマンド	説明
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
police(percent)	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
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与えます。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
shape adaptive	フレーム リレー インターフェイスまたはポイントツーポイント サブインターフェイスでトラフィック シェーピングが有効な場合、逆方向明示的輻輳通知（BECN）統合で使用可能な帯域幅を推定します。
shapemax-buffers	シェーピング キューに認められるバッファの最大数を指定します。
showpolicy-mapinterface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

shape（policy-map クラス）

指定されたアルゴリズムに従ってトラフィックを指示されたビット レートにシェーピングする、または、ATM オーバーヘッド アカウンティングを有効にするには、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 **shape** コマンドを使用します。シェーピングを削除し、トラフィックをシェーピングしない場合は、このコマンドの **no** 形式を使用します。

shape {**average**|**peak**} {*mean-rate* [*burst-size* [*excess-burst-size*]]|**percent** *percentage* [*burst-size* **ms** [*excess-burst-size* **ms**]]}
no shape [{**average**|**peak**}]
shape [{**average**|**peak**}] *mean-rate* **[burst-size]** [*excess-burst-size*] **account** {**qinq**|**dot1q**} **aal5** {*subscriber-encapsulation*|**user-defined** *offset*}
no shape [{**average**|**peak**}] *mean-rate* **[burst-size]** [*excess-burst-size*] **account** {**qinq**|**dot1q**} **aal5** {*subscriber-encapsulation*|**user-defined** *offset*}
shape [{**average**|**peak**}] *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq**|**dot1q**} **aal5** *subscriber-encap*]
no shape [{**average**|**peak**}] *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq**|**dot1q**} **aal5** *subscriber-encap*]
shape [average] *mean-rate* [*unit*] [*burst-size*] [*excess-burst-size*] [**account** {**qinq**|**dot1q**} **aal5** *subscriber-encapsulation*]
no shape [average] *mean-rate* [*unit*] [*burst-size*] [*excess-burst-size*] [**account** {**qinq**|**dot1q**} **aal5** *subscriber-encapsulation*]
shape [average] *mean-rate* [*burst-size*] [*excess-burst-size*] **account** {{**qinq**|**dot1q**} {**aal5**|**aal3**} *subscriber-encapsulation*|**user-defined** *offset* **[atm]**}
no shape [average] *mean-rate* [*burst-size*] [*excess-burst-size*] **account** {{**qinq**|**dot1q**} {**aal5**|**aal3**} *subscriber-encapsulation*|**user-defined** *offset* **[atm]**}

構文の説明

average	認定バースト（Bc）は、各間隔で送信される最大ビット数です。
peak	Bc + 超過バースト（Be）は、各間隔で送信される最大ビット数です。
mean-rate	認定情報レート（CIR）とも呼ばれます。トラフィックのシェーピングに使用されるビット レートを bps で指定します。このコマンドが、逆方向明示的輻輳通知（BECN）近似値とともに使用される場合、ビット レートは許可されるビット レート範囲の上限です。値は 1,000 ～ 1,000,000,000 bps の範囲です。
unit	（任意）指定されたビット レートの単位（kbps など）を指定します。
burst-size	（任意）測定間隔のビット数（Bc）。有効な値は 256 ～ 154400000 です。
excess-burst-size	（任意）Be を超えることが認められる許容ビット数。有効な値は 0 ～ 154400000 です。
percent	認定情報レートのインターフェイス帯域幅をパーセンテージで指定します。
percentage	パーセンテージ。有効な値は 1 ～ 100 です。
burst-size	（任意）ミリ秒単位の平均バースト。有効な値は 10 ～ 2000 です。

ms	（任意）時間をミリ秒単位で指定します。
excess-burst-size	（任意）ミリ秒単位の超過バースト。有効な値は 10 ～ 2000 です。
ms	（任意）時間をミリ秒単位で指定します。
account	（オプション）ATM オーバーヘッド アカウンティングを有効にします。 （注） ATM オーバーヘッド アカウンティングを設定する場合、このキーワードが必要です。
qinq	ATM オーバーヘッド アカウンティングのデジタル加入者線アクセス マルチプレクサ（DSLAM）のカプセル化タイプに対して、キューインキュー（qinq）のカプセル化をブロードバンド アグリゲーション システム（BRAS）として指定します。
dot1q	ATM オーバーヘッド アカウンティングの BRAS-DSLAM カプセル化タイプとして IEEE 802.1Q VLAN カプセル化を指定します。
aal5	ATM オーバーヘッド アカウンティングに ATM アダプテーション層 5 サービスを指定します。AAL5 は、コネクション型の可変ビット レート（VBR）サービスをサポートします。
aal3	コネクションレス型リンクとコネクション型リンクの両方をサポートする ATM アダプテーション層 5 を指定します。aal3 または aal5 のいずれかを指定する必要があります。 （注） Cisco 7300 および Cisco 7600 シリーズ ルータの場合、**aa13** キーワードはサポートされません。
subscriber-encap	加入者線でのカプセル化タイプを指定します。 • **snap-rbe** • **mux-rbe** • **snap-dot1q-rbe** • **mux-dot1q-rbe** • **snap-pppoa** • **mux-pppoa** • **snap-1483routed** • **mux-1483routed**
user-defined	ルータが ATM オーバーヘッドを計算する際にオフセット サイズを使用するように指定します。

offset	ATM オーバーヘッドを計算する際のオフセット サイズを指定します。有効な値は -127 ～ 127 バイトです。0 は有効な値ではありません。 （注） Cisco 7300 および Cisco 7600 シリーズ ルータの場合、有効な値は -48 ～ 48 バイトです。0 は有効な値ではありません。 （注） user-defined offset オプションを指定しない場合、ルータがオフセット サイズを設定します。
atm	ATM オーバーヘッドの計算に ATM セル タックスを適用します。 （注） Cisco 7300 および Cisco 7600 シリーズ ルータの場合、**atm** キーワードはサポートされません。 （注） offset オプションと atm オプションの両方を設定すると、オフセット サイズに対するパケット サイズの調整が行われてから、ATM セル タックスが追加されます。

コマンド デフォルト

超過バースト サイズ（Be）が設定されていない場合、デフォルトの Be の値は、認定バースト サイズ（Bc）と等しくなります。バースト サイズのデフォルトの詳細については、「使用上のガイドライン」セクションを参照してください。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングは、ディセーブルです。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.0(17)SL	このコマンドが Cisco IOS Release 12.0(17)SL に統合され、Cisco 10000 シリーズ ルータの PRE1 に実装されました。
12.2(16)BX	このコマンドが Cisco IOS Release 12.2(16)BX に統合され、Cisco 10000 シリーズ ルータの PRE2 に実装されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(31)SB2	このコマンドは、ATM オーバーヘッド アカウンティングに対応して機能拡張され、Cisco 10000 シリーズ ルータ PRE3 に実装されました。
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。

リリース	変更箇所
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。
12.2(31)SB6	このコマンドが ATM オーバーヘッドを計算する際のオフセット サイズを指定するように機能強化され、PRE3 向け Cisco 10000 シリーズ ルータに実装されました。
12.2(33)SRC	このコマンドが変更されました。Cisco 7600 シリーズ ルータのサポートが追加されました。
12.2(33)SB	このコマンドが変更されました。Cisco 7300 シリーズ ルータのサポートが追加されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。
15.2(1)T	このコマンドが変更されました。offset 引数に使用できる値が変更されました。値は -127 ～ 127 バイトにする必要があり、0 は有効な値ではありません。mean-rate 引数に使用できる値が変更されました。値は 1,000 ～ 1,000,000,000 bps の範囲です。

使用上のガイドライン

測定間隔は、認定バーストサイズ（Bc）を認定情報レート（CIR）で割ったものです。Bc は、0 に設定できません。測定間隔が大きすぎる場合（128 ミリ秒を超える場合）、システムは測定間隔をさらに短い間隔に再分割します。

認定バースト サイズ（Bc）および超過バースト サイズ（Be）を指定しない場合は、アルゴリズムによってシェープ エンティティのデフォルト値が決定されます。アルゴリズムは、4 ミリ秒の測定間隔を使用します。したがって、Bc は CIR ×（4/1000）です。

デフォルトの認定バースト サイズを超えるバースト サイズは明示的に指定する必要があります。Bc が大きくなるほど、測定間隔が長くなります。長い測定間隔は、音声トラフィックの遅延に影響する可能性があります（該当する場合）。

超過バースト サイズ（Be）が設定されていない場合、デフォルト値は、認定バースト サイズ（Bc）と等しくなります。

Cisco 10000 シリーズ パフォーマンス ルーティング エンジンにおけるトラフィック シェーピング

Cisco 10000 シリーズ ルータでは、peak キーワードはサポートされません。

PRE2 では、シェープ レートとレートの単位を指定します。レートの有効な値は、1～2488320000 で、単位は bps、kbps、mbps、gbps です。デフォルトの単位は kbps です。次に例を示します。

```
shape 128000 bps
```

PRE3 では、シェープ レートのみ指定します。PRE3 の単位は常に bps で、unit 引数は使用できません。シェープ レートの有効な値は 1000 ～ 2488320000 です。

```
shape 1000
```

PRE3 でも PRE2 の shape コマンドを隠しコマンドとして使用できます。ただし、PRE3 は、PRE3 の有効なシェープ レートの範囲（1000 ～ 2488320000）外が指定された場合、PRE2 の shape コマンドを拒否します。

ATM（Cisco 7300 シリーズ ルータ、Cisco 7600 シリーズ ルータ、および Cisco 10000 シリーズ ルータ）のトラフィック シェーピング オーバーヘッド アカウンティング

Cisco 7300 シリーズ ルータ、Cisco 7600 シリーズ ルータ、または Cisco 10000 シリーズ ルータで ATM オーバーヘッド アカウンティングを設定する場合、BRAS-DSLAM、DSLAM-CPE、および加入者線のカプセル化タイプを指定する必要があります。ルータは、次の加入者線カプセル化タイプをサポートします。

- **snap-rbe**
- **mux-rbe**
- **snap-dot1q-rbe**
- **mux-dot1q-rbe**
- **snap-pppoa**
- **mux-pppoa**
- **snap-1483routed**
- **mux-1483routed**

階層型ポリシーでは、次の方法で ATM オーバーヘッド アカウンティングを設定します。

- 親で有効：親ポリシー上の ATM オーバーヘッド アカウンティングを有効にした場合は、子ポリシー上のアカウンティングを有効にする必要はありません。
- 子および親で有効：子ポリシー上の ATM オーバーヘッド アカウンティングを有効にした場合は、親ポリシー上の ATM オーバーヘッド アカウンティングも有効にする必要があります。

カプセル化タイプは、子および親ポリシーと一致する必要があります。

ユーザ定義のオフセット値は、子および親ポリシーと一致する必要があります。

例

次に、CIR が 1 Mbps であるシェープ エンティティを設定し、インターフェイス pos1/0/0 に dts-interface-all-action というポリシー マップを付加する例を示します。

```
policy-map dts-interface-all-action
 class class-interface-all
  shape average 1000000
interface pos1/0/0
 service-policy output dts-interface-all-action
```

ATM のトラフィック シェーピング オーバーヘッド アカウンティング

親ポリシーで ATM オーバーヘッド アカウンティングがシェーピングに対して有効である場合、子レベルで police コマンドを使用してアカウンティングを有効にする必要はありません。次に、subscriber_classes という名前の子ポリシー マップの gaming クラスと class-default クラス、および、subscriber_line という名前の親ポリシー マップの class-default クラスで ATM オーバーヘッド アカウンティングが帯域幅に対してイネーブルである設定例を示します。voip クラスおよび video クラスは、ATM オーバーヘッド アカウンティングが明示的にイネーブルにされていません。これらのプライオリティ クラスは、親ポリシーで ATM オーバーヘッド アカウンティングがイネーブルにされているため、ATM オーバーヘッドアカウンティングは暗黙的にイネーブルです。親ポリシーと子ポリシーの機能で同じカプセル化タイプが使用されていることに注意してください。

```
policy-map subscriber_classes
 class voip
  priority level 1
  police 8000
 class video
  priority level 2
  police 20000
 class gaming
  bandwidth remaining percent 80 account dot1q aal5 snap-dot1q-rbe
 class class-default
  bandwidth remaining percent 20 account dot1q aal5 snap-dot1q-rbe
policy-map subscriber_line
 class class-default
  shape average 8000 account dot1q aal5 snap-dot1q-rbe
  service policy subscriber_classes
```

次の例では、ルータで ATM オーバーヘッドの計算にオーバーヘッド 20 バイトと ATM セル タックスを使用します。

```
policy-map child
 class class1
  bandwidth 500 account user-defined 20 atm
 class class2
  shape average 30000 account user-defined 20 atm
```

関連コマンド

コマンド	説明
bandwidth	ポリシー マップに属するクラスに対して割り当てられる帯域幅を指定、または変更し、ATM オーバーヘッドアカウンティングをイネーブルにします。
shapeadaptive	トラフィック シェーピングが有効なときに、BECN 統合で使用可能な帯域幅を推定するには、フレーム リレー インターフェイスまたはポイントツーポイント サブインターフェイスを設定します。
shape fecn-adapt	Q.922 TEST RESPONSE メッセージで、受信した FECN ビットを BECN ビットとして反映するために、フレーム リレー PVC を設定します。

コマンド	説明
show policy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。設定すると、コマンド出力に ATM オーバーヘッド アカウンティングに関する情報が含まれます。
show running-config	ルータの現在の設定を表示します。設定すると、コマンド出力に ATM オーバーヘッド アカウンティングに関する情報が含まれます。

shape adaptive

フレーム リレー インターフェイスまたはポイントツーポイント サブインターフェイスを設定して、トラフィック シェーピング有効時に、逆方向明示的輻輳通知（BECN）統合で使用可能な帯域幅を推定するには、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 **shapeadaptive** コマンドを使用します。使用可能な帯域幅を予測しない場合は、このコマンドの **no** 形式を使用します。

shape adaptive *mean-rate-lower-bound*
no shape adaptive

構文の説明

mean-rate-lower-bound	許可されたビット レートの範囲の下限を指定します。

コマンド デフォルト

帯域幅の予測はしません。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.2(13)T	このコマンドが、Cisco 1700 シリーズ、Cisco 2500 シリーズ、Cisco 2600 シリーズ、Cisco 3620 ルータ、Cisco 3631 ルータ、Cisco 3640 ルータ、Cisco 3660 ルータ、Cisco 3725 ルータ、Cisco 3745 ルータ、Cisco 7200 シリーズ、Cisco 7400 シリーズ ルータに実装されました。
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。

使用上のガイドライン

トラフィック シェーピングが無効の場合、このコマンドは無効です。

連続して BECN メッセージを受信すると、シェープ エンティティはすぐに各 BECN 受信メッセージに対応する最大シェープ レートを 1/4 だけ減らします。これは、設定情報レート（CIR）の下限に達するまで実行されます。複数のインターバルの後、インターフェイスに別の BECN が着信せず、トラフィックがシェープ キューで待機している場合、シェープ エンティティは各インターバルでシェープ レートを最大シェープ レートの 1/16 だけ増やします。**shapeadaptive***mean-rate-lower-bound* コマンドで設定したシェープ エンティティは平均レートの上限と下限の間で常にシェーピングされます。

（注） **shapeadaptive** コマンドと **shape(percent)** コマンドは同時には使用できません。

例

次の例では、CIR が 128 kbps のシェープ エンティティを設定し、CIR の下限を BECN 受信時は 64 kbps に設定します。

```
policy-map dts-p2p-all-action

class class-p2p-all

shape adaptive 64000
```

関連コマンド

コマンド	説明
shape(percent)	インターフェイスで使用可能な帯域幅の割合（%）に基づいて、平均レート トラフィック シェーピングとピーク レート トラフィック シェーピングを指定します。

shape fecn-adapt

フレーム リレー インターフェイスを設定して、Q.922 TEST RESPONSE メッセージ内で、受信した順方向明示的輻輳通知（FECN）ビットを逆方向明示的輻輳通知（BECN）ビットとして反映するには、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**shapefecn-adapt** コマンドを使用します。フレーム リレー インターフェイスで FECN を BECN として反映しない場合は、このコマンドの **no** 形式を使用します。

shape fecn-adapt
no shape fecn-adapt

構文の説明

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

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.2(13)T	このコマンドが、Cisco 1700 シリーズ、Cisco 2500 シリーズ、Cisco 2600 シリーズ、Cisco 3620 ルータ、Cisco 3631 ルータ、Cisco 3640 ルータ、Cisco 3660 ルータ、Cisco 3725 ルータ、Cisco 3745 ルータ、Cisco 7200 シリーズ、Cisco 7400 シリーズ ルータに実装されました。
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。

使用上のガイドライン

ダウンストリーム フレーム リレー スイッチが輻輳している場合、フレーム リレー インターフェイスまたはポイントツーポイントインターフェイスでは、FECN ビットがオンになったフレーム リレー メッセージが受信されます。このメッセージは、相手先へ BECN を伝送する待機中のトラフィックがないことを意味する場合があります（voice/multimedia トラフィックは単方向です）。**shapefecn-adapt** コマンドを設定すると、小さなバッファが割り当てられ、フレーム リレー TEST RESPONSE がフレーム リレー スイッチの代わりに作成されます。フレーム リレー TEST RESPONSE には、トリガー機能であるデータ リンク接続識別子（DLCI）のトリガーが設定されます。また、BECN ビットが設定されて、送信されます。

例

次の例では、設定情報レート（CIR）が 1 Mbps のシェープ エンティティを設定して、FECN を使用したフレーム リレー メッセージを BECN に適合させます。

```
policy-map dts-p2p-all-action

class class-p2p-all

shape average 1000000

shape fecn-adapt
```

関連コマンド

コマンド	説明
shapeadaptive	トラフィック シェーピングが有効なときに、BECN 統合で使用可能な帯域幅を推定するには、フレーム リレー インターフェイスまたはポイントツーポイント サブインターフェイスを設定します。
shape(percent)	指定されたビット レートにトラフィックをシェーピングするようにインターフェイスを設定します。

shape max-buffers

シェーピング キューで使用可能なバッファの数を指定するには、クラスマップ コンフィギュレーション モードで **shapemax-buffers** コマンドを使用します。バッファ数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。

shape max-buffers *number-of-buffers*
no shape max-buffers

構文の説明

number-of-buffers	バッファ数を指定します。バッファの最小数は 1 で、バッファの最大数は 4096 です。

コマンド デフォルト

バッファ数 1000 がプリセットされます。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更箇所
12.1(2)T	このコマンドが導入されました。
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。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されましたが、階層型キューイング フレームワーク（HQF）はサポートされていません。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。

使用上のガイドライン

ジェネリック トラフィック シェーピング（GTS）を使用するように設定されたクラスそれぞれに、シェーピング キューに認められる最大バッファ数を設定できます。

ポリシー マップのクラスの下でこのコマンドを設定できます。ただし、Cisco IOS Release 12.4(20)T の HQF については、**shapemax-buffers** はサポートされません。類似の機能の **queue-limit** コマンドを使用します。

例

次に、シェーピングを設定し、最大バッファ制限を 100 に設定する例を示します。

```
shape average 350000
shape max-buffers 100
```

関連コマンド

コマンド	説明
bandwidth	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
policy-map	1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
queue-limit	ポリシー マップで設定されているクラス ポリシーのためにキューが保持できるパケットの最大数を指定または変更します。
service-policy	入力インターフェイスまたはVC、あるいは出力インターフェイスまたはVCに、そのインターフェイスまたはVCのサービスポリシーとして使用するポリシー マップを対応付けます。
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。

show access-lists rate-limit

レート制限アクセス リストの情報を表示するには、EXEC モードで **showaccess-listsrate-limit** コマンドを使用します。

show access-lists rate-limit [*acl-index*]

構文の説明

acl-index	（任意）レート制限アクセス リストの番号は 1 ～ 299 です。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
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。

例

次に、**showaccess-listsrate-limit** コマンドの出力例を示します。

```
Router# show access-lists rate-limit
Rate-limit access list 1
    0
Rate-limit access list 2
    1
Rate-limit access list 3
    2
Rate-limit access list 4
    3
Rate-limit access list 5
    4
Rate-limit access list 6
    5
Rate-limit access list 9
    mask FF
Rate-limit access list 10
    mask 0F
Rate-limit access list 11
    mask F0
Rate-limit access list 100
    1001.0110.1111
Rate-limit access list 101
    00E0.34B8.D840
Rate-limit access list 199
    1111.1111.1111
```

次に、特定のレート制限アクセス リストを指定した場合の **showaccess-listsrate-limit** コマンドの出力例を示します。

```
Router# show access-lists rate-limit 1
Rate-limit access list 1
    0
Router# show access-lists rate-limit 9
Rate-limit access list 9
    mask FF
Router# show access-lists rate-limit 101
Rate-limit access list 101
    00E0.34B8.D840
```

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 *46 : show access-lists rate-limit* フィールドの説明

フィールド	説明
Rate-limit access list	レート制限アクセス リストの番号。1 ～ 99 の数字は、プレシデンスベースのアクセス リストを表します。100 ～ 199 の数字は、MAC アドレスベースのアクセス リストを示します。
0	このレート制限アクセス リスト内のパケットの IP プレシデンス。
mask FF	このレート制限アクセス リスト内のパケットの IP プレシデンス マスク。
1001.0110.1111	このレート制限アクセス リスト内のパケットの MAC アドレス。

関連コマンド

Command	Description
access-listrate-limit	CAR ポリシーで使用する場合のアクセス リストを設定します。
showaccess-lists	現在の IP とレート制限アクセス リストの内容を表示します。

show atm bundle

各バンドル仮想回線（VC）メンバーに割り当てられたバンドル属性と VC メンバーの現在の動作状態を表示するには、特権 EXEC モードで **showatmbundle** コマンドを使用します。

show atm bundle [*bundle-name*]

構文の説明

bundle-name	（任意）メンバー情報を表示するバンドルの名前。

コマンド デフォルト

バンドル名を指定しないと、VC に割り当てられたすべてのバンドルが表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
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。

例

次は、**showatmbundle** コマンドの出力例です（* は、この VC がすべてのプレシデンス レベルの VC であり、明示的に設定されていないことを示します）。

```
Router# show atm bundle

new-york on atm1/0.1 Status: UP
                     Config. Active  Bumping    PG/ Peak  Avg/Min  Burst
Name       VPI/VCI   Preced. Preced. Predec./   PV  kbps  kbps     Cells  Status
                                       Accept
ny-control   0/207      7        7      4  /Yes   pv  10000  5000     32      UP
ny-premium   0/206     6-5      6-5     7  /No    pg  20000  10000    32      UP
ny-priority  0/204     4-2      4-2     1  /Yes   pg  10000  3000             UP
ny-basic*    0/201     1-0      1-0     -  /Yes   pg  10000                   UP
los-angeles on atm1/0.1 - Status: UP

                     Config. Active  Bumping    pg/ Peak  Avg/Min  Burst
Name       VPI/VCI   Preced. Preced. Predec./   pv  kbps  kbps     Cells  Status
                                     Accept
la-high     0/407     7-5      7-5     4 /Yes      pv  20000  5000     32     UP
la-med      0/404     4-2      4-2     1 /Yes      pg  10000  3000             UP
la-low*     0/401     1-0      1-0     - /Yes      pg  10000                   UP
san-francisco on atm1/0.1 Status: UP
                     Config. Active  Bumping    PG/ Peak  Avg/Min  Burst
Name       VPI/VCI   Preced. Preced. Predec./   PV  kbps  kbps     Cells  Status
                                     Accept
sf-control   0/307      7        7      4 /Yes   pv  10000  5000     32      UP
sf-premium   0/306     6-5      6-5     7 /No    pg  20000  10000    32      UP
```

```
sf-priority  0/304     4-2      4-2      1 /Yes   pg  10000  3000            UP
sf-basic*    0/301     1-0      1-0      - /Yes   pg  10000                  UP
```

関連コマンド

Command	Description
bundle	バンドルを作成するか、既存のバンドルを変更します。
showatmbundlestatistics	指定されたバンドルの統計を表示します。
showatmmap	ATM ネットワーク上のリモート ホストに対する設定済み ATM スタティック マップをすべてリストします。

show atm bundle stat

指定したバンドルの統計情報または詳細な統計情報を表示するには、特権 EXEC モードで **showatmbundlestat** コマンドを使用します。

show atm bundle *bundle-name* **stat [detail]**

構文の説明

bundle-name	メンバー情報を表示するバンドルの名前。
detail	（任意）詳細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	変更箇所
12.0(3)T	このコマンドが導入されました。
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。

例

次は、**showatmbundlestat** コマンドの出力例です。

```
Router# show atm bundle san-jose stat

Bundle Name: Bundle State: UP
AAL5-NLPID
OAM frequency : 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
BUNDLE is not managed.
InARP frequency: 15 minute(s)
InPkts: 3, OutPkts: 3, Inbytes: 1836, Outbytes: 1836
InPRoc: 3, OutPRoc: 0, Broadcasts: 3
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
Router# show atm bundle san-jose stat detail
Bundle Name: Bundle State: UP
AAL5-NLPID
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
BUNDLE is not managed.
InARP frequency: 15 minute(s)
InPkts: 3, OutPkts: 3, InBytes; 1836, OutBytes: 1836
InPRoc: 3, OutPRoc: 0, Broadcasts: 3
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
ATM1/0.52: VCD: 6, VPI: 0 VCI: 218, Connection Name: sj-basic
UBR, PeakRate: 155000
AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0xE00
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
```

```
OAM up retry count: 3, OAM down retry count: 5
OAM Loopbavk status: OAM Disabled
OMA VC state: Not Managed
ILMI VC state: Not Managed
InARP frequency: 15 minute(s)
InPkts: 3, OutPkts: 3, InBytes; 1836, OutBytes: 1836
InPRoc: 3, OutPRoc: 0,Broadcasts: 3
InFast: 0, OutFast: 0, InAS: 0, OututAS: 0
OAM cells received: 0
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 0
F4 InEndloop: 0, F4 OutSegloop:0, F4 InAIS: 0, F4 InRDI: 0
OAM cells sent: 0
F5 OutEndloop: 0. F5 OutSegloop: 0, f5 Out RDI:0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OUtRDI: 0
OAM cell drops: 0
Status; UP
ATM1/0.52: VCD: 4, VPI: 0 VCI: 216, Connection Name: sj-premium
UBR, PeakRate: 155000
AAL5-LLC/SNAP, etype: 0x0, Flags: 0xC20, VCmode: 0xE000
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state:  Not Managed
ILMI VC state: Not Managed
InARP frequency: 15 minute(s)
InPkts: 0, OutPkts: 0, InBytes; 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0
OAM cells received: 0
F5 InEndloop: 0, F4 InSegloop: 0, F4InAIS; 0, F4 InRDI: 0
F4 OutEndloop: 0, F4 OutSegloop: F4 OutRDI: 0
OAM cell drops: 0
Status: UP
```

関連コマンド

Command	Description
bundle	バンドルを作成するか、既存のバンドルを変更します。
showatmbundle	各バンドルの VC メンバに割り当てられたバンドルの属性と、VC メンバの現在の稼働ステータスを表示します。
showatmmap	ATM ネットワーク上のリモート ホストに対する設定済み ATM スタティック マップをすべてリストします。

show atm bundle svc

各バンドル仮想回線（VC）メンバーに割り当てられたバンドル属性と VC メンバーの現在の動作状態を表示するには、特権 EXEC モードで **showatmbundlesvc** コマンドを使用します。

show atm bundle svc [*bundle-name*]

構文の説明

bundle-name	（任意）**bundlesvc** コマンドで指定して表示する相手先選択接続（SVC）バンドルの名前。

コマンド デフォルト

バンドル名が指定されないと、このシステムに設定されたすべての SVC バンドルが表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(4)T	このコマンドが導入されました。

例

次は、**showatmbundlesvc** コマンドの出力例です。バンドル「finance」は 8 つのメンバーを含んでおり、ATM インターフェイス 1/0.1 に設定されます。バンドル メンバー ゼロを除くすべてのメンバーはアップ状態です。バンドル メンバー ゼロはデフォルトのメンバーで、開始されると常にオン状態で、すべてのトラフィックのデフォルトとして使用されます。

```
Router# show atm bundle svc finance
finance on ATM1/0.1:UP
                        Config    Current  Peak   Avg/Min   Burst
VC Name      VPI/VCI    Preced.   Preced.  Kbps   kbps      Cells   Sts
seven        0/37         7         7      10000   5000      32     UP
six          0/36         6         6       6000                    UP
five         0/40         5         5       5000                    UP
four         0/41         4         4       4000                    UP
three        0/42         3         3       3000                    UP
two          0/43         2         2       2000                    UP
one          0/44         1         1       1000                    UP
zero*                     0
```

次の表は、表示される重要なフィールドの説明です。

表 *47 : show atm bundle svc* フィールドの説明

フィールド	説明
finance on ATM1/0.1: UP	SVC バンドルの名前、インターフェイス タイプと番号、バンドルの状態。

フィールド	説明
VC Name	SVC バンドルの名前。
VPI/VCI	仮想パス識別子と仮想チャネル識別子。
Config.Preced.	設定されているプレシデンス。
Current Preced.	現在のプレシデンス。
Peak Kbps	SVC のピーク kbps。
Avg/Min kbps	SVC の平均または最小 kbps。
Sts	バンドル メンバーの状態。
*	デフォルトのバンドル メンバーを示します。

関連コマンド

コマンド	説明
bundlesvc	SVCバンドルを作成または変更します。

show atm bundle svc stat

相手先選択接続（SVC）バンドルの統計情報を表示するには、特権 EXEC モードで **showatmbundlesvcstat** コマンドを使用します。

show atm bundle svc *bundle-name* **stat [detail]**

構文の説明

bundle-name	**bundlesvc** コマンドで指定する SVC バンドルの名前。
detail	（任意）ATMバンドル統計情報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	変更箇所
12.2(4)T	このコマンドが導入されました。

例

次は、バンドル名「city」を使用した **showatmbundlesvcstat** コマンドの出力例です。

```
Router# show atm bundle svc city stat
Bundle Name:Bundle State:INITIALIZING
AAL5-NLPID
OAM frequency:0 second(s), OAM retry frequency:10 second(s)
OAM up retry count:4, OAM down retry count:3
BUNDLE is managed by.
InARP frequency:15 minutes(s)
InPkts:0, OutPkts:0, InBytes:0, OutBytes:0
InPRoc:0, OutPRoc:0, Broadcasts:0
InFast:0, OutFast:0, InAS:0, OutAS:0
InPktDrops:0, OutPktDrops:0
CrcErrors:0, SarTimeOuts:0, OverSizedSDUs:0,
                LengthViolation:0, CPIErrors:0
```

表 *48 : show atm bundle svc statistics* フィールドの説明

フィールド	説明
Bundle Name	バンドルの名前。
State	バンドルの状態。
BUNDLE is managed by	バンドル管理。
InARP frequency	Inverse ARP メッセージ間隔（分）、Inverse ARP がこの VC で使用されていない場合は「DISABLED」。

フィールド	説明
InPkts	この仮想回線（VC）で受信するパケット（すべてのファストスイッチングおよびプロセススイッチング パケットなど）の合計数。
OutPkts	この VC から送信するパケット（すべてのファストスイッチングおよびプロセススイッチング パケットなど）の合計数。
InBytes	この VC に受信するバイト（すべてのファストスイッチングおよびプロセススイッチング パケットなど）の合計数。
OutBytes	この VC から送信するバイト（すべてのファストスイッチングおよびプロセススイッチング パケットなど）の合計数。
InPRoc	プロセススイッチングされている着信パケットの数。
OutPRoc	プロセススイッチングされている発信パケットの数。
Broadcasts	プロセススイッチング ブロードキャスト パケットの数。
InFast	ファストスイッチングされている着信パケットの数。
OutFast	ファストスイッチングされている発信パケットの数。
InAS	受信した自律スイッチングまたはシリコンスイッチング入力パケットの数。
OutAS	送信した自律スイッチングまたはシリコンスイッチング入力パケットの数。
InPktDrops	ドロップされた着信パケットの数。
OutPktDrops	ドロップされた発信パケットの数。
CrcErrors	巡回冗長検査（CRC）エラーの数。
SarTimeOuts	セグメンテーション/リアセンブリの発生までにタイムアウトしたパケットの数。
LengthViolation	長さの上限または下限を超えたパケットの数。

関連コマンド

コマンド	説明
bundlesvc	SVCバンドルを作成または変更します。

show auto discovery qos から show ip rsvp hello client lsp detail

- show auto discovery qos （1205 ページ）
- show auto qos （1209 ページ）
- show class-map （1214 ページ）
- show class-map type nat （1217 ページ）
- show class-map type port-filter （1219 ページ）
- show control-plane cef-exception counters （1221 ページ）
- show control-plane cef-exception features （1223 ページ）
- show control-plane counters （1225 ページ）
- show control-plane features （1227 ページ）
- show control-plane host counters （1229 ページ）
- show control-plane host features （1231 ページ）
- show control-plane host open-ports （1233 ページ）
- show control-plane transit counters （1236 ページ）
- show control-plane transit features （1238 ページ）
- show cops servers （1240 ページ）
- show crypto eng qos （1241 ページ）
- show crypto entropy status （1242 ページ）
- show frame-relay ip rtp header-compression （1244 ページ）
- show frame-relay ip tcp header-compression （1249 ページ）
- show interfaces fair-queue （1252 ページ）
- show interfaces random-detect （1255 ページ）
- show interfaces rate-limit （1258 ページ）
- show iphc-profile （1261 ページ）
- show ip nat translations rsvp （1263 ページ）
- show ip nbar attribute （1265 ページ）
- show ip nbar classification auto-learn top-asymmetric-sockets （1268 ページ）
- show ip nbar link-age （1271 ページ）
- show ip nbar classification auto-learn top-hosts （1273 ページ）

- show ip nbar classification granularity （1274 ページ）
- show ip nbar pdlm （1275 ページ）
- show ip nbar port-map （1276 ページ）
- show ip nbar protocol activated （1278 ページ）
- show ip nbar protocol-attribute （1279 ページ）
- show ip nbar protocol-discovery （1281 ページ）
- show ip nbar protocol-id （1285 ページ）
- show ip nbar protocol-pack （1298 ページ）
- show ip nbar resources flow （1300 ページ）
- show ip nbar statistics （1301 ページ）
- show ip nbar trace （1302 ページ）
- show ip nbar unclassified-port-stats （1304 ページ）
- show ip nbar version （1307 ページ）
- show ip rsvp （1310 ページ）
- show ip rsvp aggregation ip （1317 ページ）
- show ip rsvp aggregation ip endpoints （1321 ページ）
- show ip rsvp atm-peak-rate-limit （1325 ページ）
- show ip rsvp authentication （1327 ページ）
- show ip rsvp counters （1333 ページ）
- show ip rsvp counters state teardown （1337 ページ）
- show ip rsvp fast bw-protect （1339 ページ）
- show ip rsvp fast detail （1341 ページ）
- show ip rsvp fast-reroute （1345 ページ）
- show ip rsvp fast-reroute bw-protect （1349 ページ）
- show ip rsvp fast-reroute detail （1353 ページ）
- show ip rsvp hello （1359 ページ）
- show ip rsvp hello client lsp detail （1361 ページ）

show auto discovery qos

エンタープライズ機能用 AutoQoS の自動検出（データ収集）フェーズ中に収集したデータを表示するには、特権 EXEC モードで **showautodiscoveryqos** コマンドを使用します。

show auto discovery qos [**interface** [*type number*]]

構文の説明

interface	（任意）特定のインターフェイス タイプの設定が表示されることを示します。
type number	（オプション）インターフェイスのタイプおよび番号を指定します。

コマンド デフォルト

すべてのインターフェイス タイプ用に作成された設定を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.3(7)T	このコマンドが導入されました。
12.3(11)T	コマンド出力が変更され、推奨ポリシー マップ情報が追加されました。

使用上のガイドライン

推奨ポリシー出力（次の例に表示）を使用すると、**autoqos** コマンドをインターフェイスに実行する前にクラス マップとポリシー マップをプレビューできます。これにより、データを追加で収集するか、既存のデータをカット アンド ペーストして必要に応じて編集するまで、自動検出フェーズを継続できます。

例

次は、**showautodiscoveryqos** コマンドの出力例です。この例では、信頼モードで DSCP 分類を使用した自動検出（データ収集）フェーズ中に収集したデータを表示します。推奨ポリシー マップ情報も含まれます。

```
Router# show auto discovery qos
Serial2/1.1
 AutoQoS Discovery enabled for trusted DSCP
 Discovery up time: 2 hours, 42 minutes
 AutoQoS Class information:
 Class Voice:
  Recommended Minimum Bandwidth: 118 Kbps/1% (PeakRate)
  Detected DSCPs and data:
  DSCP value         AverageRate        PeakRate           Total
                     (kbps/%)           (kbps/%)           (bytes)
  -----------        -----------        --------           -------------
  46/ef              106/1              118/1              129510064
 Class Interactive Video:
  Recommended Minimum Bandwidth: 25 Kbps/<1% (AverageRate)
  Detected DSCPs and data:
  DSCP value         AverageRate        PeakRate           Total
```

```
                    (kbps/%)            (kbps/%)            (bytes)
  ------------      ------------        --------            ------------
   34/af41          25/<1               28/<1               31084292
  Class Signaling:
   Recommended Minimum Bandwidth: 50 Kbps/<1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   24/cs3           50/<1               56/<1               61838040
  Class Streaming Video:
   Recommended Minimum Bandwidth: 79 Kbps/<1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   32/cs4           79/<1               88/<1               96451788
  Class Transactional:
   Recommended Minimum Bandwidth: 105 Kbps/1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   18/af21          105/1               117/1               127798678
  Class Bulk:
   Recommended Minimum Bandwidth: 132 Kbps/1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   10/af11          132/1               147/1               160953984
  Class Scavenger:
   Recommended Minimum Bandwidth: 24 Kbps (AverageRate)/0% (fixed)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   8/cs1            24/<1               27/<1               30141238
  Class Management:
   Recommended Minimum Bandwidth: 34 Kbps/<1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   16/cs2           34/<1               38/<1               41419740
  Class Routing:
   Recommended Minimum Bandwidth: 7 Kbps/<1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   48/cs6           7/<1                7/<1                8634024
  Class Best Effort:
   Current Bandwidth Estimation: 820 Kbps/8% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   0/default        820/8               915/9               997576380
  Suggested AutoQoS Policy based on a discovery uptime of 2 hours, 42 minutes:
   !
   class-map match-any AutoQoS-Voice-Trust
    match ip dscp ef
   !
```

```
class-map match-any AutoQoS-Inter-Video-Trust
 match ip dscp af41
!
class-map match-any AutoQoS-Signaling-Trust
 match ip dscp cs3
!
class-map match-any AutoQoS-Stream-Video-Trust
 match ip dscp cs4
!
class-map match-any AutoQoS-Transactional-Trust
 match ip dscp af21
 match ip dscp af22
 match ip dscp af23
!
class-map match-any AutoQoS-Bulk-Trust
 match ip dscp af11
 match ip dscp af12
 match ip dscp af13
!
class-map match-any AutoQoS-Scavenger-Trust
 match ip dscp cs1
!
class-map match-any AutoQoS-Management-Trust
 match ip dscp cs2
!
class-map match-any AutoQoS-Routing-Trust
 match ip dscp cs6
!
policy-map AutoQoS-Policy-S2/1.1Trust
 class AutoQoS-Voice-Trust
  priority percent 1
 class AutoQoS-Inter-Video-Trust
  bandwidth remaining percent 1
 class AutoQoS-Signaling-Trust
  bandwidth remaining percent 1
 class AutoQoS-Stream-Video-Trust
  bandwidth remaining percent 1
 class AutoQoS-Transactional-Trust
  bandwidth remaining percent 1
  random-detect dscp-based
 class AutoQoS-Bulk-Trust
  bandwidth remaining percent 1
  random-detect dscp-based
 class AutoQoS-Scavenger-Trust
  bandwidth remaining percent 1
 class AutoQoS-Management-Trust
  bandwidth remaining percent 1
 class AutoQoS-Routing-Trust
  bandwidth remaining percent 1
 class class-default
  fair-queue
```

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 *49 : show auto discovery qos* フィールドの説明

フィールド	説明
Serial2/1.1	データが収集されるインターフェイスまたはサブインターフェイス。

フィールド	説明
AutoQoS Discovery enabled for trusted DSCP	AutoQoSのデータ収集フェーズが有効であることを示します。
Discovery up time	データが収集された期間を示します。
AutoQoS Class information	各 AutoQoS クラスの情報を表示します。
Class Voice	指定されたクラスの情報。検出されたアプリケーションに関連するデータも含まれます。このデータには、DSCP値、平均レート（キロビット/秒（kbps））、ピーク レート（kbps）、および合計パケット（バイト）が含まれます。
Suggested AutoQoS Policy based on a discovery uptime of hours and minutes	指定された検出時間に基づいた、ポリシーマップとクラスマップの統計情報。

関連コマンド

コマンド	説明
autoqos	エンタープライズ機能の AutoQoS によって作成された QoS クラス マップおよびポリシー マップをインストールします。
autodiscoveryqos	エンタープライズ機能用 AutoQoS 設定に使用するデータの検出と収集を開始します。
showautoqos	特定のインターフェイスまたはすべてのインターフェイスでAutoQoSによって作成されたインターフェイス コンフィギュレーション、ポリシーマップ、およびクラス マップを表示します。

show auto qos

特定のインターフェイスまたはすべてのインターフェイスの AutoQoS で作成されるインターフェイス設定、ポリシー マップ、およびクラス マップを表示するには、特権 EXEC モードで **showautoqos** コマンドを使用します。

show auto qos [**interface** [*type slot/ port*]]

構文の説明

interface	（任意）AutoQoS--VoIP 機能が有効になっているすべてのインターフェイスまたは PVC の AutoQoS--VoIP 機能で作成された設定を表示します。 • **interface** キーワードを設定していても、インターフェイス タイプを指定していない場合、**showautoqosinterface** コマンドは AutoQoS--VoIP 機能が有効になっているすべてのインターフェイスまたは PVC の AutoQoS--VoIP 機能で作成された設定を表示します。
type	（任意）インターフェイス タイプ：有効な値は、**atm**、**ethernet**、**fastethernet**、**ge-wan**、**gigabitethernet**、**pos**、および **tengigabitethernet** です。
slot / port	（任意）スロットおよびポート番号。

コマンド デフォルト

引数またはキーワードを指定しない場合、すべてのインターフェイス タイプに作成された設定が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(15)T	このコマンドが、AutoQoS--VoIP 機能の一部として導入されました。
12.3(7)T	このコマンドが変更され、エンタープライズ機能の AutoQoS に対応しました。出力が変更され、エンタープライズ機能用 AutoQoS の自動検出フェーズ中に収集されたデータに基づいて作成されたクラス、クラス マップ、およびポリシー マップを表示するようになりました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
15.2(1)T	このコマンドが変更されました。出力に、フレーム リレー トラフィック シェーピング設定は表示されません。

使用上のガイドライン

showautoqosinterface コマンドは、フレーム リレー データリンク接続識別子（DLCI）と ATM PVC で使用できます。

AutoQoS--VoIP またはエンタープライズ機能用 AutoQos が有効になっていると、各インターフェイスまたはPVCに対応した設定が生成されます。これらの設定を使用して、インターフェイス設定、ポリシー マップ、クラス マップ、およびアクセス コントロール リスト（ACL）を作成し、ネットワークで使用します。**showautoqos** コマンドを使用して、インターフェイス設定、ポリシー マップ、クラス マップ、および ACL の内容を検証できます。

Catalyst 6500 シリーズ スイッチ

AutoQoS は次のモジュールでサポートされています。

- WS-X6548-RJ45
- WS-X6548-RJ21
- WS-X6148-GE-TX
- WS-X6548-GE-TX-CR
- WS-X6148-RJ45V
- WS-X6148-RJ21V
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6248-TEL

例

show auto qos interface コマンド：AutoQoS--VoIP 機能に対応した設定

showautoqosinterface*typeslot/port* コマンドは、特定のインターフェイスの AutoQoS--VoIP 機能で作成された設定を表示します。

次の例では、シリアル サブインターフェイス 6/1.1 が指定されています。

```
Router# show auto qos interface serial 6/1.1
S6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
 frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output AutoQoS-Policy-UnTrust
 frame-relay fragment 640
```

interface キーワードを設定していても、インターフェイス タイプを指定していない場合、**showautoqosinterface** コマンドはAutoQoS--VoIP機能が有効になっているすべてのインターフェイスまたはPVC の AutoQoS--VoIP 機能で作成された設定を表示します。

```
Router# show auto qos interface
```

```
Serial6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
 frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output AutoQoS-Policy-UnTrust
 frame-relay fragment 640
ATM2/0.1: PVC 1/100 -
!
interface ATM2/0.1 point-to-point
 pvc 1/100
  tx-ring-limit 3
  encapsulation aal5mux ppp Virtual-Template200
!
interface Virtual-Template200
 bandwidth 512
 ip address 10.10.107.1 255.255.255.0
 service-policy output AutoQoS-Policy-UnTrust
 ppp multilink
 ppp multilink fragment-delay 10
 ppp multilink interleave
```

次の例は、AutoQoS--VoIP 機能で作成されたすべての設定を表示します。

```
Router# show auto qos
Serial6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
 frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output AutoQoS-Policy-UnTrust
 frame-relay fragment 640
```

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 *50 : show auto qos* フィールドの説明（*AutoQoS--VoIP* 機能の設定）

フィールド	説明
class AutoQoS-VoIP-FR-Serial6/1-100	AutoQoS-VoIP 機能で作成されたクラスの名前。この例では、クラスの名前は AutoQoS-VoIP-FR-Serial6/1-100 です。
service-policy output AutoQoS-Policy-UnTrust	ポリシー マップ「AutoQoS-Policy-UnTrust」が、インターフェイスの発信方向のインターフェイスに適用されていることを示します。

show auto qos interface コマンド：エンタープライズ機能用 AutoQoS に対応した設定

次は、**showautoqos** コマンドの出力例です。この例では、エンタープライズ機能用 AutoQoS の自動検出フェーズ中に収集されたデータに基づいて作成されたクラス、クラス マップ、およびポリシー マップを表示します。

```
Router# show auto qos
 !
  policy-map AutoQoS-Policy-Se2/1.1
   class AutoQoS-Voice-Se2/1.1
    priority percent 70
    set dscp ef
   class AutoQoS-Inter-Video-Se2/1.1
    bandwidth remaining percent 10
    set dscp af41
   class AutoQoS-Stream-Video-Se2/1.1
    bandwidth remaining percent 1
    set dscp cs4
   class AutoQoS-Transactional-Se2/1.1
    bandwidth remaining percent 1
    set dscp af21
   class AutoQoS-Scavenger-Se2/1.1
    bandwidth remaining percent 1
    set dscp cs1
   class class-default
    fair-queue
 !
policy-map AutoQoS-Policy-Se2/1.1-Parent
   class class-default
    shape average 1024000
    service-policy AutoQoS-Policy-Se2/1.1
 !
 class-map match-any AutoQoS-Stream-Video-Se2/1.1
  match protocol cuseeme
 !
 class-map match-any AutoQoS-Transactional-Se2/1.1
  match protocol sqlnet
 !
class-map match-any AutoQoS-Voice-Se2/1.1
  match protocol rtp audio
 !
 class-map match-any AutoQoS-Inter-Video-Se2/1.1
  match protocol rtp video
 !
 rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice Drops" owner
 AutoQoS
Serial2/1.1: DLCI 58 -
 !
 interface Serial2/1.1 point-to-point
  frame-relay interface-dlci 58
   class AutoQoS-FR-Serial2/1-58
 !
 map-class frame-relay AutoQoS-FR-Serial2/1-58
  frame-relay cir 1024000
frame-relay bc 10240
  frame-relay be 0
  frame-relay mincir 1024000
  service-policy output AutoQoS-Policy-Se2/1.1-Parent
```

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 auto qos* フィールドの説明（エンタープライズ機能用 *AutoQoS* の設定）

フィールド	説明
policy-map AutoQoS-Policy-Se2/1.1	AutoQoS 機能で作成されたポリシー マップの名前。この例では、ポリシー マップの名前は AutoQoS-Policy-Se2/1.1 です。
class AutoQoS-Voice-Se2/1.1 priority percent 70 set dscp ef	AutoQoS機能で作成されたクラスの名前。この例では、クラスの名前は AutoQoS-Voice-Se2/1.1 です。クラス名に続いて、クラスに設定された固有の QoS 機能が表示されます。
class-map match-any AutoQoS-Stream-Video-Se2/1.1 match protocol cuseeme	クラス マップの名前と指定されたパケット一致基準。

関連コマンド

コマンド	説明
autodiscoveryqos	エンタープライズ機能用 AutoQoS 設定に使用するデータの検出と収集を開始します。
autoqos	エンタープライズ機能の AutoQoS によって作成された QoS クラス マップおよびポリシー マップをインストールします。
autoqosvoip	インターフェイスに AutoQoS--VoIP 機能を設定します。
showautodiscoveryqos	エンタープライズ機能用 AutoQoS の自動検出フェーズ中に収集されたデータを表示します。

show class-map

クラス マップとその一致基準を表示するには、特権 EXEC モードで **showclass-map** コマンドを使用します。

Cisco 3660、3845、6500、7400、および 7500 シリーズ ルータ
show class-map [**type** {**stack**|**access-control**}] [*class-map-name*]

Cisco 7600 および ASR 1000 シリーズ ルータ
show class-map [*class-map-name*]

構文の説明

typestack	（任意）Flexible Packet Matching（FPM）で検査して正しいプロトコル スタックを決定するように設定されたクラス マップを表示します。
typeaccess-control	（任意）対象のプロトコル スタック内を検索するために正確なパターンを決定するように設定されたクラス マップを表示します。
class-map-name	（任意）クラス マップ名クラス マップ名には、最大 40 の英数字を使用できます。

コマンド デフォルト

すべてのクラス マップが表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.2(13)T	このコマンドが変更され、クラス マップ内のトラフィックの一致基準として、フレーム リレー データ リンク接続識別子（DLCI）番号またはレイヤ 3 パケットの長さを表示するようになりました。
12.2(14)SX	このコマンドが Cisco 7600 シリーズ ルータに実装されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
12.4(4)T	**type**、**stack** および **access-control** キーワードが追加され、FPM がサポートされるようになりました。
Cisco IOS XE Release 2.2	このコマンドが Cisco ASR アグリゲーション サービス 1000 シリーズ ルータに実装されました。

リリース	変更箇所
15.0(1)M	このコマンドが変更されました。出力が変更され、暗号化フィルタ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

すべてのクラス マップとその一致基準を表示するには、**showclass-map** コマンドを使用します。オプションの *class-map-name* 引数を入力すると、指定したクラス マップとその一致基準が表示されます。

例

次の例では、3 つのクラス マップが定義されます。アクセス リスト 103 に一致するパケットはクラス c3、IP パケットはクラス c2、イーサネット インターフェイス 1/0 経由で着信するパケットはクラス c1 に属します。**showclass-map** コマンドの出力には、3 つの定義されたクラス マップが表示されます。

```
Router# show class-map
 Class Map c3
 Match access-group 103
 Class Map c2
 Match protocol ip
 Class Map c1
 Match input-interface Ethernet1/0
```

次の例では、c1 クラス マップが定義され、一致基準としてフレーム リレー DLCI 番号が 500 に指定されます。

```
Router# show class-map
class map match-all c1
   match fr-dlci 500
```

次に、すべてのクラス マップに関するクラス マップ情報を表示する例を示します。

```
Router# show class-map
 Class Map match-any class-default (id 0)
   Match any
 Class Map match-any class-simple (id 2)
   Match any
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5
 Class Map match-all agg-2 (id 3)
```

次に、特定のクラス マップに関するクラス マップ情報を表示する例を示します。

```
Router# show class-map ipp5
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5
```

次は、**showclass-maptypeaccess-control** コマンドを使用した、暗号化 FPM フィルタの出力例です。

```
Router# show class-map type access-control accesscontrol1
 Class Map type access-control match-all accesscontrol1 (id 4)
   Match encrypted FPM filter
            filter-hash   : FC50BED10521002B8A170F29AF059C53
```

```
          filter-version: 0.0_DummyVersion_20090101_1830
          filter-id     : cisco-sa-20090101-dummy_ddts_001
  Match start TCP payload-start offset 0 size 10 regex "abc.*def"
  Match field TCP source-port eq 1234
```

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 class-map* フィールドの説明（カッコで囲んだ番号がクラス マップ名と一致基準情報の横に表示される場合があります）この番号は、*Cisco* 内部だけで使用されるものであり、無視できます。

フィールド	説明
Class Map	表示されるトラフィックのクラス。ポリシーに設定されているクラスマップごとに出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
Match	クラス マップに指定された一致基準。フレーム リレー DLCI 番号、レイヤ 3 パケット長、IP プレシデンス、IP Diffserv コードポイント（DSCP）値、マルチプロトコル ラベル スイッチング（MPLS）EXP 値、アクセス グループ、およびサービス品質（QoS）グループなどの基準があります。

関連コマンド

Command	Description
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
matchfr-dlci	クラス マップの一致基準としてフレームリレー DLCI 番号を指定します。
matchpacketlength(class-map)	IP ヘッダーのレイヤ 3 パケットの長さをクラスマップの一致基準として指定して、使用します。
showpolicy-map	指定されたサービス ポリシーマップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

show class-map type nat

ネットワークアドレス変換（NAT）クラスマップとその一致基準を表示するには、特権EXECモードで **showclass-maptypenat** コマンドを使用します。

show class-map type nat [*class-map-name*]

構文の説明

class-map-name	（任意）NAT クラス マップの名前。名前には最大 40 文字までの英数字を指定できます。

コマンド デフォルト

すべての NAT クラス マップの情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(11)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

showclass-maptypenat コマンドは、すべての NAT クラス マップとその一致基準を表示します。特定の NAT クラス マップとその一致基準を表示するには、クラス マップ名を指定します。

例

次は、**showclass-maptypenat** コマンドの出力例で、すべてのクラス マップを表示します。

```
Router# show class-map type nat
Class Map match-all ipnat-class-acl-we (id 5)
   Match access-group  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 *53 : show class-map type nat* フィールドの説明

フィールド	説明
Class Map	クラスマップの名前と着信パケットに一致するクラスマップに適用する条件を表示します。
Match	クラス マップに指定された一致基準。

関連コマンド

コマンド	説明
showclass-maptypeinspect	レイヤ3とレイヤ4またはレイヤ7（用途別）検査タイプ クラスマップおよびその一致基準を表示します。
showclass-maptypeport-filter	ポートフィルタ クラスマップおよびその一致基準を表示します。

show class-map type port-filter

ポート フィルタのクラス マップとその一致基準を表示するには、特権 EXEC モードで **showclass-maptypeport-filter** コマンドを使用します。

show class-map type port-filter [*class-map-name*]

構文の説明

class-map-name	（任意）ポートフィルタ クラス マップの名前。名前には最大 40 文字までの英数字を指定できます。

コマンド デフォルト

引数を指定しないと、すべてのポートフィルタ クラス マップの情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(11)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

コントロール プレーン パケットの TCP/UDP ポート ポリシングを表示するには、**showclass-maptypeport-filter** コマンドを使用します。**showclass-maptypeport-filter** コマンドは、すべてのポートフィルタ クラス マップとその一致基準を表示します。特定のポートフィルタ クラス マップのクラス マップを表示するには、クラス マップ名を指定します。

例

次は、**showclass-maptypeport-filter** コマンドの出力例で、すべてのクラス マップを表示します。

```
Router# show class-map type port-filter
Class Map type port-filter match-all pf-policy (id 9)
   Match  port tcp 45 56
 Class Map type port-filter match-any cl1 (id 4)
   Match none
 Class Map type port-filter match-all pf-class (id 8)
   Match not  port udp 123
   Match  closed-ports
```

次は、**showclass-maptypeport-filter** コマンドの出力例で、クラス マップ pf-class を表示します。

```
Router# show class-map type port-filter pf-class
Class Map type port-filter match-all pf-class (id 8)
   Match not  port udp 123
   Match  closed-ports
```

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 *54 : show class-map type port-filter* フィールドの説明

フィールド	説明
Class Map	表示されているポートフィルタ クラス マップ。出力は、設定されているクラス マップごとに表示されます。クラス一致の実装の選択（match-all、match-any など）はトラフィック クラスの横に表示されます。
Match	クラス マップに指定された一致基準。有効な一致基準は、**closed-ports**、**not**、および **port** です。

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラスマップを作成します。

show control-plane cef-exception counters

コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示するには、特権 EXEC モードで **showcontrol-planecef-exceptioncounters** コマンドを使用します。

show control-plane cef-exception 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 モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)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

showcontrol-planecef-exceptioncounters コマンドは、コントロール プレーン CEF 例外サブインターフェイスに設定された機能の次のパケット数を表示します。

- CEF 例外サブインターフェイスで処理されたパケットの合計数
- ドロップされたパケットの合計数
- エラーの合計数

例

次は、**showcontrol-planecef-exceptioncounters** コマンドの出力例です。

```
Router# show control-plane cef-exception counters
 Control plane cef-exception path counters:
 Feature      Packets Processed/Dropped/Errors
 Control Plane Policing       63456/9273/0
```

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 *55 : show control-plane cef-exception counters* フィールドの説明

フィールド	説明
Feature	このサブインターフェイスに設定されている機能の名前。
Packets Processed	その機能で処理されたパケットの合計数。
Dropped	その機能でドロップされたパケットの合計数。
Errors	その機能で検出されたエラーの合計数。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーン インターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	ユーザが、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始します。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
show control-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
show control-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
show control-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-planehost open-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-plane transitcounters	コントロール プレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。

show control-plane cef-exception features

コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン機能を表示するには、特権 EXEC モードで **showcontrol-planecef-exceptionfeatures** コマンドを使用します。

show control-plane cef-exception features

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)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

showcontrol-planecef-exceptionfeatures コマンドは、コントロール プレーン CEF 例外サブインターフェイスの次の集約機能設定を表示します。

- コントロール プレーン CEF 例外サブインターフェイスに設定された機能の数。
- 機能の名前
- 機能が有効化された日時

例

次は、**showcontrol-planecef-exceptionfeatures** コマンドの出力例です。

```
Router# show control-plane cef-exception features
 Total 1 features configure
  Control plane cef-exception path features:
  Control Plane Policing activated Nov 09 2005 12:40
```

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 56 : show control-plane cef-exception features フィールドの説明

フィールド	説明
Total features configured	設定された機能の数。
Feature Name	設定された機能の名前。
Activated	機能が有効化された日時。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーン インターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	ユーザが、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始します。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-planecef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planefeatures	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane hostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-plane hostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。

show control-plane counters

すべてのコントロール プレーン インターフェイスのコントロール プレーン カウンタを表示するには、特権 EXEC モードで **showcontrol-planecounters** コマンドを使用します。

show control-plane 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 モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)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

showcontrol-planecounters コマンドは、すべてのコントロール プレーン インターフェイスおよびサブインターフェイスの次の集約パケット数を表示します。

- コントロール プレーン集約ホスト、トランジット、および CEF 例外サブインターフェイスで処理されたパケットの合計数
- ドロップされたパケットの合計数
- エラーの合計数

例

次に、**showcontrol-planecounters** コマンドの出力例を示します。

```
Router# show control-plane counters
 Feature Path     Packets Processed/Dropped/Errors
  aggregate      43271/6759/0
  host      24536/4238/0
  transit      11972/2476/0
     cef-exception path       6345/0/0
```

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 *57 : show control-plane counters* フィールドの説明

フィールド	説明
Feature	表示されたインターフェイスまたはサブインターフェイスの名前。
Packets Processed	そのサブインターフェイスで処理されたパケットの合計数。
Dropped	ドロップされたパケットの合計数

フィールド	説明
Errors	検出されたエラーの合計数。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーン インターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	ユーザが、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始します。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
show control-planecef-exception features	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane hostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
show control-planehostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
show control-plane transitcounters	コントロール プレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane transitfeatures	コントロール プレーン中継サブインターフェイスに対して設定された機能を表示します。

show control-plane features

設定されたコントロール プレーン機能を表示するには、特権 EXEC モードで **showcontrol-planefeatures** コマンドを使用します。

show control-plane features

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)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

showcontrol-planefeatures コマンドは、コントロール プレーン集約サブインターフェイスで有効になっているコントロール プレーン機能を表示します。次の事項が表示されます。

- コントロール プレーンに設定された機能の数
- 機能の名前
- 機能が有効化された日時

例

次に、**showcontrol-planefeatures** コマンドの出力例を示します。

```
Router# show control-plane features
 Total 1 features configured
  Control plane host path features:
  TCP/UDP Portfilter activated Nov 09 2005 12:40
```

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 *58 : show control-plane features* フィールドの説明

フィールド	説明
Total features configured	設定された機能の数。
Feature Name	設定された機能の名前。
activated	機能が有効化された日時。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	ユーザが、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始します。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-plane hostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planetransitfeatures	コントロールプレーン中継サブインターフェイスに対して設定された機能を表示します。

show control-plane host counters

コントロール プレーン ホスト サブインターフェイスのコントロール プレーン パケット カウンタを表示するには、特権 EXEC モードで **showcontrol-planehostcounters** コマンドを使用します。

show control-plane host 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 モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)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

showcontrol-planehostcounters コマンドは、コントロール プレーン ホスト サブインターフェイスの次のパケット数を表示します。

- そのホスト サブインターフェイスに設定されている機能で処理されたパケットの合計数
- ドロップされたパケットの合計数
- エラーの合計数

例

次は、**showcontrol-planehostcounters** コマンドの出力例です。

```
Router# show control-plane host counters
 Control plane host path counters:
 Feature      Packets Processed/Dropped/Errors
 TCP/UDP portfilter       46/46/0
```

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 *59 : show control-plane host counters* フィールドの説明

フィールド	説明
Feature	ホストサブインターフェイスに設定された機能の名前。
Packets Processed	その機能で処理されたパケットの合計数。
Dropped	ドロップされたパケットの合計数
Errors	検出されたエラーの合計数。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	ユーザが、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始します。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-planehostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planetransitfeatures	コントロール プレーン トランジット サブインターフェイスに設定されている機能を表示します。

show control-plane host features

コントロール プレーン ホスト サブインターフェイスに設定されているコントロール プレーン機能を表示するには、特権 EXEC モードで **showcontrol-planehostfeatures** コマンドを使用します。

show control-plane host features

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)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

showcontrol-planehostfeatures コマンドは、コントロール プレーン ホスト サブインターフェイスに設定されている機能を表示します。次の事項が表示されます。

- コントロール プレーンに設定された機能の数
- 機能の名前
- 機能が有効化された日時

例

次は、**showcontrol-planehostfeatures** コマンドの出力例です。

```
Router# show control-plane host features
   Control plane host path features:
  TCP/UDP Portfilter activated Nov 09 2005 12:40
```

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 *60 : show control-plane host features* フィールドの説明

フィールド	説明
Feature Name	設定された機能の名前。
activated	機能が有効化された日時。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	コントロール プレーン コンフィギュレーション モードを開始します。このモードでは、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更ができます。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外のサブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane hostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planetransitfeatures	コントロールプレーン中継サブインターフェイスに対して設定された機能を表示します。

show control-plane host open-ports

ポート フィルタ データベースに登録されたオープンな TCP/UDP ポートのリストを表示するには、特権 EXEC モードで **showcontrol-planehostopen-ports** コマンドを使用します。

show control-plane host open-ports

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)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

showcontrol-planehostopen-ports コマンドは、ポート フィルタ データベースに登録されたオープンな TCP/UDP ポートのリストを表示します。

例

次に、**showcontrol-planehostopen-ports** コマンドの出力例を示します。

```
Router# show control-plane host open-ports

Active internet connections (servers and established)
Port        Local Address      Foreign Address                  Service    State
 tcp                *:23                *:0                    Telnet   LISTEN
 tcp                *:53                *:0                DNS Server   LISTEN
 tcp                *:80                *:0                 HTTP CORE   LISTEN
 tcp              *:1720                *:0                     H.225   LISTEN
 tcp              *:5060                *:0                       SIP   LISTEN
 tcp                *:23      192.0.2.18:58714              Telnet   ESTABLISHED
 udp                *:53                *:0                DNS Server   LISTEN
 udp                *:67                *:0             DHCPD Receive   LISTEN
 udp             *:52824                *:0                   IP SNMP   LISTEN
 udp               *:161                *:0                   IP SNMP   LISTEN
 udp               *:162                *:0                   IP SNMP   LISTEN
 udp              *:5060                *:0                       SIP   LISTEN
 udp              *:2517                *:0                 CCH323_CT   LISTEN
```

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 *61 : show control-plane host open-ports* フィールドの説明

フィールド	説明
Port	ポート タイプ（TCP または UDP）。

フィールド	説明
Local Address	ローカルIPアドレスとポート番号。アスタリスク（*）は、サービスがすべての設定済みネットワーク インターフェイスでリッスンしていることを示します。
Foreign Address	リモートIPアドレスとポート番号。アスタリスク（*）は、サービスがすべての設定済みネットワーク インターフェイスでリッスンしていることを示します。
Service	ポートに設定された Cisco IOS サービス リスニングの名前。
State	Listen または Established。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	コントロール プレーン コンフィギュレーション モードを開始します。このモードでは、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更ができます。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-planetransitcounters	コントロール プレーン トランジット サブインターフェイスのコントロール プレーン パケット カウンタを表示します。

コマンド	Description
showcontrol-planetransitfeatures	コントロールプレーン中継サブインターフェイスに対して設定された機能を表示します。

show control-plane transit counters

コントロールプレーン トランジット サブインターフェイスのコントロールプレーン パケット カウンタを表示するには、特権 EXEC モードで **showcontrol-planetransitcounters** コマンドを使用します。

show control-plane transit 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 モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)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

showcontrol-planetransitcounters コマンドは、コントロール プレーン トランジット サブインターフェイスの次のパケット数を表示します。

- そのトランジット サブインターフェイスで処理されたパケットの合計数
- ドロップされたパケットの合計数
- エラーの合計数

例

次は、**showcontrol-planetransitcounters** コマンドの出力例です。

```
Router# show control-plane transit counters
 Control plane transit path counters:
 Feature      Packets Processed/Dropped/Errors
     Control Plane Policing       63456/2391/0
```

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 *62 : show control-plane transit counters* フィールドの説明

フィールド	説明
Feature	トランジットサブインターフェイスに設定された機能の名前。
Packets Processed	設定された機能で処理されたパケットの合計数。
Dropped	ドロップされたパケットの合計数
Errors	検出されたエラーの合計数。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	コントロール プレーン コンフィギュレーション モードを開始します。このモードでは、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更ができます。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外のサブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-plane hostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitfeatures	コントロールプレーン中継サブインターフェイスに対して設定された機能を表示します。

show control-plane transit features

コントロール プレーン トランジット サブインターフェイスに設定されているコントロール プレーン機能を表示するには、特権 EXEC モードで **showcontrol-planetransitfeatures** コマンドを使用します。

show control-plane transit features

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)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

showcontrol-planetransitfeatures コマンドは、コントロール プレーン トランジット サブインターフェイスに設定されているコントロールプレーン機能を表示します。次の事項が表示されます。

- コントロール プレーンに設定された機能の数
- 機能の名前
- 機能が有効化された日時

例

次は、**showcontrol-planetransitfeatures** コマンドの出力例です。

```
Router# show control-plane transit features
  Control plane transit path features:
  Control Plane Policing activated Nov 09 2005 12:40
```

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 *63 : show control-plane transit features* フィールドの説明

フィールド	説明
Total Features Configured	設定された機能の数。
Feature Namef	設定された機能の名前。
Activated	機能が有効化された日時。

関連コマンド

コマンド	説明
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	コントロール プレーン コンフィギュレーション モードを開始します。このモードでは、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更ができます。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-plane hostopen-ports	ポート フィルタ データベースに登録されたオープンなポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。

show cops servers

ルータが設定されているポリシー サーバの IP アドレスと接続ステータスを表示するには、EXEC モードで **showcopsservers** コマンドを使用します。

show cops servers

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 モード

EXEC

コマンド履歴

リリース	変更箇所
12.1(1)T	このコマンドが導入されました。
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。

使用上のガイドライン

show cops server コマンドを使用して、ルータの Common Open Policy Service（COPS）クライアントに関する情報を表示することもできます。

例

次の例では、現在のポリシーサーバとクライアントの情報が表示されます。Client Type の後に整数が表示される場合、1 はリソース予約プロトコル（RSVP）を意味し、2 は差別化サービス プロビジョニングを意味します。（0 はキープアライブを示します。）

```
Router# show cops servers
COPS SERVER: Address: 10.0.0.1. Port: 3288. State: 0. Keepalive: 120 sec
Number of clients: 1. Number of sessions: 1.
 COPS CLIENT: Client type: 1.  State: 0.
```

関連コマンド

Command	Description
showiprsvppolicycops	ポリシー サーバ アドレス、ACL ID、およびルータ サーバ接続の現在の状態を表示します。

show crypto eng qos

IPSec 暗号化エンジンの低遅延キューイング（LLQ）をモニタし、管理するには、特権 EXEC モードで show crypto eng qos コマンドを使用します。

show crypto eng qos

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 モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T で導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS リリース 12(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。

使用上のガイドライン

IPSec 暗号化エンジンの LLQ で QoS が有効になっているかどうかを確認するには、**show crypto eng qos** コマンドを使用します。

例

次の例では、IPSec 暗号化エンジンの LLQ が有効になっているかどうかを確認します。

```
Router# show crypto eng qos
crypto engine name: Multi-ISA Using VAM2
        crypto engine type: hardware
                      slot: 5
                  queuing: enabled
         visible bandwidth: 30000 kbps
                   llq size: 0
    default queue size/max: 0/64
      interface table size: 32
  FastEthernet0/0 (3), iftype 1, ctable size 16, input filter:ip
precedence 5
    class voice (1/3), match ip precedence 5
          bandwidth 500 kbps, max token 100000
          IN  match pkt/byte 0/0, police drop 0
          OUT match pkt/byte 0/0, police drop 0
  class default, match pkt/byte 0/0, qdrop 0
  crypto engine bandwidth:total 30000 kbps, allocated 500 kbps
```

この表示にはフィールドの説明がされています。

show crypto entropy status

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの暗号エントロピーの状態を表示するには、EXEC モードで **show crypto entropy status** コマンドを使用します。

show crypto entropy 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

なし

コマンド モード

EXEC(#)

コマンド履歴

リリース	変更箇所
Cisco IOS XE Release 3.7.3S	このコマンドが、Cisco ASR 1000 シリーズアグリゲーション サービス ルータに導入されました。
Cisco IOS XE Release 3.8S	コマンド出力が Cisco ASR 1000 シリーズ アグリゲーション サービス ルータで変更されました。

例

次は、暗号エントロピーが有効になっている場合の **show crypto entropy status** コマンドの出力例です。

```
Router# show crypto entropy status

# Entropy source       Type Status  Entropy Bits
1 randfill              SW  Working  128(*)
2 getrandombytes        SW  Working  160(*)
3 Nitrox / Octeon       HW  Working  256
(*) - The entropy collected from SW sources were not counted as a part of
      achieving the entropy target!
```

表 64 : 表 1 show crypto entropy status フィールドの説明に、この出力で表示される重要なフィールドについて説明します。

***表 64 : 表 1 show crypto entropy status* フィールドの説明**

フィールド	説明
Entropy source	暗号エントロピーのソース。

フィールド	説明
Type	暗号エントロピーのタイプ。次のいずれかの値を指定できます。 • ソフトウェアがソースの SW エントロピー。 ハードウェアがソースの HW エントロピー。
Status	暗号エントロピーの状態。次のいずれかの値を指定できます。 • Working エントロピーは動作中。 Offline エントロピーはオフライン。
Entropy Bits	暗号エントロピーのサイズ（ビット）

次は、暗号エントロピーが無効になっている場合の **show crypto entropy status** コマンドの出力例です。

```
Router# show crypto entropy status

# Entropy source       Type Status  Entropy Bits
1 randfill              SW  Working  128
2 getrandombytes        SW  Working  160
3 Nitrox / Octeon       HW  Offline   --
```

（注） この表示内のフィールドは、表 64 : 表 1 show crypto entropy status フィールドの説明 で説明されています。

関連コマンド

コマンド	説明
platform ipsec fips-mode	

show frame-relay ip rtp header-compression

フレーム リレー Real-time Transport Protocol（RTP）ヘッダー圧縮統計情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showframe-relayiprtpheader-compression** コマンドを使用します。

show frame-relay ip rtp header-compression [**interface** *type number*] [*dlci*]

構文の説明

interface *type number*	（任意）情報を表示するインターフェイスを指定します。インターフェイスのタイプと番号の間のスペースは任意です。
dlci	（任意）情報を表示するデータ リンク接続識別子（DLCI）を指定します。範囲は 16 ～ 1022 です。

コマンド デフォルト

RTP ヘッダー圧縮が設定されたインターフェイスのすべての DLCI の RTP ヘッダー圧縮統計情報が表示されます。

コマンド モード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更箇所
11.3	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。このコマンドの出力は変更され、フレーム リレー相手先固定接続（PVC）バンドルの RTP ヘッダー圧縮統計情報を表示するようになりました。
12.2(27)SBC	このコマンドが Cisco IOS Release 12.2(27)SBC に統合され、*dlci* 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.4(9)T	*dlci* 引数が追加されました。
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。
12.4(11)T	このコマンドの出力が変更され、フレームリレー相手先固定接続（PVC）バンドルの拡張圧縮 Real-Time Transport Protocol（ECRTP）ヘッダー圧縮統計情報を表示するようになりました。
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。

例

次は、**showframe-relayiprtpheader-compression** コマンドの出力例です。

```
Router# show frame-relay ip rtp header-compression
 DLCI 21         Link/Destination info: ip 10.1.4.1
  Interface Serial3/0 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 20         Link/Destination info: ip 10.1.1.1
  Interface Serial3/1 DLCI 20 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 22         Link/Destination info: ip 10.1.3.1
  Interface Serial3/1 DLCI 22 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

次は、ECRTP が有効になっている場合の **showframe-relayiprtpheader-compression** コマンドの出力例です。

```
Router# show frame-relay ip rtp header-compression
 DLCI 16         Link/Destination info: ip 10.0.0.1
  Interface Serial4/1 DLCI 16 (compression on, IETF, ECRTP)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 16 rx slots, 16 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 16 free contexts
```

次の例では、**showframe-relayiprtpheader-compression** コマンドで DLCI 21 に関する情報を表示します。

```
Router# show frame-relay ip rtp header-compression 21
 DLCI 21         Link/Destination info: ip 10.1.4.1
  Interface Serial3/0 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
```

```
            0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

次の例では、**showframe-relayiprtpheader-compression** コマンドで、シリアルインターフェイス 3/1 のすべての DLCI に関する情報を表示します。

```
Router# show frame-relay ip rtp header-compression interface serial3/1
 DLCI 20         Link/Destination info: ip 10.1.1.1
  Interface Serial3/1 DLCI 20 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 22         Link/Destination info: ip 10.1.3.1
  Interface Serial3/1 DLCI 22 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

次の例では、**showframe-relayiprtpheader-compression** コマンドで、シリアルインターフェイス 3/1 の DLCI 21 のみに関する情報を表示します。

```
Router# show frame-relay ip rtp header-compression interface serial3/1 21
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

次の出力例では、**showframe-relayiprtpheader-compression** コマンドで、MP-3-static という名前の PVC バンドルに関する統計情報を表示します。

```
Router# show frame-relay ip rtp header-compression interface Serial1/4
 vc-bundle MP-3-static      Link/Destination info:ip 10.1.1.1
  Interface Serial1/4:
    Rcvd:   14 total, 13 compressed, 0 errors
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:   15 total, 14 compressed,
```

```
          474 bytes saved, 119 bytes sent
          4.98 efficiency improvement factor
Connect:256 rx slots, 256 tx slots,
          1 long searches, 1 misses 0 collisions, 0 negative cache hits
          93% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

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 *65 : show frame-relay ip rtp header-compression* 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タイプと番号、およびヘッダー圧縮のタイプ。
Rcvd:	受信パケットの詳細情報の表。
total	インターフェイスの受信パケット数。
compressed	圧縮されたヘッダーを持つパケット数
errors	エラー数。
dropped	ドロップされたパケット数
buffer copies	コピーされたバッファの数。
buffer failures	バッファの割り当てに失敗した回数。
Sent:	送信パケットの詳細情報の表。
total	送信されたパケットの合計数。
compressed	圧縮されたヘッダーを持つ送信パケット数
bytes saved	圧縮によって節約できた合計バイト数。
bytes sent	圧縮後に送信された合計バイト数
efficiency improvement factor	圧縮効率。
Connect:	接続の詳細情報の表。
rx slots	受信されたスロットの合計数。
tx slots	送信されたスロットの合計数。
long searches	複数のルックアップが必要だった検索。
misses	作成された新規ステート数。
hit ratio	既存のステートが修正された回数。

フィールド	説明
five minute miss rate	平均ミス レート。
max	最大ミス レート。

関連コマンド

Command	Description
frame-relayiprtpcompression-connections	フレーム リレー インターフェイスの RTP ヘッダー圧縮接続の最大数を指定します。
frame-relayiprtpheader-compression	物理インターフェイス上のすべてのフレームリレーマップについて RTP ヘッダー圧縮をイネーブルにします。
frame-relaymapipcompress	RTP と TCP の両方のヘッダー圧縮をリンクで有効にします。
frame-relaymapipnocompress	RTP と TCP の両方のヘッダー圧縮をリンクで無効にします。
frame-relaymapiprtpheader-compression	DLCI ごとに RTP ヘッダー圧縮を有効にします。
showiprpfevents	RTP ヘッダー圧縮の統計情報を表示します。

show frame-relay ip tcp header-compression

フレーム リレー Transmission Control Protocol（TCP）/IP ヘッダー圧縮統計情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showframe-relayiptcpheader-compression** コマンドを使用します。

show frame-relay ip tcp header-compression [**interface** *type number*] [*dlci*]

構文の説明

interface *type number*	（任意）情報を表示するインターフェイスを指定します。type と number の間のスペースは任意です。
dlci	（任意）情報を表示するデータ リンク接続識別子（DLCI）を指定します。範囲は 16 ～ 1022 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	変更箇所
10.3	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。このコマンドは変更され、フレーム リレー相手先固定接続（PVC）バンドルの RTP ヘッダー圧縮統計情報を表示するようになりました。
12.2(27)SBC	このコマンドが Cisco IOS Release 12.2(27)SBC に統合され、*dlci* 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.4(9)T	*dlci* 引数が追加されました。
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。

例

次は、**showframe-relayiptcpheader-compression** コマンドの出力例です。

```
Router# show frame-relay ip tcp header-compression
DLCI 200          Link/Destination info: ip 10.108.177.200
Interface Serial0:
Rcvd:     40 total, 36 compressed, 0 errors
          0 dropped, 0 buffer copies, 0 buffer failures
Sent:     0 total, 0 compressed
```

```
          0 bytes saved, 0 bytes sent
Connect:  16 rx slots, 16 tx slots, 0 long searches, 0 misses, 0% hit ratio
          Five minute miss rate 0 misses/sec, 0 max misses/sec
```

次の出力例では、**showframe-relayiptcpheader-compression** コマンドで「MP-3-static」という名前の PVC バンドルに関する統計情報を表示します。

```
Router# show frame-relay ip tcp header-compression interface Serial1/4
 vc-bundle MP-3-static      Link/Destination info:ip 10.1.1.1
  Interface Serial1/4:
    Rcvd:   14 total, 13 compressed, 0 errors
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:   15 total, 14 compressed,
             474 bytes saved, 119 bytes sent
             4.98 efficiency improvement factor
    Connect:256 rx slots, 256 tx slots,
             1 long searches, 1 misses 0 collisions, 0 negative cache hits
             93% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

次の例では、**showframe-relayiptcpheader-compression** コマンドで DLCI 21 に関する情報を表示します。

```
Router# show frame-relay ip tcp header-compression 21
DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface POS2/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
DLCI 21         Link/Destination info: ip 10.1.4.1
  Interface Serial3/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

次の出力例では、**showframe-relayiptcpheader-compression** コマンドで、特定のインターフェイスの特定の DLCI を表示します。

```
Router# show frame-relay ip tcp header-compression pos2/0 21
DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface POS2/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

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。

表 *66 : show frame-relay ip tcp header-compression* フィールドの説明

フィールド	説明
Rcvd:	受信パケットの詳細情報の表。
total	受信した圧縮パケットと非圧縮パケットの合計数。
compressed	受信した圧縮パケットの数。
errors	ヘッダー フィールドのエラーが原因のエラー数（バージョン、全体の長さ、または IP チェックサム）。
dropped	廃棄されたパケット数。回線エラー後にのみ発生。
buffer failures	新しいバッファが必要な場合に取得できなかった回数。
Sent:	送信パケットの詳細情報の表。
total	送信した圧縮パケットと非圧縮パケットの合計数。
compressed	送信された圧縮パケットの数。
bytes saved	圧縮によって節約されたバイト数。
bytes sent	送信された実際のバイト数。
Connect:	接続の詳細情報の表。
rx slots、tx slots	1 回の TCP 接続で許可される状態の数。状態は、発信元アドレス、宛先アドレス、および IP ヘッダー長で認識されます。
long searches	着信パケットの接続 ID が処理済みの前回のものと異なる回数。
misses	一致するエントリが接続テーブル内に見つからず、新しいエントリを入力する必要があった回数。
hit ratio	一致するエントリが圧縮テーブル内で見つかり、ヘッダーが圧縮された回数のパーセンテージ。
Five minute miss rate	直近 5 分間で計算されたミス レート、およびこの期間の 1 秒あたりの最大ミス レート。

show interfaces fair-queue

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**showinterfacesfair-queue** コマンドは非表示です。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンド シーケンス）を使用する必要があります。代替コマンドのリストなど詳細については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**showinterfacesfair-queue** コマンドは、モジュラ QoS CLI（MQC）コマンド（または MQC コマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

Versatile Interface Processor（VIP）ベースのインターフェイスの重み付け均等化キューイング（WFQ）に関する詳細と統計情報を表示するには、EXEC モードで **showinterfacesfair-queue** コマンドを使用します。

show interfaces [*type number*] **fair-queue**

構文の説明

type	（任意）インターフェイスのタイプ。
number	（任意）インターフェイスの番号。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
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。

リリース	変更箇所
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

例

次の出力例では、**showinterfacesfair-queue** コマンドで VIP 分散 WFQ（DWFQ）を表示します。

```
Router# show interfaces fair-queue
Hssi0/0/0 queue size 0
        packets output 1417079, drops 2
 WFQ: aggregate queue limit 54, individual queue limit 27
    max available buffers 54

     Class 0: weight 10 limit 27 qsize 0 packets output 1150 drops 0
     Class 1: weight 20 limit 27 qsize 0 packets output 0 drops 0
     Class 2: weight 30 limit 27 qsize 0 packets output 775482 drops 1
     Class 3: weight 40 limit 27 qsize 0 packets output 0 drops 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 *67 : show interfaces fair-queue* フィールドの説明

フィールド	説明
queue size	このインターフェイスの現在の出力キュー サイズ。
packets output	このインタ フェースから送信されるパケット数またはインターフェイスから送信されるこのクラスのパケット数。
drops	ドロップされたパケットの数またはドロップされたこのクラスのパケットの数。
aggregate queue limit	集約制限（パケット数）。
individual queue limit	個別制限（パケット数）。
max available buffers	集約キュー制限（パケット数）に割り当てられた使用可能バッファ スペース。
Class	QoS グループまたはタイプ オブ サービス（ToS）クラス。

フィールド	説明
weight	輻輳期間中にこのクラスに割り当てられた帯域幅のパーセント。
limit	このクラスのキュー制限（パケット数）
qsize	このクラスの現在のキュー サイズ。

関連コマンド

Command	Description
showinterfaces	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。

show interfaces random-detect

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**showinterfacesrandom-detect** コマンドは非表示です。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンド シーケンス）を使用する必要があります。代替コマンドのリストなど詳細については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**showinterfacesrandom-detect** コマンドは、モジュラ QoS CLI（MQC）コマンド（またはMQCコマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

Versatile Interface Processor（VIP）ベースのインターフェイスの重み付けランダム早期検出（WRED）に関する情報を表示するには、EXEC モードで **showinterfacesrandom-detect** コマンドを使用します。

show interfaces [*type number*] **random-detect**

構文の説明

type	（任意）インターフェイスのタイプ。
number	（任意）インターフェイスの番号。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
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。

リリース	変更箇所
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

例

次の出力例では、**showinterfacesrandom-detect** コマンドで VIP 分散 WRED（DWRED）を表示します。

```
Router# show interfaces random-detect
 FastEthernet1/0/0 queue size 0
        packets output 29692, drops 0
 WRED: queue average 0
       weight 1/512
     Precedence 0: 109 min threshold, 218 max threshold, 1/10 mark weight
       1 packets output, drops: 0 random, 0 threshold
     Precedence 1: 122 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 2: 135 min threshold, 218 max threshold, 1/10 mark weight
       14845 packets output, drops: 0 random, 0 threshold
     Precedence 3: 148 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 4: 161 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 5: 174 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 6: 187 min threshold, 218 max threshold, 1/10 mark weight
       14846 packets output, drops: 0 random, 0 threshold
     Precedence 7: 200 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
```

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 *68 : show interfaces random-detect* フィールドの説明

フィールド	説明
queue size	このインターフェイスの現在の出力キュー サイズ。
packets output	このインターフェイスから送信されるパケットの数。
drops	ドロップされたパケットの数
queue average	平均キューの長さ。

フィールド	説明
weight	平均キューの長さの決定に使用する重み係数。
Precedence	このプレシデンスの WRED パラメータ。
min threshold	このプレシデンスの最小しきい値。
max threshold	キューの最大長。平均キューがこの長さの場合、追加のパケットはドロップされます。
mark weight	平均キューが最大しきい値に達したときのパケットがドロップされる確率。
packets output	このプレシデンスが指定された送信済みパケットの数。
random	WRED プロセスによってランダムにドロップされたパケットの数。
threshold	平均キューが最大しきい値長に達したため自動的にドロップされるパケットの数。
(no traffic)	このプレシデンスが指定されたパケットはありません。

関連コマンド

Command	Description
random-detect(interface)	WRED または DWRED をイネーブルにします。
random-detectflow	フローベース WRED をイネーブルにします。
showinterfaces	ルータまたはアクセスサーバで設定されているすべてのインターフェイスの統計情報を表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

show interfaces rate-limit

インターフェイスの専用アクセス レート（CAR）の情報を表示するには、EXEC モードで **showinterfacesrate-limit** コマンドを使用します。

show interfaces [*type number*] **rate-limit**

構文の説明

type	（任意）インターフェイスのタイプ。
number	（任意）インターフェイスの番号。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
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。

例

次に、**showinterfacesrate-limit** コマンドの出力例を示します。

```
Router# show interfaces fddi2/1/0 rate-limit
Fddi2/1/0
 Input
  matches: access-group rate-limit 100
   params: 800000000 bps, 64000 limit, 80000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-continue 1
   exceeded 0 packets, 0 bytes; action: set-prec-continue 0
   last packet: 4737508ms ago, current burst: 0 bytes
   last cleared 01:05:47 ago, conformed 0 bps, exceeded 0 bps
  matches: access-group 101
   params: 80000000 bps, 56000 limit, 72000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 4738036ms ago, current burst: 0 bytes
   last cleared 01:02:05 ago, conformed 0 bps, exceeded 0 bps
  matches: all traffic
   params: 50000000 bps, 48000 limit, 64000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 4738036ms ago, current burst: 0 bytes
   last cleared 01:00:22 ago, conformed 0 bps, exceeded 0 bps
 Output
  matches: all traffic
   params: 80000000 bps, 64000 limit, 80000 extended limit
   conformed 0 packets, 0 bytes; action: transmit
   exceeded 0 packets, 0 bytes; action: drop
```

```
last packet: 4809528ms ago, current burst: 0 bytes
last cleared 00:59:42 ago, conformed 0 bps, exceeded 0 bps
```

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 *69 : show interfaces rate-limit* フィールドの説明

フィールド	説明
Input	これらのレート制限はインターフェイスで受信したパケットに適用されます。
matches	このレート制限に一致するパケット。
params	**rate-limit** コマンドで設定した、このレート制限のパラメータ。
bps	平均レート（ビット/秒）です。
limit	バイト単位の通常バースト サイズ。
extended limit	バイト単位の超過バースト サイズ。
conformed	レート制限に一致したパケットの数。
action	Conform アクション。
exceeded	レート制限を超過したパケットの数。
アクション	Exceed アクション。
last packet	最後のパケットから経過した時間（ミリ秒）。
current burst	現時点のバースト サイズ。
last cleared	**clearcounters** コマンドでバースト カウンタをゼロに戻してから経過した時間。
conformed	一致したトラフィックの割合。
exceeded	超過したトラフィックの割合。
Output	これらのレート制限は、インターフェイスから送信されたパケットに適用されます。

関連コマンド

Command	Description
access-listrate-limit	CAR ポリシーで使用する場合のアクセス リストを設定します。
clearcounters	インターフェイス カウンタをクリアします。
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。
showaccess-lists	現在の IP とレート制限アクセス リストの内容を表示します。

Command	Description
showinterfaces	ルータまたはアクセスサーバで設定されているすべてのインターフェイスの統計情報を表示します。

show iphc-profile

1 つ以上の IP ヘッダー圧縮（IPHC）プロファイルの設定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 **showiphc-profile** コマンドを使用します。

show iphc-profile [*profile-name*]

構文の説明

profile-name	（任意）表示する IPHC プロファイルの名前。

コマンド デフォルト

IPHC プロファイルの名前を指定しない場合は、すべての IPHC プロファイルが表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(9)T	このコマンドが導入されました。
12.4(24)T	このコマンドが変更されました。出力は、EcRTP が設定されている場合に、回復可能な損失を表示するように拡張されました。

使用上のガイドライン

表示に含まれている情報

表示に含まれる情報には、プロファイル タイプ、有効なヘッダー圧縮のタイプ、コンテキストの数、更新間隔（Real-Time Transport [RTP] ヘッダー圧縮の場合）、フィードバック メッセージが無効になっているかどうか、IPHC プロファイルが添付されるインターフェイスなどがあります。

IPHC プロファイルの詳細について

IPHC プロファイルは、ネットワークでのヘッダー圧縮を有効および設定するために使用されます。IPHC プロファイルを使用したヘッダー圧縮の設定の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

例

次は、**showiphc-profile** コマンドの出力例です。出力では、profile19 および profile20 という IPHC プロファイルの情報が表示されています。

```
Router# show iphc-profile
IPHC Profile "profile19"
Type: IETF
  Compressing: NON-TCP (RTP)
  Contexts   : NON-TCP fixed at 0
  Refresh    : NON-TCP every 5 seconds or 256 packets
  EcRTP      : recoverable loss enabled 1
  Controlled interfaces: (0)
  Reference Count:  (1)
```

```
IPHC Profile "profile20"
Type: IETF
  Compressing: NON-TCP (RTP)
  Contexts   : NON-TCP fixed at 0
  Refresh    : NON-TCP every 5 seconds or 256 packets
  EcRTP      : recoverable loss enabled 4 (dynamic)
  Controlled interfaces: (0)
  Reference Count:  (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 *70 : show iphc-profile* フィールドの説明

フィールド	説明
IPHC Profile	IPHC プロファイル名。
Type	IPHC プロファイル タイプ：VJ（van-jacobson の場合）または IETF。
Compressing	TCP、TCP 以外、RTP など使用されたヘッダー圧縮のタイプ。
Contexts	コンテキスト番号の計算に使用されたコンテキストの数および設定。
Refresh	コンテキスト更新間のパケットの最大数または最大時間を示します。
EcRTP	回復可能損失が有効かどうか、および EcRTP 回復可能損失がダイナミックに設定されているかどうかを示します。
Controlled interfaces	IPHC プロファイルが添付されるインターフェイス。
Reference Count	アクティブな IPHC プロファイル サブモードの数を示します。

関連コマンド

コマンド	説明
iphc-profile	IPHCプロファイルを作成します。

show ip nat translations rsvp

リソース予約プロトコル（RSVP）メッセージのアクティブなネットワーク アドレス変換（NAT）を表示するには、特権 EXEC モードで **show ip nat translations rsvp** コマンドを使用します。

show ip nat translations rsvp [**vrf** *vrf-name*]

構文の説明

vrf *vrf-name*	（任意）VPN ルーティングおよび転送（VRF）トラフィック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	変更箇所
15.2(2)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

RSVP パケットに RSVP-NAT アプリケーション レイヤ ゲートウェイ（ALG）によって実行された IP アドレス/ポート変換を表示するには、**show ip nat translations rsvp** コマンドを使用します。

例

次に、**show ip nat translations rsvp** コマンドの出力例を示します。

```
Router# show ip nat translations rsvp

RSVP-NAT-ALG:
 Inside Local: Address: <ip-address>, Port: <port-number>
 Outside Local: Address: <ip-address>, Port: <port-number>
 Inside Global: Address: <ip-address>, Port: <port-number>
 Outside Global: Address: <ip-address>, Port: <port-number>
 L4-Protocol: <protocol-number>
 Local Path Phop: <ip-address>
 Local Resv Phop: <ip-address>
 Local Resv Confirm: <ip-address>
```

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 *71 : show ip nat translations rsvp* フィールドの説明

フィールド	説明
Inside Local	内部ネットワーク上のホストに割り当てられた IP アドレスおよびポート番号（多くの場合ネットワーク インターフェイス カード（NIC）やサービス プロバイダーにより割り当てられた正当なアドレスではありません）。

フィールド	説明
Outside Local	外部ホストが内部ネットワークに出現するときのIPアドレスおよびポート番号（多くの場合NICやサービスプロバイダーにより割り当てられた正当なアドレスではありません）。
Inside Global	1 つ以上の内部のローカル IP アドレスを外部に対して表す正当な IP アドレスおよびポート番号。
Outside Global	外部ネットワーク上のホストに、所有者が割り当てた IP アドレスおよびポート番号。
Address	変換の適切なカテゴリを表す IP アドレス。
Port	変換の適切なカテゴリを表すポート番号。
L4-Protocol	アドレスを識別するポートのレイヤ 4 プロトコル。
Local Path Phop	グローバルからローカルへ Resv メッセージを送信するために使用する前回のローカル ホップのアドレス。
Local Resv Phop	Resv メッセージがローカルからグローバルに着信したときに保存される前回のローカル ホップのアドレス。このアドレスは、Resv エラー メッセージの通過時に使用されます。
Local Resv Confirm	Resv メッセージの処理時に保存されるローカルホップのアドレスで、Resv 確認メッセージの通過に使用されます。

show ip nbar attribute

Network-Based Application Recognition（NBAR）で使用する設定属性を表示するには、特権 EXEC モードで **showipnbarattribute** コマンドを使用します。

show ip nbar attribute [{**application-group** |**business-relevance** |**category** |**encrypted** |**p2p-technology** |**sub-category** |**traffic-class** |**tunnel**}]

show ip nbar attribute *attribute-name attribute-value* [{*attribute-name attribute-value*}]

構文の説明

application-group	（任意）アプリケーション グループ属性を指定します。
business-relevance	（任意）ビジネス関連属性を指定します。
category	（任意）カテゴリ属性を指定します。
encrypted	（任意）暗号化アプリケーションを指定します。
p2p-technology	（任意）P2P アプリケーションを指定します。
sub-category	（任意）サブカテゴリ属性を指定します。
traffic-class	（任意）トラフィック クラス属性を指定します。
tunnel	（任意）トンネル アプリケーションを指定します。
attribute-name	（任意）プロトコル属性の名前。*attribute-value* を指定すると、コマンドには指定した属性値に一致するプロトコルのリストが表示されます。
attribute-value	（任意）*attribute-name* で指定した属性の値。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.4S	このコマンドが導入されました。
Cisco IOS XE Denali 16.4.1	2つの属性/属性値の組み合わせを照合する機能が追加されました。このモードでは、指定した属性の両方に一致するプロトコルのリストが表示されます。

使用上のガイドライン

showipnbarattribute コマンドは、複数のモードで動作します。

- 属性を指定せずに **showipnbarattribute** を実行すると、NBAR で使用するすべての属性のリストが表示されます。

- 属性（application-group、business-relevance、category、encrypted、p2p-technology、sub-category、traffic-class、tunnel）を指定して、**showipnbarattribute** *attribute-name* を実行すると、指定した属性のみ表示されます。
- 1 つまたは 2 つの属性と値を指定して **showipnbarattribute** *attribute-name attribute-value* [*attribute-name attribute-value*] を実行すると、指定した属性値に一致する、ルータにロードされたプロトコルのリストが表示されます。2 つの属性が指定されると、両方に一致するプロトコルのみが表示されます。

  たとえば、次のように「traffic-class voip-telephony」と「business-relevance business-relevant」を指定します。

  ```
  show ip nbar attribute traffic-class voip-telephony business-relevance
  business-relevant
  ```

  この場合、traffic-class の値は voip-telephony で、business-relevance の値は business-relevant のプロトコルのリストが表示されます。

  このリストには、ロードされたプロトコル パックまたはカスタム プロトコルによって定義されたプロトコルが含まれる場合があります。

例

次は、**showipnbarattribute** コマンドの出力例です。属性のリストが表示されます。

```
Router# show ip nbar attribute
      Name :  category
      Help :  category attribute
      Type :  group
    Groups :  email, newsgroup, location-based-services, instant-messaging, netg
      Need :  Mandatory
   Default :  other
      Name :  sub-category
      Help :  sub-category attribute
      Type :  group
    Groups :  routing-protocol, terminal, epayement, remote-access-terminal, nen
      Need :  Mandatory
   Default :  other
      Name :  application-group
      Help :  application-group attribute
      Type :  group
    Groups :  skype-group, wap-group, pop3-group, kerberos-group, tftp-group, bp
      Need :  Mandatory
   Default :  other
      Name :  tunnel
      Help :  Tunnelled applications
      Type :  group
    Groups :  tunnel-no, tunnel-yes, tunnel-unassigned
      Need :  Mandatory
   Default :  tunnel-unassigned
      Name :  encrypted
      Help :  Encrypted applications
      Type :  group
    Groups :  encrypted-yes, encrypted-no, encrypted-unassigned
      Need :  Mandatory
   Default :  encrypted-unassigned
```

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 *72 : show ip nbar attribute* フィールドの説明

フィールド	説明
Name	属性の名前を示します。
Help	属性情報を表示します。
Type	属性のタイプを示します。
Groups	属性内のグループを指定します。
Need	属性の必要性を指定します。
Default	属性のデフォルト状態を表示します。

次は、属性と値が指定されたモードでこのコマンドを使用した場合の出力例です。一致するプロトコルのリストと各プロトコルの説明が表示されます。

```
Router# show ip nbar attribute traffic-class voip-telephony business-relevance
business-relevant
  cisco-collab-audio     Cisco Collaboration Voice by various Cisco unified communication
 clients.
  cisco-jabber-audio     Cisco Jabber Client; Audio Calls and Voice Mail
  cisco-media-audio      Cisco IP Phones and PC-based Unified Communicators
  cisco-phone-audio      Cisco IP Phones and PC-based Unified Communicators; Audio Calls

  citrix-audio           Citrix Audio Traffic
  ms-lync-audio          Skype provides cost effective and collaborative tools for
businesses
  rtp-audio              Real Time Protocol Audio
  telepresence-audio     Telepresentce Voice by various Cisco unified communication
clients.
```

関連コマンド

コマンド	説明
matchprotocolattributeapplication-group	アプリケーション グループに基づいてクラス マップの一致基準を設定します。
matchprotocolattributecategory	カテゴリに基づいてクラス マップの一致基準を設定します。
matchprotocolattributeencrypted	暗号化に基づいてクラス マップの一致基準を設定します。
matchprotocolattributesub-category	サブカテゴリに基づいてクラス マップの一致基準を設定します。
matchprotocolattributetunnel	トンネリングに基づいてクラス マップの一致基準を設定します。

show ip nbar classification auto-learn top-asymmetric-sockets

不明、HTTP および SSL トラフィックの非対称フローを表示するには、特権 EXEC モードで **showipnbarclassificationauto-learntop-asymmetric-sockets** コマンドを使用します。

show ip nbar classification auto-learn top-asymmetric-sockets *number-of-flows*[{**detailed**|**http**|**ssl**|**tcp**|**udp**|**unknown**}]

構文の説明

number-of-flows	表示するフロー数です。範囲：1 ～ 100
detailed	非対称フロー数が 0 のソケットも表示します。
http、**ssl**、**tcp**、**udp**、**unknown**	指定したタイプのソケットのみを含む出力をフィルタします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
Cisco IOS XE Releases 16.3.2 および 16.4.1	このコマンドが導入されました。

使用上のガイドライン

showipnbarclassificationauto-learn top-asymmetric-sockets コマンドは、不明、HTTP、または SSL に分類されたトラフィックの非対称フローを表示します。これは、非対称フローが NBAR2 分類に影響を与えているかどうかを判断する場合に役立つことがあります。

例

次は、**showipnbarclassificationauto-learn top-asymmetric-sockets** コマンドの出力例です。

```
Router# show ip nbar classification auto-learn top-asymmetric-sockets 100
Total tracked flows:               19.609 K
Asymmetric tracked flows:          19.609 K  (100%)
           Unknown TCP  asymmetric flows:         19.609 K (100%)
           Unknown UDP  asymmetric flows:          0       (0%)
          Generic HTTP asymmetric flows:         4.559 K (23%) -> percent are calculated
 from the total tracked flows.
           Generic SSL  asymmetric flows:         60       (0%)
DNS: Response without request (blocked by DNS guard): 100%

Asymmetric Tracked Flows Per Socket:
---|---------------
|--------|-----|---------------|---------|-----------|----|--------------|----|
#  |IP (*)          |Vrf name|Port |Classification |Transport|Asymmetric |Asym|Total
      |Host|
   |                |        |     |               |         |Flows      |%   |Flows
      |    |
---|---------------
|--------|-----|---------------|---------|-----------|----|--------------|----|
1  |171.71.196.84   |global  |4282 |unknown        |TCP      |  8.994 K  |100%|  8.994
K     |N/A |
2  |173.36.9.202    |global  |4282 |unknown        |TCP      |  2.998 K  |100%|  2.998
K     |N/A |
```

```
3  |171.71.196.85   |global  |4282 |unknown        |TCP      |  2.998 K  |100%|  2.998
K     |N/A |
4  |74.125.71.148   |global  |80   |http           |TCP      |600        |100%|600
      |N/A |
5  |54.246.114.214  |global  |80   |http           |TCP      |120        |100%|120
      |N/A |
6  |54.246.114.211  |global  |80   |http           |TCP      |120        |100%|120
      |N/A |
7  |54.246.114.212  |global  |80   |http           |TCP      |120        |100%|120
      |N/A |
8  |54.246.114.215  |global  |80   |http           |TCP      |120        |100%|120
      |N/A |
9  |54.246.114.213  |global  |80   |http           |TCP      |120        |100%|120
      |N/A |
10 |20.20.20.4      |global  |80   |http           |TCP      | 90        |100%| 90
      |N/A |
11 |20.20.20.8      |global  |80   |http           |TCP      | 90        |100%| 90
      |N/A |
12 |20.20.20.3      |global  |80   |http           |TCP      | 90        |100%| 90
      |N/A |
13 |20.20.20.15     |global  |80   |http           |TCP      | 90        |100%| 90
      |N/A |
```

次は、**showipnbarclassificationauto-learn top-asymmetric-sockets** コマンドの出力例です。HTTP ソケットのみをフィルタするため、**http** キーワードを追加しています。Classification 列には「http」ソケットのみが表示されることに注意してください。

```
Router# show ip nbar classification auto-learn top-asymmetric-sockets 100 http
Total tracked flows:               24.912 M
Asymmetric tracked flows:          24.555 M  (98%)
           Unknown TCP  asymmetric flows:         19.934 M (80%)
           Unknown UDP  asymmetric flows:          4.620 M (18%)
           Generic HTTP asymmetric flows:          1.775 M (7%)
           Generic SSL  asymmetric flows:         17.405 M (69%)
DNS: Response without request (blocked by DNS guard): 3%


Asymmetric Tracked Flows Per Socket:
---|-----------------
|--------|-----|---------------|---------|-----------|----|----------|---------------|
#  |IP (*)            |Vrf name|Port |Classification |Transport|Asymmetric |Asym|Total
    |Host           |
   |                  |        |     |               |         |Flows      |%   |Flows
    |               |
---|-----------------
|--------|-----|---------------|---------|-----------|----|----------|---------------|
1  |10.42.9.30        |global  |80   |http           |TCP      |563.666 K  |100%|563.666
 K |N/A            |
2  |10.42.7.65        |global  |80   |http           |TCP      |446.010 K  |100%|446.010
 K |N/A            |
3  |10.42.23.213      |global  |80   |http           |TCP      |280.411 K  |100%|280.411
 K |N/A            |
4  |10.194.30.208     |global  |80   |http           |TCP      |163.195 K  |100%|163.195
 K |10.10.10.10    |
5  |10.42.5.71        |global  |80   |http           |TCP      | 57.136 K  |100%| 57.136
 K |N/A            |
6  |10.42.5.200       |global  |80   |http           |TCP      | 56.170 K  |100%| 56.170
 K |N/A            |
7  |172.19.137.134    |global  |80   |http           |TCP      | 49.931 K  |100%| 49.931
 K |test-test-test2|
8  |74.125.28.121     |global  |80   |http           |TCP      | 19.517 K  |100%| 19.517
 K |ip.kuku.com    |
```

```
9  |10.42.4.56        |global  |80   |http           |TCP      | 16.561 K  |100%| 16.561
 K |N/A            |
10 |10.34.161.43      |global  |80   |http           |TCP      | 15.036 K  |100%| 15.036
 K |10.34.161.43   |
11 |10.42.9.27        |global  |80   |http           |TCP      | 13.414 K  |100%| 13.414
 K |N/A            |
12 |10.35.45.42       |global  |80   |http           |TCP      |  6.169 K  |100%|  6.169
 K |N/A            |
13 |10.42.1.64        |global  |80   |http           |TCP      |  3.323 K  |100%|  3.323
 K |N/A            |
14 |10.42.38.81       |global  |80   |http           |TCP      |  3.100 K  |100%|  3.100
 K |N/A            |
15 |10.35.33.15       |global  |80   |http           |TCP      |  3.099 K  |98 %|  3.147
 K |N/A            |
16 |10.42.28.115      |global  |8081 |http           |TCP      |  3.047 K  |100%|  3.047
 K |N/A            |
17 |10.42.28.59       |global  |8081 |http           |TCP      |  2.993 K  |100%|  2.993
 K |N/A            |
18 |10.42.1.10        |global  |80   |http           |TCP      |  2.804 K  |100%|  2.804
 K |N/A            |
19 |10.42.28.59       |global  |80   |http           |TCP      |  2.472 K  |100%|  2.472
 K |N/A            |
20 |10.42.28.115      |global  |80   |http           |TCP      |  2.411 K  |100%|  2.411
 K |N/A            |
```

show ip nbar link-age

Network-Based Application Recognition（NBAR）ごとにプロトコルのリンク期限を表示するには、特権 EXEC モードで **showipnbarlink-age** コマンドを使用します。

show ip nbar link-age [*protocol-name*]

構文の説明

protocol-name	（任意）指定されたプロトコル名のリンク期限のみ表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(20)T	このコマンドが導入されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

showipnbarlink-age コマンドは、すべての NBAR プロトコルのリンク期限を表示します。特定のプロトコルの表示を制限するには、*protocol-name* 引数を使用します。

例

次は、**showipnbarlink-age** コマンドの出力例です。

```
Router# show ip nbar link-age

System Link Age: 30 seconds
No.  Protocol                  Link Age (seconds)
1    skype                        120
2  bittorrent                     120
3  winmx                          120
```

次は、特定のプロトコルについて表示する **showipnbarlink-age** コマンドの出力例です。

```
Router# show ip nbar link-age
 eigrp
System Link Age: 30 seconds
Protocol                  Link Age (seconds)
eigrp                        120
```

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 *73 : show ip nbar link-age* フィールドの説明

フィールド	説明
No.	表示するプロトコル リストのシリアル番号です。
Protocol	NBAR プロトコルの名前です。

フィールド	説明
Link Age (seconds)	プロトコルのリンクが期限切れになる時間（秒）です。

関連コマンド

コマンド	説明
ipnbarresourcesprotocol	プロトコル ベースで、NBAR フロー リンク テーブルの有効期限を設定します。

show ip nbar classification auto-learn top-hosts

ジェネリックとして分類されたネットワーク トラフィックの上位ホストを示す Network Based Application Recognition（NBAR）の機能を有効にするには、**ip nbar classification auto-learn top-hosts** コマンドを使用します。

show ip nbar custom auto-learn top-hosts *number-of-hosts* ［**details**］

構文の説明

number-of-hosts	上位ホストを自動学習するサンプル レートを設定します。
details	汎用に分類されたトップ ホストの統計情報とデータベース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	変更箇所
15.5(2)T	このコマンドが導入されました。

例

次の例では、ネットワーク トラフィックの汎用に分類されたトップ ホストの統計情報とデータベースを表示します。

```
Device> show ip nbar classification auto-learn top-hosts 100
```

関連コマンド

コマンド	説明
ipnbarclassificationauto-learntop-hosts	ジェネリックとして分類されたネットワーク トラフィックの上位ホストの統計およびデータベースを示す NBAR の機能を有効にします。
clearipnbarclassificationauto-learntop-hosts	ジェネリックとして分類されたネットワーク トラフィックの上位ホストの統計情報およびデータベースの表示をクリアします。

show ip nbar classification granularity

現在設定されている Network Based Application Recognition（NBAR）分類モードを表示するには、特権 EXEC モードで **show ip nbar classificationgranularity** コマンドを使用します。

show ip nbar classification granularity protocol *protocol-name*

構文の説明

protocol *protocol-name*	アプリケーションを示す指定されたプロトコルに対して、細粒分類を強制します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.14S	このコマンドが導入されました。
15.5(1)T	このコマンドが、15.5(1)T に統合されました。
15.5(2)T	このコマンドが変更されました。**protocol** *protocol-name* のキーワードと引数のペアが追加されました。
Cisco IOS XE Release 3.15S	このコマンドが、Cisco IOS XE Release 3.15S に統合されました。

例

次は、**show ip nbar granularity** コマンドの出力例です。この例では、現在設定されている NBAR 分類モード（粗粒）が表示されます。

```
Device#  show ip nbar classification granularity

NBAR classification granularity mode: coarse-grain
```

次は、**show ip nbar granularity** コマンドの出力例です。この例では、3pc プロトコルが細粒分類に強制設定されます。

```
Device# show ip nbar classification granularity protocol 3pc

Protocol                  Force mode
--------------------------------------
3pc                       fine-grain
```

関連コマンド

コマンド	説明
ipnbarclassificationgranularity	分類モード（細粒または粗粒）を NBAR に設定します。

show ip nbar pdlm

Network-Based Application Recognition（NBAR）で使用する Packet Description Language Module（PDLM）を表示するには、特権 EXEC モードで **showipnbarpdlm** コマンドを使用します。

show ip nbar pdlm

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.1(13)E	このコマンドが、FlexWAN モジュールを備えていない Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
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。

使用上のガイドライン

ipnbarpdlm コマンドで NBAR にロードしたすべての PDLM のリストを表示するには、このコマンドを使用します。

例

この例では、**showipnbarpdlm** コマンドで、citrix.pdlm PDLM をフラッシュ メモリからロードします。

```
Router# show ip nbar pdlm

The following PDLMs have been loaded:
flash://citrix.pdlm
```

関連コマンド

コマンド	説明
ipnbarpdlm	シスコが提供する PDLM によって、NBAR が認識するプロトコルのリストを拡張および強化します。

show ip nbar port-map

このコマンドは廃止されました。

Network-Based Application Recognition（NBAR）で使用する現在のプロトコルからポートへのマッピングを表示するには、特権EXECモードで**showipnbarport-map**コマンドを使用します。

show ip nbar port-map [*protocol-name* [*protocol-type*]]

構文の説明

protocol-name	（任意）プロトコルの名前。使用可能なプロトコルの詳細については、疑問符（?）オンライン ヘルプ機能を使用してください。
protocol-type	（任意）プロトコルのタイプ。2 つのタイプのプロトコルを指定できます。 • **tcp**：Transmission Control Protocol（TCP）ポートに関する情報を表示します。 • **udp**：User Datagram Protocol（UDP）ポート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	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(13)E	このコマンドがCatalyst 6000 ファミリ スイッチに実装されました。FlexWAN モジュールが削除されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
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。
12.4(22)T	このコマンドが Cisco IOS Release 12.4(22)T に統合されました。
15.1(3)T	このコマンドが Cisco IOS Release 15.1(3)T に統合されました。
Cisco IOS XE Release 3.10S	このコマンドは廃止されました。

使用上のガイドライン

showipnbarport-map コマンドは、NBAR プロトコルのポート割り当てを表示します。

NBAR で使用する現在のプロトコルからポートへのマッピングを表示するには、**showipnbarport-map** コマンドを使用します。**ipnbarport-map** コマンドを使用すると、**showipnbarport-map** コマンドでは、プロトコルに割り当てたポートが表示されます。プロトコルの設定に **ipnbarport-map** コマンドを使用しないと、**showipnbarport-map** コマンドでは、デフォルトのポートが表示されます。特定のプロトコルの表示を制限するには、*protocol-name* 引数を使用します。*protocol-type* 引数タイプには、UDP または TCP を使用できます。

例

次は、**showipnbarport-map** コマンドの出力例です。

```
Router# show ip nbar port-map
port-map    cuseeme    udp    7648    7649    24032
port-map    cuseeme    tcp    7648    7649
port-map    dhcp       udp    67      68
port-map    dhcp       tcp    67      68
```

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 *74 : show ip route track-table* フィールドの説明

フィールド	説明
port-map	割り当てられたポートを示します。
cuseeme	CU-SeeMe プロトコルが使用されていることを示します。
udp	User Datagram Protocol タイプが使用されていることを示します。
tcp	Transmission Control Protocol タイプが使用されていることを示します。
dhcp	Dynamic Host Configuration Protocol タイプが使用されていることを示します。

関連コマンド

コマンド	説明
ipnbarport-map	ウェルノウン ポート番号以外のポート番号を使用して、プロトコルまたはプロトコル名を検索するように NBAR を設定します。

show ip nbar protocol activated

デバイスのアクティブ化された Network-Based Application Recognition（NBAR）プロトコルをすべて表示するには、特権 EXEC モードで **show ip nbar protocol activated** コマンドを使用します。

show ip nbar protocol activated

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.2(4)M	このコマンドが導入されました。

使用上のガイドライン

デバッグには NBAR を有効にする必要があります。

例

次は、**show ip nbar protocol activated** コマンドの出力例です。

```
Device# show ip nbar protocol activated

Following Protocol are enabled
 Feature:PD
       Hwidb:Ethernet0/0 MI:1 SI:0 FR:0 PVC:0
All iana protocols
```

次の表で、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ています。

表 *75 : show ip nbar protocol activated* フィールドの説明

フィールド	説明
Hwidb	設定されたハードウェア IDB を表示します。
MT1	設定されたメインインターフェイスを表示します。
SI	設定されたサブインターフェイスを表示します。
FR	設定されたフレーム リレーを表示します。
PVC	設定された ATM PVC を表示します。

show ip nbar protocol-attribute

Network-Based Application Recognition（NBAR）で使用するプロトコル属性を表示するには、特権 EXEC モードで **showipnbarprotocol-attribute** コマンドを使用します。

show ip nbar protocol-attribute [*protocol-name*]

構文の説明

protocol-name	（任意）属性を表示するプロトコルの名前です。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.4S	このコマンドが導入されました。

使用上のガイドライン

すべてのプロトコルの属性を表示するには、**showipnbarprotocol-attribute** コマンドを使用します。特定のプロトコルの属性を表示するには、プロトコル名を指定します。

例

次は、**showipnbarprotocol-attribute** コマンドの出力例です。出力にはフィールドの説明も表示されます。

```
Router# show ip nbar protocol-attribute ospf
    Protocol Name :  ospf
                category :  net-admin
            sub-category :  routing-protocol
       application-group :  other
                  tunnel :  tunnel-no
               encrypted :  encrypted-no

Router# show ip nbar protocol-attribute
           Protocol Name :  ftp
                category :  file-sharing
            sub-category :  client-server
       application-group :  ftp-group
                  tunnel :  tunnel-no
               encrypted :  encrypted-no

           Protocol Name :  http
                category :  browsing
            sub-category :  other
       application-group :  other
                  tunnel :  tunnel-no
               encrypted :  encrypted-no

           Protocol Name :  egp
                category :  net-admin
            sub-category :  routing-protocol
       application-group :  other
                  tunnel :  tunnel-no
               encrypted :  encrypted-no
```

```
    Protocol Name :  gre
         category :  net-admin
     sub-category :  tunneling-protocols
application-group :  other
           tunnel :  tunnel-yes
        encrypted :  encrypted-no

    Protocol Name :  icmp
         category :  net-admin
     sub-category :  network-management
application-group :  other
           tunnel :  tunnel-no
        encrypted :  encrypted-no

    Protocol Name :  eigrp
         category :  net-admin
     sub-category :  routing-protocol
application-group :  other
           tunnel :  tunnel-no
        encrypted :  encrypted-no
```

関連コマンド

コマンド	説明
matchprotocolattributeapplication-group	アプリケーション グループに基づいてクラス マップの一致基準を設定します。
matchprotocolattributecategory	カテゴリに基づいてクラス マップの一致基準を設定します。
matchprotocolattributeencrypted	暗号化に基づいてクラス マップの一致基準を設定します。
matchprotocolattributesub-category	サブカテゴリに基づいてクラス マップの一致基準を設定します。
matchprotocolattributetunnel	トンネリングに基づいてクラス マップの一致基準を設定します。

show ip nbar protocol-discovery

Network-Based Application Recognition（NBAR）Protocol Discovery 機能で収集された統計情報を表示するには、**showipnbarprotocol-discoverycommandinprivilegedEXEC**モードを使用します。

show ip nbar protocol-discovery [**interface** *type number*] [**stats** {**byte-count**|**bit-rate**|**packet-count**|**max-bit-rate**}] [**protocol** *protocol-name*] [**top-n** *number*]

構文の説明

interface	（任意）このインターフェイスの Protocol Discovery 統計情報が表示されることを示します。
type	ポリシー設定が表示されるサブインターフェイスのインターフェイス タイプ。
number	ポート、コネクタ、VLAN、またはインターフェイス カードの番号です。
stats	（任意）バイト カウント、バイト レート、またはパケット カウントが表示されることを示します。
byte-count	（任意）バイト カウントが表示されることを示します。
max-bit-rate	（任意）最大ビット レートが表示されることを示します。
packet-count	（任意）パケット カウントが表示されることを示します。
protocol	（任意）特定のプロトコルの統計情報が表示されることを示します。
protocol-name	（任意）統計情報を表示するユーザ指定のプロトコル名です。
top-n	（任意）top-n が表示されることを示します。top-n はアクティブな NBAR サポート プロトコルのなかの上位プロトコル数です。n は表示するプロトコル数を表します。たとえば、top-n 3 と入力すると、アクティブな NBAR サポート プロトコルの上位 3 つが表示されます。
number	（任意）表示するアクティブな NBAR サポート プロトコルの上位の数を指定します。

コマンド デフォルト

NBAR Protocol Discovery 機能が有効になっているすべてのインターフェイスの統計情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。

リリース	変更箇所
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.1(13)E	このコマンドが、FlexWAN モジュールを備えていない Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
12.3(7)T	このコマンド出力が変更され、最大ビット レートが追加されました。
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。
12.2(18)ZYA	このコマンドが、Cisco IOS Release 12.2(18)ZYA に統合されました。このコマンドが変更され、VLAN に関する情報表示（必要に応じて）、およびレイヤ 2 とレイヤ 3 両方の EtherChannel のサポート（Catalyst スイッチのみ）が追加されました。
15.1(3)T	このコマンドが Cisco IOS Release 15.1(3)T に統合されました。

使用上のガイドライン

NBAR Protocol Discovery 機能で収集した統計情報を表示するには、**showipnbarprotocol-discovery** コマンドを使用します。このコマンドのデフォルトでは、Protocol Discovery が現在有効になっているすべてのインターフェイスの統計情報を表示します。デフォルトの出力では、入力ビットレート（bps）、入力バイトカウント、入力パケットカウント、およびプロトコル名が、この順番で表示されます。

プロトコルディスカバリは、入力トラフィックと出力トラフィックの両方をモニタするために使用でき、有効なサービス ポリシーがあってもなくても適用できます。NBAR Protocol Discovery によって、出力インターフェイスへスイッチされたパケットの統計情報が収集されます。パケットはさまざまな理由（出力インターフェイス、アクセス リスト、またはキュー ドロップでのポリシングなど）でスイッチング後にドロップされた可能性があるため、これらの統計情報は、出力インターフェイスのルータから出たパケットに関するものとは限りません。

レイヤ 2/3 Etherchannel サポート

Cisco IOS Release 12.2(18)ZYA は、Supervisor 32/Programmable Intelligent Services Accelerator（PISA）搭載の Cisco 6500 シリーズ スイッチ用に設計されているため、**showipnbarprotocol-discovery** コマンドは、レイヤ 2 およびレイヤ 3 EtherChannel の両方でサポートされます。

例

次の例では、イーサネット インターフェイスのアクティブなプロトコルの上位 5 つについて、**showipnbarprotocol-discovery** コマンドの出力を表示する例を示します。

```
Router# show ip nbar protocol-discovery top-n 5

 Ethernet2/0
                              Input                     Output
```

```
                                -----                    ------
  Protocol                      Packet Count             Packet Count
                                Byte Count               Byte Count
                                30sec Bit Rate (bps)     30sec Bit Rate (bps)
                                30sec Max Bit Rate (bps) 30sec Max Bit Rate (bps)
--------------------------- ----------------------- -----------------------
   rtp                          3272685                  3272685
                                                242050604                242050604

                                768000                   768000
                                2002000                  2002000
   gnutella                     513574                   513574
                                118779716                118779716
                                383000                   383000
                                987000                   987000
   ftp                          482183                   482183
                                37606237                 37606237
                                121000                   121000
                                312000                   312000
   http                         144709                   144709
                                32351383                 32351383
                                105000                   105000
                                269000                   269000
   netbios                      96606                    96606
                                10627650                 10627650
                                36000                    36000
                                88000                    88000
   unknown                      1724428                  1724428
                                534038683                534038683
                                2754000                  2754000
                                4405000                  4405000
   Total                        6298724                  6298724
                                989303872                989303872
                                4213000                  4213000
                                8177000                  8177000
```

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 *76 : show ip nbar protocol-discovery* 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タイプと番号です。
Input	インターフェイスの着信トラフィックです。
Output	インターフェイスの発信トラフィックです。
Protocol	使用されているプロトコルです。unknown は、何らかの理由で NBAR が分類できなかったプロトコルすべての合計です。
Packet Count	インターフェイスで送受信されるパケットの数です。
Byte Count	インターフェイスで送受信されるバイト数です。
30sec Bit Rate	Protocol Discovery 有効化後のビット/秒（bps）単位でのプロトコルごとのビット レートの平均値です（直近 30 秒間）。

フィールド	説明
30sec Max Bit Rate	Protocol Discovery 有効化後のビット/秒（bps）単位でのプロトコルごとのビット レートの最大値です（直近 30 秒間）。
Total	入出力トラフィックの合計です。

関連コマンド

コマンド	説明
ipnbarprotocol-discovery	特定のインターフェイス上で NBAR が認識するすべてのプロトコルについて、トラフィックを検出するように NBAR を設定します。

show ip nbar protocol-id

Network Based Application Recognition（NBAR）プロトコル ID の情報を表示するには、特権 EXEC モードで **showipnbarprotocol-id** コマンドを使用します。

show ip nbar protocol-id [*protocol-name*]

構文の説明

protocol-name	（任意）プロトコルの名前。

コマンド デフォルト

オプションの引数を指定しないと、すべてのプロトコルの NBAR プロトコル ID が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.0(1)M	このコマンドが導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.1(1)S	このコマンドが、Cisco IOS Release 15.1(1)S に統合されました。
Cisco IOS Release XE 3.2S	このコマンドが変更されました。追加 IANA プロトコルのサポートが追加されました。

例

次は、**showipnbarprotocol-id** コマンドの出力例です。

```
Router# show ip nbar protocol-id
Protocol Name              id             type
-----------------------------------------------
ftp                        2           Standard
http                       3           Standard
egp                        8           L3 IANA
gre                        47          L3 IANA
icmp                       1           L3 IANA
eigrp                      88          L3 IANA
ipinip                     4           L3 IANA
ipsec                      9           Standard
ospf                       89          L3 IANA
bgp                        179         L4 IANA
cuseeme                    12          Standard
dhcp                       13          Standard
finger                     79          L4 IANA
gopher                     70          L4 IANA
secure-http                16          Standard
imap                       17          Standard
secure-imap                18          Standard
irc                        194         L4 IANA
secure-irc                 994         L4 IANA
kerberos                   21          Standard
```

```
l2tp                      1701         L4 IANA
ldap                      389         L4 IANA
secure-ldap               636         L4 IANA
sqlserver                 1433         L4 IANA
netbios                   26          Standard
nfs                       2049         L4 IANA
nntp                      28          Standard
secure-nntp               563         L4 IANA
notes                     1352         L4 IANA
ntp                       123         L4 IANA
pcanywhere                32          Standard
pop3                      110         L4 IANA
secure-pop3               995         L4 IANA
pptp                      1723         L4 IANA
rip                       520         L4 IANA
rsvp                      37          Standard
snmp                      38          Standard
socks                     39          Standard
ssh                       22          L4 IANA
syslog                    41          Standard
telnet                    23          L4 IANA
secure-telnet             992         L4 IANA
secure-ftp                990         L4 IANA
xwindows                  45          Standard
printer                   515         L4 IANA
novadigm                  47          Standard
tftp                      48          Standard
exchange                  49          Standard
vdolive                   50          Standard
sqlnet                    51          Standard
rcmd                      52          Standard
netshow                   53          Standard
sunrpc                    54          Standard
streamwork                55          Standard
citrix                    56          Standard
fasttrack                 57          Standard
gnutella                  58          Standard
kazaa2                    59          Standard
rtsp                      60          Standard
rtp                       61          Standard
mgcp                      62          Standard
skinny                    63          Standard
h323                      64          Standard
sip                       65          Standard
rtcp                      66          Standard
winmx                     68          Standard
bittorrent                69          Standard
directconnect             70          Standard
smtp                      71          Standard
dns                       72          Standard
hl7                       73          Standard
fix                       74          Standard
msn-messenger             75          Standard
dicom                     76          Standard
yahoo-messenger           77          Standard
mapi                      78          Standard
aol-messenger             79          Standard
cifs                      80          Standard
cisco-phone               81          Standard
youtube                   82          Standard
skype                     83          Standard
sap                       84          Standard
blizwow                   85          Standard
whois++                   63          L4 IANA
```

```
klogin                      543         L4 IANA
kshell                      544         L4 IANA
ora-srv                     1525         L4 IANA
sqlexec                     9088         L4 IANA
clearcase                   371         L4 IANA
appleqtc                    458         L4 IANA
rcp                         469         L4 IANA
isakmp                      500         L4 IANA
ibm-db2                     523         L4 IANA
lockd                       4045         L4 IANA
npp                         92          L4 IANA
microsoftds                 98          Standard
doom                        666         L4 IANA
vnc                         100         Standard
echo                        7           L4 IANA
systat                      11          L4 IANA
daytime                     13          L4 IANA
chargen                     19          L4 IANA
time                        37          L4 IANA
isi-gl                      55          L4 IANA
rtelnet                     107         L4 IANA
server-ipx                  213         L4 IANA
xdmcp                       177         L4 IANA
nicname                     43          L4 IANA
corba-iiop                  111         Standard
tacacs                      112         Standard
telepresence-media          113         Standard
telepresence-control        114         Standard
edonkey                     243         Custom
custom-10                   244         Custom
custom-09                   245         Custom
custom-08                   246         Custom
custom-07                   247         Custom
custom-06                   248         Custom
custom-05                   249         Custom
custom-04                   250         Custom
custom-03                   251         Custom
custom-02                   252         Custom
custom-01                   253         Custom
mftp                        349         L4 IANA
matip-type-a                350         L4 IANA
matip-type-b                351         L4 IANA
dtag-ste-sb                 352         L4 IANA
ndsauth                     353         L4 IANA
datex-asn                   355         L4 IANA
cloanto-net-1               356         L4 IANA
bhevent                     357         L4 IANA
shrinkwrap                  358         L4 IANA
nsrmp                       359         L4 IANA
scoi2odialog                360         L4 IANA
semantix                    361         L4 IANA
srssend                     362         L4 IANA
rsvp_tunnel                 363         L4 IANA
aurora-cmgr                 364         L4 IANA
dtk                         365         L4 IANA
odmr                        366         L4 IANA
mortgageware                367         L4 IANA
qbikgdp                     368         L4 IANA
rpc2portmap                 369         L4 IANA
codaauth2                   370         L4 IANA
ulistproc                   372         L4 IANA
legent-1                    373         L4 IANA
legent-2                    374         L4 IANA
hassle                      375         L4 IANA
```

```
tnETOS                    377         L4 IANA
is99c                     379         L4 IANA
is99s                     380         L4 IANA
hp-collector              381         L4 IANA
hp-managed-node           382         L4 IANA
hp-alarm-mgr              383         L4 IANA
arns                      384         L4 IANA
ibm-app                   385         L4 IANA
asa                       386         L4 IANA
aurp                      387         L4 IANA
unidata-ldm               388         L4 IANA
fatserv                   347         L4 IANA
uis                       390         L4 IANA
synotics-relay            391         L4 IANA
synotics-broker           392         L4 IANA
meta5                     393         L4 IANA
embl-ndt                  394         L4 IANA
netware-ip                396         L4 IANA
mptn                      397         L4 IANA
kryptolan                 398         L4 IANA
iso-tsap-c2               399         L4 IANA
ups                       401         L4 IANA
genie                     402         L4 IANA
decap                     403         L4 IANA
nced                      404         L4 IANA
ncld                      405         L4 IANA
imsp                      406         L4 IANA
timbuktu                  407         L4 IANA
prm-sm                    408         L4 IANA
prm-nm                    409         L4 IANA
decladebug                410         L4 IANA
rmt                       411         L4 IANA
synoptics-trap            412         L4 IANA
smsp                      413         L4 IANA
infoseek                  414         L4 IANA
bnet                      415         L4 IANA
onmux                     417         L4 IANA
hyper-g                   418         L4 IANA
ariel1                    419         L4 IANA
ariel2                    421         L4 IANA
ariel3                    422         L4 IANA
opc-job-start             423         L4 IANA
opc-job-track             424         L4 IANA
smartsdp                  426         L4 IANA
svrloc                    427         L4 IANA
ocs_cmu                   428         L4 IANA
ocs_amu                   429         L4 IANA
utmpsd                    430         L4 IANA
utmpcd                    431         L4 IANA
iasd                      432         L4 IANA
nnsp                      433         L4 IANA
mobileip-agent            434         L4 IANA
mobilip-mn                435         L4 IANA
dna-cml                   436         L4 IANA
comscm                    437         L4 IANA
dsfgw                     438         L4 IANA
dasp                      439         L4 IANA
sgcp                      440         L4 IANA
decvms-sysmgt             441         L4 IANA
cvc_hostd                 442         L4 IANA
snpp                      444         L4 IANA
ddm-rdb                   446         L4 IANA
ddm-dfm                   447         L4 IANA
ddm-ssl                   448         L4 IANA
```

```
as-servermap              449         L4 IANA
tserver                   450         L4 IANA
sfs-smp-net               451         L4 IANA
sfs-config                452         L4 IANA
creativeserver            453         L4 IANA
contentserver             3365         L4 IANA
creativepartnr            455         L4 IANA
scohelp                   457         L4 IANA
skronk                    460         L4 IANA
datasurfsrv               461         L4 IANA
datasurfsrvsec            462         L4 IANA
alpes                     463         L4 IANA
kpasswd                   464         L4 IANA
digital-vrc               466         L4 IANA
mylex-mapd                467         L4 IANA
photuris                  468         L4 IANA
scx-proxy                 470         L4 IANA
mondex                    471         L4 IANA
ljk-login                 472         L4 IANA
hybrid-pop                473         L4 IANA
tn-tl-fd1                 476         L4 IANA
ss7ns                     477         L4 IANA
spsc                      478         L4 IANA
iafserver                 479         L4 IANA
iafdbase                  480         L4 IANA
bgs-nsi                   482         L4 IANA
ulpnet                    483         L4 IANA
integra-sme               484         L4 IANA
powerburst                485         L4 IANA
avian                     486         L4 IANA
saft                      487         L4 IANA
gss-http                  488         L4 IANA
nest-protocol             489         L4 IANA
micom-pfs                 490         L4 IANA
go-login                  491         L4 IANA
ticf-1                    492         L4 IANA
ticf-2                    493         L4 IANA
pov-ray                   494         L4 IANA
intecourier               495         L4 IANA
pim-rp-disc               496         L4 IANA
dantz                     497         L4 IANA
siam                      498         L4 IANA
iso-ill                   499         L4 IANA
stmf                      501         L4 IANA
asa-appl-proto            502         L4 IANA
intrinsa                  503         L4 IANA
mailbox-lm                505         L4 IANA
ohimsrv                   506         L4 IANA
crs                       507         L4 IANA
xvttp                     508         L4 IANA
snare                     509         L4 IANA
fcp                       510         L4 IANA
passgo                    511         L4 IANA
exec                      512         L4 IANA
shell                     430         Standard
videotex                  516         L4 IANA
talk                      517         L4 IANA
ntalk                     518         L4 IANA
utime                     519         L4 IANA
ripng                     521         L4 IANA
ulp                       522         L4 IANA
pdap                      344         L4 IANA
ncp                       524         L4 IANA
timed                     525         L4 IANA
```

```
tempo                    526         L4 IANA
stx                      527         L4 IANA
custix                   528         L4 IANA
irc-serv                 529         L4 IANA
courier                  530         L4 IANA
conference               531         L4 IANA
netnews                  532         L4 IANA
netwall                  533         L4 IANA
iiop                     535         L4 IANA
opalis-rdv               536         L4 IANA
nmsp                     537         L4 IANA
gdomap                   538         L4 IANA
apertus-ldp              539         L4 IANA
uucp                     540         L4 IANA
uucp-rlogin              541         L4 IANA
commerce                 542         L4 IANA
appleqtcsrvr             545         L4 IANA
dhcpv6-client            546         L4 IANA
dhcpv6-server            547         L4 IANA
idfp                     549         L4 IANA
new-rwho                 550         L4 IANA
cybercash                551         L4 IANA
pirp                     553         L4 IANA
remotefs                 556         L4 IANA
openvms-sysipc           557         L4 IANA
sdnskmp                  558         L4 IANA
teedtap                  559         L4 IANA
rmonitor                 560         L4 IANA
monitor                  561         L4 IANA
chshell                  562         L4 IANA
9pfs                     564         L4 IANA
whoami                   565         L4 IANA
streettalk               566         L4 IANA
banyan-rpc               567         L4 IANA
ms-shuttle               568         L4 IANA
ms-rome                  569         L4 IANA
meter                    570         L4 IANA
sonar                    572         L4 IANA
banyan-vip               573         L4 IANA
ftp-agent                574         L4 IANA
vemmi                    575         L4 IANA
ipcd                     576         L4 IANA
vnas                     577         L4 IANA
ipdd                     578         L4 IANA
decbsrv                  579         L4 IANA
sntp-heartbeat           580         L4 IANA
bdp                      581         L4 IANA
scc-security             582         L4 IANA
philips-vc               583         L4 IANA
keyserver                584         L4 IANA
password-chg             586         L4 IANA
submission               587         L4 IANA
tns-cml                  590         L4 IANA
http-alt                 8008         L4 IANA
eudora-set               592         L4 IANA
http-rpc-epmap           593         L4 IANA
tpip                     594         L4 IANA
cab-protocol             595         L4 IANA
smsd                     596         L4 IANA
ptcnameservice           597         L4 IANA
sco-websrvrmg3           598         L4 IANA
acp                      599         L4 IANA
ipcserver                600         L4 IANA
urm                      606         L4 IANA
```

```
nqs                         607          L4 IANA
sift-uft                    608          L4 IANA
npmp-trap                   609          L4 IANA
npmp-local                  610          L4 IANA
npmp-gui                    611          L4 IANA
hmmp-ind                    612          L4 IANA
hmmp-op                     613          L4 IANA
sshell                      614          L4 IANA
sco-inetmgr                 615          L4 IANA
sco-sysmgr                  616          L4 IANA
sco-dtmgr                   617          L4 IANA
dei-icda                    618          L4 IANA
sco-websrvrmgr              620          L4 IANA
escp-ip                     621          L4 IANA
collaborator                622          L4 IANA
cryptoadmin                 624          L4 IANA
dec_dlm                     625          L4 IANA
passgo-tivoli               627          L4 IANA
qmqp                        628          L4 IANA
3com-amp3                   629          L4 IANA
rda                         630          L4 IANA
ipp                         631          L4 IANA
bmpp                        632          L4 IANA
servstat                    633          L4 IANA
ginad                       634          L4 IANA
rlzdbase                    635          L4 IANA
lanserver                   637          L4 IANA
mcns-sec                    638          L4 IANA
msdp                        639          L4 IANA
entrust-sps                 640          L4 IANA
repcmd                      641          L4 IANA
esro-emsdp                  642          L4 IANA
sanity                      643          L4 IANA
dwr                         644          L4 IANA
ldp                         646          L4 IANA
dhcp-failover               647          L4 IANA
rrp                         648          L4 IANA
aminet                      2639          L4 IANA
obex                        650          L4 IANA
ieee-mms                    651          L4 IANA
hello-port                  652          L4 IANA
repscmd                     653          L4 IANA
aodv                        654          L4 IANA
tinc                        655          L4 IANA
spmp                        656          L4 IANA
rmc                         657          L4 IANA
tenfold                     658          L4 IANA
mac-srvr-admin              660          L4 IANA
hap                         661          L4 IANA
pftp                        662          L4 IANA
purenoise                   663          L4 IANA
sun-dr                      665          L4 IANA
disclose                    667          L4 IANA
mecomm                      668          L4 IANA
meregister                  669          L4 IANA
vacdsm-sws                  670          L4 IANA
vacdsm-app                  671          L4 IANA
vpps-qua                    672          L4 IANA
cimplex                     673          L4 IANA
acap                        674          L4 IANA
dctp                        675          L4 IANA
vpps-via                    676          L4 IANA
vpp                         677          L4 IANA
ggf-ncp                     678          L4 IANA
```

```
mrm                         679         L4 IANA
entrust-aaas                680         L4 IANA
entrust-aams                681         L4 IANA
mdc-portmapper              685         L4 IANA
hcp-wismar                  686         L4 IANA
asipregistry                687         L4 IANA
realm-rusd                  688         L4 IANA
nmap                        689         L4 IANA
vatp                        690         L4 IANA
msexch-routing              691         L4 IANA
hyperwave-isp               692         L4 IANA
connendp                    693         L4 IANA
ha-cluster                  694         L4 IANA
ieee-mms-ssl                695         L4 IANA
rushd                       696         L4 IANA
uuidgen                     697         L4 IANA
olsr                        698         L4 IANA
accessnetwork               699         L4 IANA
elcsd                       704         L4 IANA
agentx                      705         L4 IANA
silc                        706         L4 IANA
borland-dsj                 707         L4 IANA
entrust-kmsh                709         L4 IANA
entrust-ash                 710         L4 IANA
cisco-tdp                   711         L4 IANA
netviewdm1                  729         L4 IANA
netviewdm2                  730         L4 IANA
netviewdm3                  731         L4 IANA
netgw                       741         L4 IANA
netrcs                      742         L4 IANA
flexlm                      744         L4 IANA
fujitsu-dev                 747         L4 IANA
ris-cm                      748         L4 IANA
pump                        751         L4 IANA
qrh                         752         L4 IANA
rrh                         753         L4 IANA
tell                        754         L4 IANA
nlogin                      758         L4 IANA
con                         759         L4 IANA
ns                          760         L4 IANA
rxe                         761         L4 IANA
quotad                      762         L4 IANA
cycleserv                   763         L4 IANA
omserv                      764         L4 IANA
webster                     765         L4 IANA
phonebook                   767         L4 IANA
vid                         769         L4 IANA
cadlock                     770         L4 IANA
rtip                        771         L4 IANA
cycleserv2                  772         L4 IANA
submit                      643         Standard
entomb                      775         L4 IANA
multiling-http              777         L4 IANA
wpgs                        780         L4 IANA
device                      801         L4 IANA
itm-mcell-s                 828         L4 IANA
pkix-3-ca-ra                829         L4 IANA
dhcp-failover2              847         L4 IANA
rsync                       873         L4 IANA
iclcnet-locate              886         L4 IANA
iclcnet_svinfo              887         L4 IANA
accessbuilder               888         L4 IANA
omginitialrefs              900         L4 IANA
smpnameres                  901         L4 IANA
```

```
xact-backup                 911          L4 IANA
ftps-data                   989          L4 IANA
nas                         991          L4 IANA
vsinet                      996          L4 IANA
maitrd                      997          L4 IANA
applix                      999          L4 IANA
surf                        1010          L4 IANA
rmiactivation               1098          L4 IANA
rmiregistry                 1099          L4 IANA
ms-sql-m                    1434          L4 IANA
ms-olap                     2393          L4 IANA
msft-gc                     3268          L4 IANA
msft-gc-ssl                 3269          L4 IANA
tlisrv                      1527          L4 IANA
coauthor                    1529          L4 IANA
rdb-dbs-disp                1571          L4 IANA
oraclenames                 1575          L4 IANA
oraclenet8cman              1630          L4 IANA
net8-cman                   1830          L4 IANA
micromuse-lm                1534          L4 IANA
orbix-locator               3075          L4 IANA
orbix-config                3076          L4 IANA
orbix-loc-ssl               3077          L4 IANA
shockwave                   1626          L4 IANA
sitaraserver                2629          L4 IANA
sitaramgmt                  2630          L4 IANA
sitaradir                   2631          L4 IANA
mysql                       3306          L4 IANA
net-assistant               3283          L4 IANA
msnp                        1863          L4 IANA
groove                      2492          L4 IANA
directplay                  2234          L4 IANA
directplay8                 6073          L4 IANA
kali                        2213          L4 IANA
worldfusion                 2595          L4 IANA
directv-web                 3334          L4 IANA
directv-soft                3335          L4 IANA
directv-tick                3336          L4 IANA
directv-catlg               3337          L4 IANA
wap-push                    2948          L4 IANA
wap-pushsecure              2949          L4 IANA
wap-push-http               4035          L4 IANA
wap-push-https              4036          L4 IANA
wap-wsp                     9200          L4 IANA
wap-wsp-wtp                 9201          L4 IANA
wap-wsp-s                   9202          L4 IANA
wap-wsp-wtp-s               9203          L4 IANA
wap-vcard                   9204          L4 IANA
wap-vcal                    9205          L4 IANA
wap-vcard-s                 9206          L4 IANA
wap-vcal-s                  9207          L4 IANA
ibprotocol                  6714          L4 IANA
gtp-user                    2152          L4 IANA
xdtp                        3088          L4 IANA
parsec-game                 6582          L4 IANA
hopopt                      0            L3 IANA
ggp                         3            L3 IANA
st                          5            L3 IANA
cbt                         7            L3 IANA
zserv                       346          L4 IANA
igrp                        9            L3 IANA
bbnrccmon                   10           L3 IANA
pawserv                     345          L4 IANA
texar                       333          L4 IANA
```

```
rtsps                    322         L4 IANA
pip                      1321         L4 IANA
ptp-general              320         L4 IANA
nat-stun                 3478         L4 IANA
compressnet              2           L4 IANA
rje                      5           L4 IANA
discard                  9           L4 IANA
qotd                     17          L4 IANA
msp                      18          L4 IANA
ftp-data                 20          L4 IANA
nsw-fe                   27          L4 IANA
msg-icp                  29          L4 IANA
csi-sgwp                 348         L4 IANA
msg-auth                 31          L4 IANA
dsp                      33          L4 IANA
rap                      38          L4 IANA
rlp                      39          L4 IANA
graphics                 41          L4 IANA
name                     42          L4 IANA
profile                  136         L4 IANA
mpm-flags                44          L4 IANA
mpm                      45          L4 IANA
mpm-snd                  46          L4 IANA
ni-ftp                   47          L4 IANA
auditd                   48          L4 IANA
emfis-data               140         L4 IANA
re-mail-ck               50          L4 IANA
la-maint                 51          L4 IANA
xns-time                 52          L4 IANA
emfis-cntl               141         L4 IANA
xns-ch                   54          L4 IANA
bl-idm                   142         L4 IANA
xns-auth                 56          L4 IANA
xns-mail                 58          L4 IANA
ni-mail                  61          L4 IANA
acas                     62          L4 IANA
covia                    64          L4 IANA
sql*net                  66          L4 IANA
bootps                   67          L4 IANA
bootpc                   68          L4 IANA
uaac                     145         L4 IANA
iso-tp0                  146         L4 IANA
netrjs-1                 71          L4 IANA
netrjs-2                 72          L4 IANA
netrjs-3                 73          L4 IANA
netrjs-4                 74          L4 IANA
deos                     76          L4 IANA
iso-ip                   147         L4 IANA
xfer                     82          L4 IANA
mit-ml-dev               83          L4 IANA
ctf                      84          L4 IANA
mfcobol                  86          L4 IANA
jargon                   148         L4 IANA
su-mit-tg                89          L4 IANA
dnsix                    90          L4 IANA
mit-dov                  91          L4 IANA
aed-512                  149         L4 IANA
dcp                      93          L4 IANA
objcall                  94          L4 IANA
supdup                   95          L4 IANA
dixie                    96          L4 IANA
swift-rvf                97          L4 IANA
tacnews                  98          L4 IANA
metagram                 99          L4 IANA
```

```
hostname                 101         L4 IANA
iso-tsap                 102         L4 IANA
acr-nema                 104         L4 IANA
csnet-ns                 105         L4 IANA
3com-tsmux               106         L4 IANA
sql-net                  150         L4 IANA
snagas                   108         L4 IANA
pop2                     109         L4 IANA
hems                     151         L4 IANA
mcidas                   112         L4 IANA
auth                     113         L4 IANA
sftp                     115         L4 IANA
ansanotify               116         L4 IANA
uucp-path                117         L4 IANA
sqlserv                  118         L4 IANA
cfdptkt                  120         L4 IANA
erpc                     121         L4 IANA
smakynet                 122         L4 IANA
bftp                     152         L4 IANA
ansatrader               124         L4 IANA
locus-map                125         L4 IANA
nxedit                   126         L4 IANA
locus-con                127         L4 IANA
gss-xlicen               128         L4 IANA
pwdgen                   129         L4 IANA
cisco-fna                130         L4 IANA
sgmp                     153         L4 IANA
netsc-prod               154         L4 IANA
netsc-dev                155         L4 IANA
knet-cmp                 157         L4 IANA
pcmail-srv               158         L4 IANA
nss-routing              159         L4 IANA
sgmp-traps               160         L4 IANA
cmip-man                 163         L4 IANA
cmip-agent               164         L4 IANA
xns-courier              165         L4 IANA
s-net                    166         L4 IANA
namp                     167         L4 IANA
rsvd                     168         L4 IANA
send                     169         L4 IANA
print-srv                170         L4 IANA
multiplex                171         L4 IANA
xyplex-mux               173         L4 IANA
mailq                    174         L4 IANA
vmnet                    175         L4 IANA
genrad-mux               176         L4 IANA
nextstep                 178         L4 IANA
ris                      180         L4 IANA
unify                    181         L4 IANA
audit                    182         L4 IANA
ocbinder                 183         L4 IANA
ocserver                 184         L4 IANA
remote-kis               185         L4 IANA
kis                      186         L4 IANA
mumps                    188         L4 IANA
qft                      189         L4 IANA
gacp                     190         L4 IANA
prospero                 191         L4 IANA
osu-nms                  192         L4 IANA
srmp                     193         L4 IANA
dn6-nlm-aud              195         L4 IANA
dls                      197         L4 IANA
dls-mon                  198         L4 IANA
smux                     199         L4 IANA
```

```
src                           200         L4 IANA
at-rtmp                       201         L4 IANA
at-nbp                        202         L4 IANA
at-3                          203         L4 IANA
at-echo                       204         L4 IANA
at-5                          205         L4 IANA
at-zis                        206         L4 IANA
at-7                          207         L4 IANA
at-8                          208         L4 IANA
qmtp                          209         L4 IANA
z39.50                        210         L4 IANA
914c/g                        211         L4 IANA
anet                          212         L4 IANA
vmpwscs                       214         L4 IANA
softpc                        215         L4 IANA
CAIlic                        216         L4 IANA
dbase                         217         L4 IANA
mpp                           218         L4 IANA
uarps                         219         L4 IANA
fln-spx                       221         L4 IANA
rsh-spx                       222         L4 IANA
cdc                           223         L4 IANA
masqdialer                    224         L4 IANA
sur-meas                      243         L4 IANA
inbusiness                    244         L4 IANA
dsp3270                       246         L4 IANA
subntbcst_tftp                247         L4 IANA
bhfhs                         248         L4 IANA
set                           257         L4 IANA
esro-gen                      259         L4 IANA
openport                      260         L4 IANA
nsiiops                       261         L4 IANA
arcisdms                      262         L4 IANA
hdap                          263         L4 IANA
bgmp                          264         L4 IANA
x-bone-ctl                    265         L4 IANA
sst                           266         L4 IANA
td-service                    267         L4 IANA
td-replica                    268         L4 IANA
http-mgmt                     280         L4 IANA
personal-link                 281         L4 IANA
cableport-ax                  282         L4 IANA
rescap                        283         L4 IANA
corerjd                       284         L4 IANA
k-block                       287         L4 IANA
novastorbakcup                308         L4 IANA
bhmds                         310         L4 IANA
asip-webadmin                 311         L4 IANA
vslmp                         312         L4 IANA
magenta-logic                 313         L4 IANA
opalis-robot                  314         L4 IANA
dpsi                          315         L4 IANA
decauth                       316         L4 IANA
zannet                        317         L4 IANA
pkix-timestamp                318         L4 IANA
ptp-event                     319         L4 IANA
cisco-tna                     131         L4 IANA
cisco-sys                     132         L4 IANA
statsrv                       133         L4 IANA
ingres-net                    134         L4 IANA
Konspire2b                    6085         L4 IANA
Total protocols:              721
```

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 *77 : show ip nbar protocol-id* フィールドの説明

フィールド	説明
Protocol Name	NBAR プロトコルの名前です。
id	NBAR プロトコルに割り当てられている固有識別子です。
type	プロトコルが標準かカスタマイズされているかを示します。

関連コマンド

コマンド	説明
ipnbarcustom	NBAR Protocol Discovery 機能を拡張し、追加のスタティック ポート アプリケーションを分類および監視できます。または、NBAR はサポートしていないスタティック ポート トラフィックを分類できるようになります。

show ip nbar protocol-pack

プロトコル パック情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show ip nbar protocol-pack** コマンドを使用します。

show ip nbar protocol-pack {*protocol-pack*|**active**} **[detail]**

構文の説明

protocol-pack	プロトコル パック ファイルのパスおよび名前です。
active	アクティブなプロトコル パック情報を表示します。
detail	（任意）詳細なプロトコルパック情報を表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.3S	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

プロトコル パックは、複数のプロトコル記述言語（PDL）ファイルとマニフェスト ファイルを含む単一の圧縮ファイルです。このプロトコルパックが導入される前は、PDL を個別にロードする必要がありました。Network-Based Application Recognition（NBAR）プロトコル パックを使用すると、必須のプロトコル セットをロードでき、ご使用のネットワークでの分類で、NBAR が認識可能なプロトコルを追加できます。

例

次の **show ip nbar protocol-pack** コマンドからの出力例では、アクティブなプロトコル パックの情報が表示されています。

```
Router# show ip nbar protocol-pack active
ACTIVE protocol pack:
Name:                            Default Protocol Pack
Version:                         1.0
Publisher:                       Cisco Systems Inc.
```

次の **show ip nbar protocol-pack** コマンドからの出力例では、アクティブなプロトコル パックの詳細情報が表示されています。

```
Router# show ip nbar protocol-pack active detail
ACTIVE protocol pack:
Name:                            Default Protocol Pack
Version:                         1.0
Publisher:                       Cisco Systems Inc.
```

```
Protocols:
base                                Mv: 4
ftp                                 Mv: 5
http                                Mv: 18
static                              Mv: 6
socks                               Mv: 2
nntp                                Mv: 2
tftp                                Mv: 2
exchange                            Mv: 3
vdolive                             Mv: 1
sqlnet                              Mv: 2
netshow                             Mv: 3
sunrpc                              Mv: 3
streamwork                          Mv: 2
citrix                              Mv: 11
fasttrack                           Mv: 3
gnutella                            Mv: 7
kazaa2                              Mv: 11
```

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 *78 : show ip nbar protocol-pack* フィールドの説明

フィールド	説明
Name	プロトコル パックの名前です。
Version	プロトコル パックのバージョンです。
Publisher	プロトコル パックのパブリッシャの名前です。
Protocols	プロトコルパックに含まれるプロトコルのリストです。

関連コマンド

コマンド	説明
defaultipnbarprotocol-pack	プロトコル パックのベース バージョンをロードし、ロード済みのその他のすべてのプロトコル パックを削除します。
ipnbarprotocol-pack	プロトコル パックをロードします。

show ip nbar resources flow

Network-Based Application Recognition（NBAR）の現在の設定およびリソースの使用率を表示するには、特権 EXEC モードで **showipnbarresourcesflow** コマンドを使用します。

show ip nbar resources flow

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.4S	このコマンドが導入されました。

例

次は、**showipnbarresourcesflow** コマンドの出力例です。出力にはフィールドの説明も表示されます。

```
Router# show ip nbar resources flow

NBAR flow statistics
        Maximum no of sessions allowed : 3500000
        Maximum memory usage allowed   : 734003 KBytes
        Active sessions                : 3499950
        Active memory usage            : 665364 KBytes
        Peak session                   : 3499950
        Peak memory usage              : 672396 KBytes
```

関連コマンド

コマンド	説明
ipnbarresourcesflowmax-session	最大フローセッションが、フローテーブルで使用できるように設定します。

show ip nbar statistics

Network-Based Application Recognition（NBAR）が動作するデバイスの障害統計情報、フローごとのパケット数、および異なるタイプの分類を表示するには、特権 EXEC モードで **show ip nbar statistics** コマンドを使用します。

show ip nbar 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 モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.2(4)M	このコマンドが導入されました。

例

次は、**show ip nbar statistics** コマンドの出力例です。出力にはフィールドの説明も表示されます。

```
Device# show ip nbar statistics

Compiler statistics
Malloc failure = 0
Control-plane statistics
Malloc failure = 0
Invalid iterators = 0
Data-plane statistics
Malloc failure = 0
FO create failure = 0
CFT Age set failure = 0
```

show ip nbar trace

データ プレーンのパケットが通過するパスを表示するには、特権 EXEC モードで **show ip nbar trace** コマンドを使用します。

show ip nbar trace{**detail**|**summary**}[{**config**}]

構文の説明

detail	分類トレースの詳細を表示します。
summary	分類トレースの概要を表示します。
config	（任意）状態グラフのトレースの設定情報を表示します。

コマンド デフォルト

パケットが通過するすべてのパスに関する情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.2(4)M	このコマンドが導入されました。

使用上のガイドライン

トレースおよびサマリー デバッグを有効にする必要があります。

例

次は、**show ip nbar trace summary** コマンドの出力例です。出力にはフィールドの説明も表示されます。

```
Device# show ip nbar trace summary

Classification: 76, flag: 163
Searched Source WKP
Searched Dest WKP
Classifying using Heuristic regexp
Classifying using Heuristic General
Classifying using MPE

Classification: 1, flag: 160
Searched Source WKP
Searched Dest WKP
Classifying using Heuristic regexp
Classifying using Heuristic General
Classifying using MPE
```

次は、**show ip nbar trace detail** コマンドの出力例です。出力にはフィールドの説明も表示されます。

```
Device# show ip nbar trace detail

Graph Id 1
Classification: 82, flag: 163
Packet No: 1
```

```
String: Searching Source V4 WKP
String: Searching Destination V4 WKP
String: Entering loop core from Heuristic Regex
State Node:http-verify-heuristic-entry-point-get
State Node:http-verify-heuristic-entry-point-get
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:youtube-found-url
State Node:http-check-url-fe
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-end-of-request-check
State Node:HTTP-request-check-end-of-packet
State Node:HTTP-request-check-end-of-packet
State Node:HTTP-request-headers-parser
State Node:HTTP-request-headers-parser
Graph Id 1
```

関連コマンド

コマンド	説明
clear ip nbar trace summary	分類モジュールをクリアします。
debug ip nbar config	NBAR の有効化および無効化で設定するすべてのコマンドのデバッグを有効にします。

show ip nbar unclassified-port-stats

未分類パケットの Network-Based Application Recognition（NBAR）ポート統計情報を表示するには、特権 EXEC モードで **showipnbarunclassified-port-stats** コマンドを使用します。

show ip nbar unclassified-port-stats [{*top-talkers*|**ip** [{*protocol-number* [*number-protocols*]|**top** *top-talkers*}]|[{**tcp**|**udp**}] [{*port-number* [*number-ports*]|**top** *top-talkers*|**bottom** *bottom-talkers*}]}]

構文の説明

top-talkers	（任意）表示するトップ トーカーの数です。
ip	（任意）TCP 以外/UDP 以外の未分類パケットのポート統計情報を表示します。
protocol-number	（任意）開始 IP プロトコル番号です。
number-protocols	（任意）表示するプロトコルの数です。
top	（任意）top-n が表示されることを示します。top-n はアクティブな NBAR サポート プロトコルのなかの上位プロトコル数です。n は表示するプロトコル数を表します。たとえば、top-n 3 と入力すると、アクティブな NBAR サポート プロトコルの上位 3 つが表示されます。
tcp	（任意）未分類 TCP パケットのポート統計情報を表示します。
udp	（任意）未分類 UDP パケットのポート統計情報を表示します。
port-number	（任意）開始 TCP または UDP ポート番号です。
number-ports	（任意）表示するポートの数です。
bottom	（任意）bottom-n が表示されることを示します。bottom-n はアクティブな NBAR サポート プロトコルのなかの下位プロトコル数です。n は表示するプロトコル数を表します。たとえば、bottom-n 3 と入力すると、アクティブな NBAR サポート プロトコルの下位 3 つが表示されます。
bottom-talkers	（任意）表示するボトム トーカーの数です。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。

リリース	変更箇所
12.1(13)E	このコマンドが、FlexWAN モジュール非搭載の Cisco Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
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。
12.2(18)ZYA	このコマンドが、Cisco IOS Release 12.2(18)ZYA に統合されました。このコマンドが変更され、VLAN に関する情報表示（必要に応じて）、およびレイヤ 2 とレイヤ 3 両方の EtherChannel のサポート（Cisco Catalyst スイッチのみ）が追加されました。

使用上のガイドライン

デフォルトでは、NBAR未分類メカニズムは無効です。ルータを設定してパケットが着信するポートのトラッキングを開始するには、**debugipnbarunclassified-port-stats** コマンドを使用します。次に **showipnbarunclassified-port-stats** コマンドを使用して、収集した情報を確認します。

例

次は、**showipnbarunclassified-port-stats** コマンドの出力例です。

```
Router# show ip nbar unclassified-port-stats

-tcp-
      80/tcp:48
    1443/tcp:3
    1423/tcp:2
    1424/tcp:2
    1425/tcp:2
-udp-
    1985/udp:158
    1029/udp:13
     496/udp:4
    1445/udp:3
    1449/udp: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 *79 : show ip nbar unclassified-port-stats* フィールドの説明

フィールド	説明
-tcp-	TCP プロトコルです。
80/tcp:48	80 はポート番号、tcp はプロトコル、48 はパケット数を示します。
-udp-	UDP プロトコルです。
1985/udp:158	1855 はポート番号、udp はプロトコル、158 はパケット数を示します。

出力には、ポート番号、プロトコル、およびパケット数が表示されます。たとえば、80/tcp:48 において 80 はポート番号、tcp はプロトコル、48 はパケット数を示します。

関連コマンド

コマンド	説明
ipnbarcustom	NBAR Protocol Discovery 機能を拡張し、追加のスタティック ポートアプリケーションを分類および監視できます。または、NBARはサポートしていないスタティック ポート トラフィックを分類できるようになります。
ipnbarpdlm	シスコが提供する PDLM によって、NBAR が認識するプロトコルのリストを拡張および強化します。
ipnbarport-map	ウェルノウン ポート番号以外のポート番号を使用して、プロトコルまたはプロトコル名を検索するように NBAR を設定します。
ipnbarprotocol-discovery	特定のインターフェイス上で NBAR が認識するすべてのプロトコルについて、トラフィックを検出するように NBAR を設定します。
ipnbarresourcesprotocol	プロトコル ベースで、NBAR フロー リンク テーブルの有効期限を設定します。
ipnbarresourcessystem	システム全体で、NBAR フローリンク テーブルの有効期限とメモリ要件を設定します。
showipnbarpdlm	NBAR で使用されている PDLM を表示します。
showipnbarport-map	NBAR に現在使用されているプロトコルからポートへのマッピングを表示します。
showipnbarprotocol-discovery	NBAR Protocol Discovery 機能によって収集された統計情報を表示します。
showipnbarversion	Cisco IOS リリースの NBAR ソフトウェア バージョンまたは Cisco IOS ルータの NBAR PDLM のバージョンに関する情報を表示します。

show ip nbar version

Cisco IOS リリースの Network-Based Application Recognition（NBAR）ソフトウェア バージョンまたは Cisco IOS ルータの NBAR Packet Description Language Module（PDLM）のバージョンに関する情報を表示するには、特権 EXEC モードで **showipnbarversion** コマンドを使用します。
rivilegedEXEC

show ip nbar version [*PDLM-name*]

構文の説明

PDLM-name	（任意）情報を表示する特定の PDLM の名前を指定します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.3(4)T	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
15.1(3)T	このコマンドが Cisco IOS Release 15.1(3)T に統合されました。

使用上のガイドライン

showipnbarversion コマンドは、最初の NBAR リリース後に NBAR に追加されたすべてのプロトコル（ユーザが Cisco.com から PDLM をダウンロードせずに Cisco IOS ソフトウェアに追加されたプロトコルを含む）を PDLM として処理します。ユーザが Cisco.com からダウンロードし NBAR に追加した PDLM も、**showipnbarversion** コマンドを入力すると、表示されます。

NBAR を使用すると、NBAR 内の各種の要素にバージョン番号が割り当てられます。これらのバージョン番号は、PDLM をダウンロードするときに必要です。PDLM（これもバージョン付けされます）は、PDLM バージョン番号が Cisco IOS ソフトウェアの NBAR バージョン番号と互換性がある場合、特定の Cisco IOS リリースの NBAR のみにダウンロードできます。

次の NBAR 関連のバージョン情報が入手できます。

- NBAR Software Version：現在のバージョンの Cisco IOS ソフトウェアで動作している NBAR ソフトウェアのバージョン。
- Resident Module Version：NBAR がサポートする PDLM プロトコルのバージョン。

次のバージョン番号が PDLM に保持されています。

- NBAR Software Version：この PDLM をロードする場合に必要な NBAR ソフトウェアの最小バージョン。

showipnbarversion コマンドを使用すると、Cisco IOS ソフトウェアにロード済みの PDLM のバージョン情報を表示できます。

例

次に、show ip nbar version コマンドの出力例を示します。

```
Router# show ip nbar version
NBAR software version:  3
1   base                 Mv: 2
2   ftp                  Mv: 2
3   http                 Mv: 7, Nv: 3; slot1:http_vers.pdlm
4   static-port          Mv: 6
5   tftp                 Mv: 1
6   exchange             Mv: 1
7   vdolive              Mv: 1
8   sqlnet               Mv: 1
9   rcmd                 Mv: 1
10  netshow              Mv: 1
11  sunrpc               Mv: 2
12  streamwork           Mv: 1
13  citrix               Mv: 5
14  fasttrack            Mv: 2
15  gnutella             Mv: 1
16 kazaa                Mv: 6, Nv: 3; slot1:kazaa2_vers.pdlm
17 custom-protocols     Mv: 1
18 rtsp                 Mv: 1
19  rtp                  Mv: 2
20  mgcp                 Mv: 1
21  skinny               Mv: 1
22 h323                 Mv: 1
23 sip                  Mv: 1
24 rtcp                 Mv: 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 *80 : show ip nbar version* コマンドのフィールドの説明

フィールド	説明
NBAR Software Version	現在の Cisco IOS ソフトウェアで動作している NBAR ソフトウェア バージョン。この例では、Cisco IOS ソフトウェアの現在のバージョンで動作している NBAR ソフトウェアは、バージョン 3 です。
Mv	Resident Module Version。Resident Module Version は NBAR がサポートする PDLM プロトコルのバージョンなので、プロトコルによって異なります。たとえば、TFTP の Resident Module Version は 1 です。
Nv	非ネイティブ PDLM のロードに必要な NBAR ソフトウェアの最小バージョン。この番号は、Kazaa PDLM（プロトコル 17）など、ルータにロードされている非ネイティブ PDLM にのみ使用できます。この場合、Nv バージョンは 3 です。

同じネットワーク設定の場合、次の例は、**showipnbarversion** CLI で PDLM の特定のプロトコルを指定して出力します。

```
Router# show ip nbar version http
http                 Mv: 7, Nv: 3; slot1:http_vers.pdlm
```

関連コマンド

コマンド	説明
ipnbarpdlm	NBAR でサポートするプロトコルを追加するために、ルータへ PDLM をダウンロードします。

show ip rsvp

リソース予約プロトコル（RSVP）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 **showiprsvp** コマンドを使用します。

show ip rsvp

構文の説明

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	変更箇所
12.0(3)T	このコマンドが導入されました。
12.2(13)T	このコマンドが変更されました。**listeners** キーワードおよび **policy** キーワードが追加され、このコマンドはキーワードや引数が入力されていないときには RSVP グローバル設定を表示するように変更されました。
12.2(33)SRB	このコマンドが変更されました。コマンド出力が高速ローカル修復（FLR）情報を表示するように変更されました。
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。
12.2(33)SRC	このコマンドが変更されました。コマンド出力は、次の情報を表示するように変更されました。 • RSVP Quality of Service（QoS）およびマルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）情報。 • RSVP 集約情報。
15.0(1)M	このコマンドが変更されました。 [**atm-peak-rate-limit** | **counters** | **host** | **installed** | **interface** | **listeners** | **neighbor** | **policy** | **precedence** | **request** | **reservation** | **sbm** | **sender** | **signalling** | **tos**] 構文は、コマンドから削除されました。キーワード オプションは、次の個別のコマンド ファイルで表されます。show ip rsvp **atm-peak-rate-limit,**show ip rsvp **counters,**show ip rsvp **host,**show ip rsvp installed、show ip rsvp interface、show ip rsvp listeners、show ip rsvp neighbor、show ip rsvp policy、show ip rsvp precedence、show ip rsvp request、show ip rsvp reservation、show ip rsvp sbm、show ip rsvp sender、show ip rsvp signalling、show ip rsvp tos の各コマンドです。

リリース	変更箇所
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

例

次に、**showiprsvp** コマンドの出力例を示します。

```
Router# show ip rsvp
RSVP: enabled (on 1 interface(s))
   RSVP QoS signalling enabled
   MPLS/TE signalling enabled
Signalling:
   Refresh interval (msec): 30000
   Refresh misses: 4
Rate Limiting: enabled
   Burst: 8
   Limit: 37
   Maxsize: 2000
   Period (msec): 20
   Max rate (msgs/sec): 400
Refresh Reduction: disabled
   ACK delay (msec): 250
   Initial retransmit delay (msec): 1000
   Local epoch: 0xCE969B
   Message IDs: in use 0, total allocated 0, total freed 0
Neighbors: 0
   Raw IP encap: 0  UDP encap: 0  Raw IP, UDP encap: 0
RFC 3175 Aggregation: Enabled
   Level: 1
   Default QoS service: Controlled-Load
   Router ID: 10.22.22.22
   Number of signaled aggregate reservations:     0
   Number of signaled E2E reservation:            0
   Number of configured map commands:             0
   Number of configured reservation commands:     0
Hello:
   RSVP Hello for Fast-Reroute/Reroute: Disabled
     Statistics: Disabled
   BFD for Fast-Reroute/Reroute: Disabled
   RSVP Hello for Graceful Restart: Disabled
Graceful Restart: Disabled
   Refresh interval: 10000 msecs
   Refresh misses: 4
   DSCP: 0x30
   Advertised restart time: 5 msecs
   Advertised recovery time: 0 msecs
   Maximum wait for recovery: 3600000 msecs
Fast-Reroute:
   PSBs w/ Local protection desired
     Yes: 0
     No:  0
Fast Local Repair: enabled
   Max repair rate (paths/sec): 400
   Max processed   (paths/run): 1000
Local policy:
COPS:
Generic policy settings:
     Default policy: Accept all
     Preemption:     Disabled
```

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 *81 : show ip rsvp* フィールドの説明

フィールド	説明
RSVP	RSVP、QoS、および MPLS TE シグナリングの状態。値は、[有効（アクティブ化）（enabled (activated)）] または [無効（非アクティブ化）（disabled (deactivated)）] です。 （注） このフィールドが無効になるのは、RIB に登録するときに内部エラーが発生した場合のみです。
Signalling	有効な RSVP シグナリング パラメータは次のとおりです。 • [更新間隔（Refresh interval）] : RSVP 状態ごとの更新送信間の時間（ミリ秒（ms））。 • [更新ミス（Refresh misses）] : RSVP が状態の期限切れと見なし、ティアダウンするまでに、未受信の可能性がある連続した更新メッセージの数。
Rate Limiting: enabled or disabled	有効な RSVP レート制限パラメータは次のとおりです。 • [バースト（Burst）] : インターバル中に隣接ルータへの送信が許可された RSVP メッセージの最大数。 • [制限（Limit）] : キュー間隔あたりの最大送信 RSVP メッセージ数。 • [最大サイズ（Maxsize）] : メッセージ キューの最大サイズ（バイト）。 • [期間（Period）] : 間隔（時間枠）の長さ（ミリ秒（ms））。 • [最大レート（Max rate）] : 送信が許可された 1 秒あたりのメッセージの最大数。
Refresh Reduction: enabled or disabled	有効な RSVP 更新削減パラメータは次のとおりです。 • [ACK 遅延（ミリ秒）（ACK delay (msec)）] : 受信側ルータが確認応答（ACK）を送信するまでの期間（ミリ秒）。 • [初期再送信遅延（ミリ秒）（Initial retransmit delay (msec)）] : ルータがメッセージを再送信するまでの期間（ミリ秒）。 • [ローカル エポック（Local epoch）] : RSVP プロセス識別子（ID）。ノードが再起動するか、または RSVP プロセスが再実行されるたびにランダムに生成されます。 • [メッセージ ID（Message IDs）] : 使用中のメッセージ ID の数、割り当て済みの合計数、および使用可能な（解放された）合計数。

フィールド	説明
Neighbors	使用中のネイバーの合計数およびカプセル化の種類。RSVP や User Datagram Protocol（UDP）などがあります。
RFC 3175 Aggregation	RFC 3175（*AggregationofRSVPforIPv4andIPv6Reservations*）に定義された集約の状態。値は次のとおりです。 • Enabled：アクティブ。 • Disabled：非アクティブ。
show ip rsvp Field Descriptions	予約の集約レベル。一般的な値は次のとおりです。 • 0：エンドツーエンド（E2E）予約。 • 1：集約予約。 レベル x 予約を集約して、レベル *x* +1 で予約を形成できます。
Default QoS service	設定された QoS のタイプ。値は次のとおりです。 • Controlled-Load：アプリケーションはその要件を満足する帯域幅を予約できます。たとえば、重み付けランダム早期検出（WRED）を使用した RSVP では、このタイプのサービスが提供されます。 • Guaranteed-Rate：アプリケーションには、輻輳発生時でも低遅延かつ高スループットが保証されます。たとえば、RSVP を使用した重み付け均等化キューイング（WFQ）では、このタイプのサービスが提供されます。
Number of signaled aggregate reservations	シグナル集約予約の累積数。
Number of signaled E2E reservations	シグナル E2E 予約の累積数。
Number of configured map commands	設定された map コマンドの累積数。
Number of configured reservation commands	設定された reservation コマンドの累積数。
Hello	後続のフィールドは、hello が有効または無効になっているプロセスについて説明したものです。選択肢は、Fast Reroute、再ルーティング（hello ステート タイマー）、双方向フォワーディング検出（BFD）、およびグレースフル リスタート（リスタート機能を備えたノードの場合）です。

フィールド	説明
Statistics	hello 統計のステータス。有効な値は、次のとおりです。 • Enabled：統計が設定されています。helloパケットは、helloインプットキューに到着すると、その処理にかかる時間を記録する目的でタイムスタンプが付けられます。 • Disabled：hello 統計は設定されていません。 • [シャットダウン（Shutdown）]：hello 統計は設定されていますが、動作していません。インプットキューが長すぎです（つまり、10,000を超えるパケットがキュー内に滞留しています）。
Graceful Restart: Enabled or Disabled	有効な RSVP グレースフル リスタート パラメータは次のとおりです。 • [更新間隔（Refresh interval）]：ノードがそのネイバーに hello メッセージを送信する頻度（ミリ秒（ms））。 • [更新ミス（Refresh misses）]：ネイバー ダウン イベントをトリガーしてステートフル スイッチオーバー（SSO）プロシージャを起動させた、未受信の hello メッセージの数。 • [DSCP]：hello メッセージの IP ヘッダーにある DiffServ コード ポイント（DSCP）値。 • [再起動時刻のアドバタイズ（Advertised restart time）]：障害発生後に送信者が RSVP トラフィック エンジニアリング コンポーネントを再起動し、helloメッセージを交換するのに必要な時間（ミリ秒）。 • [リカバリ時間のアドバタイズ（Advertised recovery time）]：リカバリしているノードがそのネイバー ルータに対し、SSO 後に RSVP または MPLS フォワーディング ステートの再同期を求める期限（ミリ秒）。ゼロ値は、RSVP または MPLS 転送状態が SSO 後に保持されないことを示します。 • [リカバリの最大待機（Maximum wait for recovery）]：ルータがネイバーのリカバリを待機する最大時間（ミリ秒）。
Fast-Reroute	有効な Fast Reroute パラメータは次のとおりです。 • [必要なローカル保護を備えたPSB（PSBs w/ Local protection desired）]：[はい（Yes）] にすると、トンネルが停止したときに、パケット フローが中断していなければ、パス ステート ブロック（PSB）が再ルーティングされます。PSB が再ルーティングされないという意味ではありません。

フィールド	説明
Fast Local Repair: enabled or disabled	有効な高速ローカル修復パラメータは次のとおりです。 • [最大修復レート（パス/秒）（Max repair rate (paths/sec)）]：最大修復レート（1 秒あたりのパス数）。 • [最大処理（パス/実行）（Max processed (paths/run)）]：処理する最大通知要素（1 回の実行あたりのパス数）。
Local policy	現在設定されているローカル ポリシー。
COPS	現在有効な Common Open Policy Service（COPS）。
Generic policy settings	COPS またはローカル ポリシーに固有ではないポリシー設定。 • Default policy：「Accept all」は、すべての RSVP メッセージが受け入れられ、転送されることを意味します。[すべて拒否（Reject all）] とは、すべての RSVP メッセージを拒否するということです。 • [プリエンプション（Preemption）]：[無効（Disabled）] にすると、RSVP は予約の優先順位付けとそれに応じた帯域幅の割り当てを行いません。[有効（Enabled）] にすると、RSVP は予約に優先順位を付けて、最も優先順位の高い予約により多くの帯域幅を割り当てます。

関連コマンド

Command	Description
debugiprsvp	RSVP カテゴリのデバッグ メッセージを表示します。
showiprsvpatm-peak-rate-limit	あるインターフェイスまたはすべてのインターフェイスに対して設定された現在のピーク レート制限を表示します。
showiprsvpcounters	各インターフェイスで送受信した RSVP メッセージの数を表示します。
showiprsvphost	RSVP ホストに固有の情報を表示します。
showiprsvpinstalled	RSVP 関連のインストールされているフィルタと対応する帯域幅情報を表示します。
showiprsvpinterface	RSVP が有効になっているインターフェイスの情報を表示します。
show iprsvplisteners	指定したポートまたはプロトコルの RSVP リスナーを表示します。
showiprsvpneighbor	現在の RSVP ネイバーに関する情報を表示します。

Command	Description
showiprsvppolicy	現在設定されている RSVP ポリシーに関する情報を表示します。
showiprsvpprecedence	RSVP が有効になっているインターフェイスに関する IP プレシデンス情報を表示します。
showiprsvprequest	現在の RSVP 関連の要求情報を表示します。
showiprsvpreservation	現在の RSVP 関連の受信側情報を表示します。
showiprsvpsbm	RSVP 対応のインターフェイスに関する SBM 設定情報を表示します。
showiprsvpsender	RSVP PATH 関連の送信側情報を表示します。
showiprsvpsignalling	RSVP シグナリング情報を表示します。
showiprsvptos	RSVP が有効になっているインターフェイスに関する IP ToS 情報を表示します。

show ip rsvp aggregation ip

リソース予約プロトコル（RSVP）の要約集約情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpaggregationip** コマンドを使用します。

show ip rsvp aggregation ip [{**endpoints [detail]** [**dscp** *value*] [**remote** *ip-address*] [**role** {**aggregator**|**deaggregator**}]|**interface** [*if-name*]|**map** [**dscp** *value*]|**reservation** [**dscp** *value* [**aggregator** *ip-address*]]}]

構文の説明

endpoints	（任意）集約領域のアグリゲータとデアグリゲータを指定します。
interface *if-name*	（任意）インターフェイス名を指定します。
map	（任意）マップ コンフィギュレーション ルールを表示します。
dscp *value*	（任意）**map** キーワードに DiffServ コード ポイント（DSCP）を指定します。有効な値は次のとおりです。 • 0 ～ 63：DSCP の数値。デフォルト値は 0 です。 • af11 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）プレシデンス値。 • default：デフォルト DSCP 値。 • ef：Expedited Forwarding（EF; 完全優先転送）DSCP 値。
reservation	（任意）予約設定を表示します。
dscp *value*	（任意）**reservation** キーワードに DiffServ コード ポイント（DSCP）を指定します。有効な値は次のとおりです。 • 0 ～ 63：DSCP の数値。デフォルト値は 0 です。 • af11 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）プレシデンス値。 • default：デフォルト DSCP 値。 • ef：Expedited Forwarding（EF; 完全優先転送）DSCP 値。
aggregator *ip-address*	（任意）アグリゲータの IP アドレスを指定します。

コマンド デフォルト

showiprsvpaggregationip コマンドをオプション キーワードを指定せずに入力すると、すべての集約予約の概要情報が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRC	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

集約、マップ、および予約の設定の数を含む、集約に関する概要情報を表示するには、**showiprsvpaggregationip** コマンドを使用します。

例

show ip rsvp aggregation ip コマンドの出力例

次は、**showiprsvpaggregationip** コマンドの出力例です。

```
Router# show ip rsvp aggregation ip
RFC 3175 Aggregation:  Enabled
  Level: 1
  Default QoS service: Controlled-Load
  Number of signaled aggregate reservations:  2
  Number of signaled E2E reservations:        8
  Number of configured map commands:          4
  Number of configured reservation commands:  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 *82 : show ip rsvp aggregation ip* フィールドの説明

フィールド	説明
RFC 3175 Aggregation	RFC 3175（*AggregationofRSVPforIPv4andIPv6Reservations*）に定義された集約の状態。値は次のとおりです。 • Enabled：アクティブ。 • Disabled：非アクティブ。
Level	予約の集約レベル。一般的な値は次のとおりです。 • 0：エンドツーエンド（E2E）予約。 • 1：集約予約。 （注） レベル x 予約を集約すると、次の高いレベルの予約を作成できます。たとえばレベル x+1 などです。

フィールド	説明
Default QoS service	設定されているサービス品質（QoS）のタイプ。値は次のとおりです。 • Controlled-Load：アプリケーションはその要件を満足する帯域幅を予約できます。たとえば、重み付けランダム早期検出（WRED）を使用した RSVP では、このタイプのサービスが提供されます。 • Guaranteed-Rate：アプリケーションには、輻輳発生時でも低遅延かつ高スループットが保証されます。たとえば、RSVP を使用した重み付け均等化キューイング（WFQ）では、このタイプのサービスが提供されます。
Number of signaled aggregate reservations	シグナル集約予約の累積数。
Number of signaled E2E reservations	シグナル E2E 予約の累積数。
Number of configured map commands	設定された map コマンドの累積数。
Number of configured reservation commands	設定された reservation コマンドの累積数。

show ip rsvp aggregation ip interface の出力例

次は、**showiprsvpaggregationipinterface** コマンドの出力例です。

```
Router# show ip rsvp aggregation ip interface
Interface Name       Role
-------------------- --------
Ethernet0/0          interior
Serial2/0            exterior
Serial3/0            exterior
```

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 *83 : show ip rsvp aggregation ip interface* フィールドの説明

フィールド	説明
Interface Name	インターフェイスの名前および番号。
Role	ルータのインターフェイスの設定。値は、interior または exterior。

次は、インターフェイスを指定した場合の **showiprsvpaggregationipinterface** コマンドの出力例です。

```
Router# show ip rsvp aggregation ip interface Ethernet0/0
Interface Name       Role
-------------------- --------
Ethernet0/0          interior
```

関連コマンド

コマンド	説明
iprsvpaggregationip	ルータでRSVP集約を有効にします。

show ip rsvp aggregation ip endpoints

アグリゲータおよびデアグリゲータ ルータに関するリソース予約プロトコル（RSVP）情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpaggregationipendpoints** コマンドを使用します。

show ip rsvp aggregation ip endpoints [detail] [**dscp** *value*] [**remote** *ip-address*] [**role** {**aggregator**|**deaggregator**}]

構文の説明

detail	（任意）アグリゲータおよびデアグリゲータに関する追加情報を表示します。
dscp *value*	（任意）アグリゲータおよびデアグリゲータ ルータに DiffServ コード ポイント（DSCP）を指定します。有効な値は次のとおりです。 • 0 ～ 63：DSCP の数値。デフォルト値は 0 です。 • af11 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）プレシデンス値。 • default：デフォルト DSCP 値。 • ef：Expedited Forwarding（EF; 完全優先転送）DSCP 値。
remote	（任意）リモート デアグリゲータを指定します。
ip-address	リモート デアグリゲータの IP アドレスです。
role	（任意）集約領域でのルータの位置を指定します。
aggregator	（任意）集約領域の始点のルータを指定します。
deaggregator	（任意）集約領域の終点のルータを指定します。

コマンド デフォルト

showiprsvpaggregationipendpoints コマンドをオプション キーワードを指定せずに入力すると、すべての集約予約の情報が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRC	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

アグリゲータおよびデアグリゲータ ルータにおける次の出力のいずれかを表示するには、**showiprsvpaggregationipendpoints** コマンドを使用します。

- すべての集約予約。
- ノードがアグリゲータのすべての集約予約。
- ノードがデアグリゲータのすべての集約予約。
- リモート ノードが IP アドレスで指定されるすべての集約予約。
- 指定した DSCP のすべての集約予約。
- 上記オプションの組み合わせ。ノードがアグリゲータで、リモート ノードが IP アドレスで指定される、DSCP 指定のすべての集約などがあります。
- 詳細情報付きの上記オプションのいずれか。

例

次は、**showiprsvpaggregationipendpointsdetail** コマンドの出力例です。

```
Router# show ip rsvp aggregation ip endpoints detail
Role  DSCP Aggregator      Deaggregator    State  Rate    Used    QBM PoolID
----- ---- --------------- --------------- ------ ------- ------- ----------
Agg   46   10.3.3.3         10.4.4.4         ESTABL 100K    100K    0x00000003
   Aggregate Reservation for the following E2E Flows (PSBs):
To             From          Pro DPort Sport  Prev Hop       I/F      BPS
10.4.4.4       10.1.1.1       UDP 1     1     10.23.20.3     Et1/0    100K
   Aggregate Reservation for the following E2E Flows (RSBs):
To             From          Pro DPort Sport  Next Hop       I/F      Fi Serv BPS
10.4.4.4       10.1.1.1       UDP 1     1     10.4.4.4       Se2/0    FF RATE 100K
   Aggregate Reservation for the following E2E Flows (Reqs):
To             From          Pro DPort Sport  Next Hop       I/F      Fi Serv BPS
10.4.4.4       10.1.1.1       UDP 1     1     10.23.20.3     Et1/0    FF RATE 100K
```

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 *84 : show ip rsvp aggregation ip endpoints detail* フィールドの説明

フィールド	説明
Role	ルータの機能。値は、aggregator または deaggregator です。
DSCP	DSCP 値。
Aggregator	アグリゲータの IP アドレスです。
Deaggregator	デアグリゲータの IP アドレスです。

フィールド	説明
State	予約の状態です。各集約予約は、次のいずれかの状態になります。 • PATH_WAIT：デアグリゲータのみで有効。デアグリゲータの集約予約が、必要な新しい集約を要求する PATHERROR メッセージをデアグリゲータが送信後に、この状態になります。 • RESV_WAIT：アグリゲータのみで有効。アグリゲータの集約予約が、集約予約の PATH メッセージをアグリゲータが送信後に、この状態になります。 • RESVCONF_WAIT：デアグリゲータのみで有効。デアグリゲータの集約予約が、集約予約の RESV メッセージをデアグリゲータが送信後に、この状態になります。 • ESTABLISHED：アグリゲータおよびデアグリゲータ両方で有効。アグリゲータは、RESVCONF メッセージを送信後に、この状態になります。デアグリゲータは、集約予約の RESVCONF メッセージの受信後に、この状態になります。 • SHUT_DELAY：アグリゲータおよびデアグリゲータ両方で有効。アグリゲータおよびデアグリゲータは、最後のエンドツーエンド（E2E）予約が削除された後に、この状態になります。
Rate	ビット/秒（bps）単位での割り当てられた帯域幅です。
Used	ビット/秒（bps）単位で使用された帯域幅量です。
QBM Pool ID	予約の Quality of Service（QoS）帯域幅マネージャ（QBM）ID です。
Aggregate Reservation for the following E2E Flows	予約に関する情報： PSB：パス ステート ブロック。PATH メッセージ ダウンストリームの転送に使用するデータが含まれます。 RSB：予約ステートブロック。着信RESV メッセージのデータが含まれます。 Reqs：要求。PATH メッセージを送信したノードへ RESV メッセージ アップストリームを転送するために必要なデータが含まれます。
To	受信者の IP アドレス。
From	送信元の IP アドレス。
Pro	プロトコル コード。コードは、TCP、User Datagram Protocol（UDP）などの IP プロトコルを示します。
DPort	宛先ポート番号。

フィールド	説明
Sport	送信元ポート番号です。
Prev Hop or Next Hop	前のホップまたはネクスト ホップの IP アドレスです。
I/F	前のホップまたは ネクスト ホップのインターフェイスです。
Fi	フィルタです（Wildcard Filter、Shared-Explicit、または Fixed-Filter）。
Serv	サービスです（RATE または LOAD）。
BPS	ビット/秒（bps）単位での集約予約で使用された帯域幅です。

関連コマンド

コマンド	説明
iprsvpaggregationip	ルータでRSVP集約を有効にします。

show ip rsvp atm-peak-rate-limit

インターフェイスまたはすべてのインターフェイス（該当する場合）に設定された現在のピーク レート制限を表示するには、EXEC モードで **showiprsvpatm-peak-rate-limit** コマンドを使用します。

show ip rsvp atm-peak-rate-limit [*interface-type interface-number*]

構文の説明

interface-type interface-number	（任意）インターフェイス タイプおよびインターフェイス番号。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
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。

使用上のガイドライン

showiprsvpatm-peak-rate-limit コマンドは、省略形として次の表記を使用して、設定済みのピーク レートを表示します。

- キロバイトは、K bytes と表示されます。たとえば、1200 キロバイトは 1200K bytes と表示されます。
- 1000 キロバイトは、1M bytes と表示されます。

インターフェイス名が指定されないと、すべてのリソース予約プロトコル（RSVP）対応インターフェイスの設定済みピーク レートが表示されます。

例

次の例は、**showiprsvpatm-peak-rate-limit** コマンドの結果です。この例では、**iprsvpatm-peak-rate-limit** コマンドを使用して ATM サブインターフェイス 2/0/0.1 の予約ピーク レート制限が 100 KB に設定済みです。

次は、**showiprsvpatm-peak-rate-limit** コマンドの出力例です。*interface-type interface-number* 引数を使用しています。

```
Router# show ip rsvp atm-peak-rate-limit atm2/0/0.1
RSVP: Peak rate limit for ATM2/0/0.1 is 100K bytes
```

次は、インターフェイス名を指定しない場合の **showiprsvpatm-peak-rate-limit** コマンドの出力例です。

```
Router# show ip rsvp atm-peak-rate-limit


Interface name          Peak rate limit
Ethernet0/1/1          not set
```

```
ATM2/0/0              not set
ATM2/0/0.1            100K
Router# show ip rsvp atm-peak-rate-limit
Interface name        Peak rate limit
Ethernet0/1           not set
ATM2/1/0              1M
ATM2/1/0.10           not set
ATM2/1/0.11           not set
ATM2/1/0.12           not set
```

関連コマンド

Command	Description
iprsvpatm-peak-rate-limit	現在のインターフェイスまたはそのサブインターフェイス上に確立された、すべての新しく作成されたRSVP SVCの予約のピーク セルレートに制限を設定します。

show ip rsvp authentication

リソース予約プロトコル（RSVP）が他の RSVP ネイバーと確立したセキュリティ アソシエーションを表示するには、ユーザ EXEC または特権 EXEC モードで show **iprsvpauthentication** コマンドを使用します。

show ip rsvp authentication [detail] [from {*ip-addresshostname*}] [**to** {*ip-addresshostname*}]

構文の説明

detail	（任意）RSVPセキュリティ アソシエーションの追加情報を表示します。
from	（任意）セキュリティ アソシエーションの始点を指定します。
to	（任意）セキュリティ アソシエーションの終点を指定します。
ip-address	（任意）IP アドレスを指定したネイバーに関する情報。
hostname	（任意）特定のホストに関する情報。

コマンド モード

ユーザ EXEC（<）
特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(15)T	このコマンドが導入されました。
12.0(29)S	オプションの **from** および **to** キーワードが追加されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

RSVP が他の RSVP ネイバーと確立したセキュリティ アソシエーションを表示するには、show ip rsvp authentication コマンドを使用します。すべてのセキュリティ アソシエーションを表示するか、特定の RSVP ネイバーの IP アドレスまたはホスト名を指定できます。表示サイズには制限があります。

ip-address と *hostname* 引数の違いは、IP アドレスまたは名前でネイバーを指定することです。

例

次に、**showiprsvpauthenticationcommand** の出力例を示します。

```
Router# show ip rsvp authentication
Codes: S - static, D - dynamic, N - neighbor, I -interface, C - chain
From            To              I/F      Mode    Key-Source Key-ID       Code
192.168.102.1   192.168.104.3   Et2/2    Send    RSVPKey    1            DNC
192.168.104.1   192.168.104.3   Et2/2    Send    RSVPKey    1            DNC
192.168.104.1   192.168.104.3   AT1/0.1  Send    RSVPKey    1            DNC
192.168.106.1   192.168.104.3   AT1/0.1  Send    RSVPKey    1            DNC
```

```
192.168.106.1   192.168.106.2   AT1/0.1  Send    RSVPKey    1            DNC
192.168.106.2   192.168.104.1   AT1/0.1  Receive RSVPKey    1            DNC
192.168.106.2   192.168.106.1   AT1/0.1  Receive RSVPKey    1            DNC
```

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 *85 : show ip rsvp authentication* フィールドの説明

フィールド	説明
Codes	キーは、static（手動設定）または dynamic（ACL 単位キーから作成、または Kerberos などのキー管理サーバから取得）です。Cisco IOS ソフトウェアでは、キー管理サーバからのダイナミック キーは現在サポートされていません。このフィールドに文字列 per-neighbor が含まれている場合、セキュリティ アソシエーションではネイバー単位キーが使用されています。このフィールドに文字列 per-interface が含まれている場合、セキュリティ アソシエーションではインターフェイス単位キーが使用されています。このフィールドに文字列 chain が含まれている場合、セキュリティアソシエーションのキーは Key Source に指定されたキー チェーンから取得されます。
From	セキュリティ アソシエーションの始点。
To	セキュリティ アソシエーションの終点。
I/F	セキュリティアソシエーションが保持されているインターフェイスの名前および番号。
Mode	特定の RSVP ネイバーの RSVP メッセージを送受信するために保持されている個別のアソシエーション。有効な値は、**Send** または **Receive** です。
Key-Source	キーが設定されている場所を示します。
Key-ID	IP アドレスと組み合わせて、セキュリティアソシエーションを一意に識別するための文字列。per-interface **iprsvpauthenticationkey** コマンドを使用すれば、Cisco IOS ソフトウェアで自動的にキー ID が生成されますが、ネイバー単位またはインターフェイス単位 RSVP キーのキー チェーンを使用する場合、Cisco IOS ソフトウェアでキー ID が設定されます。キー ID は、他の RSVP プラットフォームで設定可能です。送信元が送信した RSVP 認証済みメッセージすべてにキー ID が割り当てられ、すべての受信者がこれを保存します。 （注） **KeyExpired** ：このフィールド内では、このネイバーに使用可能なキーがすべて期限切れになっていることを意味します。
コード（Code）	使用するキー ID のタイプを示します。

次は、s**howiprsvpauthentication** detail コマンドの出力例です。

```
Router# show ip rsvp authentication detail
From:                   192.168.102.1
```

```
To:                     192.168.104.3
Neighbor:               192.168.102.2
Interface:              Ethernet2/2
Mode:                   Send
Key ID:                 1
Key ACL:                R2 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 01000411
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:17:08
Challenge:              Supported
Window size:            1
Last seq # sent:        14167519095569779135
From:                   192.168.104.1
To:                     192.168.104.3
Neighbor:               192.168.102.2
Interface:              Ethernet2/2
Mode:                   Send
Key ID:                 1
Key ACL:                R2 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 0400040F
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:22:06
Challenge:              Supported
Window size:            1
Last seq # sent:        14167520384059965440
From:                   192.168.104.1
To:                     192.168.104.3
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Send
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 02000404
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:16:37
Challenge:              Supported
Window size:            1
Last seq # sent:        14167518979605659648
From:                   192.168.106.1
To:                     192.168.104.3
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Send
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 01000408
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:11:37
Challenge:              Supported
Window size:            1
Last seq # sent:        14167517691115473376
From:                   192.168.106.1
```

```
To:                     192.168.106.2
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Send
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 8D00040E
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:29:29
Challenge:              Supported
Window size:            1
Last seq # sent:        14167808344437293057
From:                   192.168.106.2
To:                     192.168.104.1
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Receive
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 CD00040A
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:29:33
Challenge:              Not configured
Window size:            1
Last seq # rcvd:        14167808280012783626
From:                   192.168.106.2
To:                     192.168.106.1
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Receive
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 C0000412
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:29:33
Challenge:              Not configured
Window size:            1
Last seq # rcvd:        14167808280012783619
```

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 *86 : show ip rsvp authentication detail* フィールドの説明

フィールド	説明
From	セキュリティ アソシエーションの始点。
To	セキュリティ アソシエーションの終点。
Neighbor	セキュリティ アソシエーションが保持されている RSVP ネイバーの IP アドレス。

フィールド	説明
Interface	セキュリティ アソシエーションが保持されているインターフェイスの名前および番号。
Mode	特定の RSVP ネイバーの RSVP メッセージを送受信するために保持されている個別のアソシエーション。有効な値は、Send または Receive です。
Key ID	IP アドレスと組み合わせて、セキュリティ アソシエーションを一意に識別するための文字列。per-interface **iprsvpauthenticationkey** コマンドを使用すれば、Cisco IOS ソフトウェアで自動的にキー ID が生成されますが、ネイバー単位またはインターフェイス単位 RSVP キーのキー チェーンを使用する場合、Cisco IOS ソフトウェアでキー ID が設定されます。キー ID は、他の RSVP プラットフォームで設定可能です。送信元が送信した RSVP 認証済みメッセージすべてにキー ID が割り当てられ、すべての受信者がこれを保存します。 （注） **KeyExpired** ：このフィールド内では、このネイバーに使用可能なキーがすべて期限切れになっていることを意味します。
Key ACL	dynamic、chain などのキー タイプの場合、このフィールドはネイバーに一致した ACL を示します。つまり、使用するキー チェーンを示します。有効な値は次のとおりです。 • **populated**：ACL のエントリが存在します。 • **removed** ：設定から ACL が削除されています。
Key Source	キーが設定済みかどうか、有効かどうかを示します。キーチェーンの場合、キー チェーンの名前を示します。Key ID フィールドはチェーン内の現在使用中のキーを示します。インターフェイス単位キーの場合、このキーで設定されたインターフェイスの名前を示します。
Key Type	static（手動設定）または dynamic（ACL 単位キーから作成、または Kerberos などのキー管理サーバから取得）。 （注） Cisco IOS ソフトウェアでは、キー管理サーバからのダイナミック キーは現在サポートされていません。
Handle	経理目的でRSVPによってセキュリティ アソシエーションに割り当てられた内部データ ベース ID。
Hash Type	ネイバーで使用するセキュア ハッシュ アルゴリズムのタイプ。
Lifetime	セキュリティ アソシエーションが期限切れになるまでの最大時間（時間、分、および秒単位）。 （注） これはキーの有効期間ではありません。キーの有効期間を取得するには、**showkeychain** コマンドを使用します。

フィールド	説明
Expires	セキュリティ アソシエーションが期限切れになるまでの残り時間（日、時間、分、および秒単位）。 （注） これは現在のキーの期限ではありません。キーの期限を取得するには、**showkeychain** コマンドを使用します。
Challenge	receive タイプのセキュリティ アソシエーションの場合、有効な値は **NotConfigured**、**Completed**、**InProgress**、および **Failed** です。send タイプのセキュリティ アソシエーションの場合、値は **Supported** です。Cisco IOS ソフトウェアは常にチャレンジに応答できますが、シスコ以外のネイバーではチャレンジが実装されていない場合があります。
Window size	receive タイプのセキュリティ アソシエーションのウィンドウ サイズ、およびリプレイ アタックを疑うまでに、順序が不正であっても受信することを許容する認証済み RSVP メッセージの最大数を示します。
Last seq # sent	send タイプのセキュリティ アソシエーションにのみ表示されます。最後の認証済みメッセージを RSVP ネイバーに送信するために使用するシーケンス番号を示します。この情報を使用して、特定タイプの認証問題をトラブルシューティングします。
Last valid seq # rcvd	receive タイプのセキュリティ アソシエーションにのみ表示されます。ネイバーから受信した最後の有効な RSVP メッセージの認証シーケンス番号を示します。デフォルトでは、1 つのシーケンス番号が表示されます。ただし、ip rsvp authentication window-size コマンドを使用して、認証ウィンドウ サイズを n に増やす場合、最後から n 個の有効な受信シーケンス番号が表示されます。この情報を使用して、特定タイプの認証問題をトラブルシューティングします。

関連コマンド

コマンド	説明
cleariprsvpauthentication	ライフタイムの期限が切れる前に RSVP セキュリティ アソシエーションを削除します。

show ip rsvp counters

各インターフェイスで送受信されたリソース予約プロトコル（RSVP）メッセージ数を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpcounters** コマンドを使用します。

show ip rsvp counters [authentication] [{**interface** *type number*|**neighbor** [**vrf** {******vrf-name*}]|**state teardown|summary**}]

構文の説明

authentication	（任意）RSVP 認証カウンタのリストを表示します。
interface *type number*	（任意）指定したインターフェイス名の送受信 RSVP メッセージの数を表示します。
neighbor	（任意）指定したネイバーの送受信 RSVP メッセージの数を表示します。
vrf *	（任意）設定された Virtual Routing and Forwarding（VRF）インスタンスをすべて表示します。
vrf *vrf-name*	（任意）指定した VRF の名前を表示します。
stateteardown	（任意）RSVP メッセージ状態の数とティアダウンの理由を表示します。
summary	（任意）すべてのインターフェイス上でルータによって送受信された RSVP メッセージの累積数を表示します。

コマンド デフォルト

showiprsvpcounters コマンドをオプションのキーワードを指定せずに入力すると、RSVP が設定された各インターフェイスで送受信された RSVP メッセージの数が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(14)ST	このコマンドが導入されました。
12.2(13)T	**neighbor** キーワードが追加され、このコマンドが Cisco IOS Release 12.2(13)T に統合されました。
12.2(15)T	コマンド出力が変更され、RSVP 認証が有効なインターフェイスに RSVP メッセージが着信し、そのメッセージの認証チェックに失敗するとエラー数が増えるエラー カウンタを表示するようになりました。
12.2(11)S	このコマンドが、Cisco IOS Release 12.2(11)S に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。

リリース	変更箇所
12.0(29)S	**authentication** キーワードが追加されました。コマンド出力が変更され、Hello およびメッセージ キュー情報も表示されるようになりました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
15.0(1)M	このコマンドが変更されました。**vrf** および ***** キーワードと *vrf-name* 引数が追加されました。

例

Summary の例

次の例では、すべてのインターフェイスのルータで送受信された各タイプの RSVP メッセージ数を、Hello およびメッセージ キュー情報とともに表示します。

```
Router# show ip rsvp counters summary
All Interfaces          Recv      Xmit                        Recv      Xmit
    Path                  110        15    Resv                  50        28
    PathError               0         0    ResvError              0         0
    PathTear                0         0    ResvTear               0         0
    ResvConf                0         0    RTearConf              0         0
    Ack                     0         0    Srefresh               0         0
    Hello                5555      5554    IntegrityChalle        0         0
    IntegrityRespon         0         0    DSBM_WILLING           0         0
    I_AM_DSBM               0         0
    Unknown                 0         0    Errors                 0         0
Recv Msg Queues                Current       Max
    RSVP                             0         2
    Hello (per-I/F)                  0         1
    Awaiting Authentication          0         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 *87 : show ip rsvp counters summary* フィールドの説明

フィールド	説明
All Interfaces	すべてのインターフェイスについて表示されるメッセージのタイプ。 （注） Hello はグレースフル リスタート、再ルーティング（Hello ステート タイマー）、および Fast Reroute メッセージのサマリーです。
Recv	指定したインターフェイスまたはすべてのインターフェイスで受信されたメッセージの数。

フィールド	説明
Xmit	指定したインターフェイスまたはすべてのインターフェイスから送信されたメッセージの数。
Recv Msg Queues	RSVP、インターフェイスごとのHello、および待機中の認証向けの受信メッセージ キュー。 • Current：キューイング中のメッセージの数。 • Max：過去にキューイングされたメッセージの最大数。

VRF の例

次の例では、VRF名がmyvrfの指定したネイバーのRSVPメッセージ数を表示します。

```
Router# show ip rsvp counters neighbor vrf myvrf
VRF: myvrf
Neighbor: 10.10.15.13
      Rate-Limiting:
        Output queue overflow, number of dropped RSVP messages: 0
      Refresh-Reduction:
        Number of RSVP messages received out of order: 0
        Number of retransmitted RSVP messages: 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 *88 : show ip rsvp counters neighbor vrf* フィールドの説明

フィールド	説明
VRF	VRF の名前。
Neighbor	ネイバーの IP アドレス。
Rate-Limiting	有効な rate-limiting パラメータは次のとおりです。 • Output queue overflow, number of dropped RVSP messages：キューのオーバーフロー時にネイバーによってドロップされたメッセージの数。
Refresh-Reduction	有効な refresh-reduction パラメータは次のとおりです。 • Number of RSVP messages received out of order：シーケンシャルな順番ではないためドロップされたメッセージの数。 • Number of retransmitted RSVP messages：ネイバーに再送信されたメッセージの数。

関連コマンド

コマンド	説明
clearipr svpcounters	保持されている IP RSVP カウンタをすべてクリア（0 に設定）します。

show ip rsvp counters state teardown

ティアダウン状態の原因になったリソース予約プロトコル（RSVP）イベントのカウンタを表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpcountersstateteardown** コマンドを使用します。

show ip rsvp counters state teardown

構文の説明

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	変更箇所
12.0(29)S	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

ラベルスイッチドパス（LSP）がダウン状態の場合は **showiprsvpcountersstateteardown** コマンドを使用します。グレースフル リスタートでティアダウン状態がトリガーされた場合、「例」セクションの Path、Resv-In、および Resv-Out 列の数値は 0 より大きくなります。

例

次は、**showiprsvpcountersstateteardown** コマンドの出力例です。

```
Router# show ip rsvp counters state teardown
States
  Reason for Teardown                          State torn down
                                                 Path    Resv-In   Resv-Out
  PathTear arrival                                  0          0          0
  ResvTear arrival                                  0          0          0
  Local application requested tear                  0          0          0
  Output or Input I/F went down                     0          0          0
  Missed refreshes                                  0          0          0
  Preemption                                        0          0          0
  Backup tunnel failed for FRR Active LSP           0          0          0
  Reroutabilty changed for FRR Active LSP           0          0          0
  Hello RR Client (HST) requested tear              0          0          0
  Graceful Restart (GR) requested tear              0          0          0
  Downstream neighbor SSO-restarting                0          0          0
  Resource unavailable                              0          0          0
  Policy rejection                                  0          0          0
  Policy server sync failed                         0          0          0
  Traffic control error                             0          0          0
  Error in received message                         0          0          0
```

```
Non RSVP HOP upstream, TE LSP                    0          0          0
Other                                            0          0          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 *89 : show ip rsvp counters state teardown* フィールドの説明

フィールド	説明
States	パス ステート ブロック（PSB）および予約ステート ブロック（RSB）情報を含む RSVP 状態。
Reason for Teardown	ティアダウンをトリガーしたイベント。

関連コマンド

コマンド	説明
clearipsvpcounters	保持されている IP RSVP カウンタをクリア（0 に設定）します。

show ip rsvp fast bw-protect

バックアップ帯域幅保護が有効かどうか、その保護を提供するために使用するバックアップ トンネルの状態を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpfastbw-protect** コマンドを使用します。

show ip rsvp fast bw-protect [detail] [**filter** [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]]

構文の説明

detail	（任意）追加の受信者情報を指定します。
filter	（任意）表示する受信者のサブネットを指定します。
destination *ip-address*	（任意）受信者の宛先 IP アドレスを指定します。
hostname	（任意）受信者のホスト名を指定します。
dst-port *port-number*	（任意）宛先ポート番号を指定します。有効な宛先ポート番号は、0 ～ 65535 の範囲内の値です。
source *ip-address*	（任意）受信者の送信元 IP アドレスを指定します。
src-port *port-number*	（任意）送信元ポートの番号を指定します。有効な送信元ポート番号は、0 ～ 65535 の範囲内の値です。

コマンド デフォルト

バックアップ帯域幅保護およびバックアップ トンネル状態の情報は表示されません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(29)S	このコマンドが導入されました。
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。
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました

例

次は、**showiprsvpfastbw-protect** コマンドの出力例です。

```
Router# show ip rsvp fast bw-protect
```

```
Primary          Protect  BW         Backup
Tunnel           I/F      BPS:Type   Tunnel:Label  State   BW-P    Type
---------------  -------  --------   -----------   -----   ----    ----
PRAB-72-5_t500   PO2/0    500K:S     Tu501:19      Ready   ON      Nhop
PRAB-72-5_t601   PO2/0    103K:S     Tu501:20      Ready   OFF     Nhop
PRAB-72-5_t602   PO2/0    70K:S      Tu501:21      Ready   ON      Nhop
PRAB-72-5_t603   PO2/0    99K:S      Tu501:22      Ready   ON      Nhop
PRAB-72-5_t604   PO2/0    100K:S     Tu501:23      Ready   OFF     Nhop
PRAB-72-5_t605   PO2/0    101K:S     Tu501:24      Ready   OFF     Nhop
```

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 *90 : show ip rsvp fast bw-protect* フィールドの説明

フィールド	説明
Primary Tunnel	保護されているトンネルの ID。
Protect I/F	インターフェイス名。
BW BPS:Type	帯域幅（bps）および帯域幅のタイプ。可能な値は次のとおりです。 • S：サブプール • G：グローバル プール
Backup Tunnel:Label	バックアップ トンネルの ID。
State	バックアップ トンネルの状態有効な値は次のとおりです。 • Ready：データはプライマリ トンネルを通過していますが、プライマリ トンネルがダウンした場合はバックアップ トンネルに切り替わります。 • Active：プライマリ トンネルがダウンしたため、バックアップ トンネルがトラフィックに使用されています。 • None：バックアップ トンネルはありません。
BW-P	バックアップ帯域幅保護の状態。有効な値は、ON または OFF です。
Type	バックアップ トンネルのタイプ。可能な値は次のとおりです。 • Nhop：ネクスト ホップ • NNHOP：ネクスト ネクスト ホップ

関連コマンド

コマンド	説明
tunnelmplstraffic-engfast-reroutebw-protect	MPLS TE トンネルが、リンクまたはノードの障害発生時に、確立されたバックアップ トンネルを使用できるようにします。

show ip rsvp fast detail

リソース予約プロトコル（RSVP）カテゴリ固有の情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpfastdetail** コマンドを使用します。

show ip rsvp fast detail [**filter** [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]]

構文の説明

filter	（任意）表示する受信者のサブネットを指定します。
destination *ip-address*	（任意）受信者の宛先 IP アドレスを指定します。
hostname	（任意）受信者のホスト名を指定します。
dst-port *port-number*	（任意）宛先ポート番号を指定します。有効な宛先ポート番号は、0 ～ 65535 の範囲内の値です。
source *ip-address*	（任意）受信者の送信元 IP アドレスを指定します。
src-port *port-number*	（任意）送信元ポートの番号を指定します。有効な送信元ポート番号は、0 ～ 65535 の範囲内の値です。

コマンド デフォルト

RSVP カテゴリ固有の情報は表示されません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(24)S	このコマンドが導入されました。
12.0(29)S	必要な Bandwidth Prot がコマンド出力の Flag フィールドに追加されました。
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。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

例

次に、**show ip rsvp fast detail** コマンドの出力例を示します。

```
Router# show ip rsvp fast detail

PATH:
  Tun Dest:   10.0.0.7  Tun ID: 500  Ext Tun ID: 10.0.0.5
  Tun Sender: 10.0.0.5  LSP ID: 8
  Path refreshes:
    sent:     to   NHOP 10.5.6.6 on POS2/0
  Session Attr:
```

```
  Setup Prio: 7, Holding Prio: 7
  Flags: Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
  Session Name: PRAB-72-5_t500
ERO: (incoming)
  10.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.5.6 (Strict IPv4 Prefix, 8 bytes, /32)
  10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
ERO: (outgoing)
  10.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
  10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
Fast-Reroute Backup info:
  Inbound  FRR: Not active
  Outbound FRR: Ready -- backup tunnel selected
    Backup Tunnel: Tu501      (label 19)
    Bkup Sender Template:
      Tun Sender: 10.5.6.5  LSP ID: 8
    Bkup FilerSpec:
      Tun Sender: 10.5.6.5, LSP ID: 8
Path ID handle: 04000405.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxied
Output on POS2/0. Policy status: Forwarding. Handle: 02000406
```

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 *91 : show ip rsvp fast detail* フィールドの説明

フィールド	説明
Tun Dest	受信者の IP アドレス。
Tun ID	トンネル ID 番号。
Ext Tun ID	拡張トンネル ID 番号。
Tun Sender	送信元の IP アドレス。
LSP ID	ラベルスイッチド パス ID 番号。
Setup Prio	確立プライオリティ。
Holding Prio	ホールディング プライオリティ。
Flags	バックアップ帯域幅保護がラベルスイッチド パス（LSP）に設定されています。
Session Name	セッションの名前を指定します。
ERO (incoming)	着信 path メッセージの EXPLICIT_ROUTE オブジェクト。
ERO (outgoing)	発信 path メッセージの EXPLICIT_ROUTE オブジェクト。
Traffic params Rate	平均レート（ビット/秒）です。

フィールド	説明
Max. burst	最大バースト サイズ（バイト）。
Min Policed Unit	最小ポリシング単位（バイト）。
Max Pkt Size	最大パケット サイズ（バイト）。
Inbound FRR	着信 Fast Reroute（FRR）バックアップ トンネルの状態。このノードが再ルーティングされた LSP の下流にある（この LSP のマージ ポイントなど）場合、状態はアクティブです。
Outbound FRR	発信 FRR バックアップ トンネルの状態。このノードが、LSP のローカル修復点（PLR）である場合、次の 3 つの状態があります。 • Active：おそらくダウンストリーム障害があったため、この LSP はアクティブにバックアップ トンネルを使用しています。 • No Backup：この LSP にはローカルの（Fast Reroute）保護がありません。障害時に使用するためのバックアップ トンネルが選択されていません。 • Ready：この LSP は、ダウンストリーム リンクまたはノードの障害発生時にバックアップ トンネルが使用できます。障害時に使用するためのバックアップ トンネルが選択されています。
Backup Tunnel	発信 FRR 状態が Ready または Active の場合、このフィールドには次の内容が表示されます。 • 障害時に使用するためこの LSP に選択されているバックアップ トンネル。 • バックアップ トンネルテール（マージポイント）で受信するため、LSP のデータ パケットの先頭に追加される着信ラベル。
Bkup Sender Template	発信 FRR 状態が Ready または Active の場合、SENDER_TEMPLATE および FILTERSPEC オブジェクトが表示されます。LSP がアクティブにバックアップ トンネルの使用を開始すると、これらのオブジェクトは、バックアップ トンネルから送信される RSVP メッセージ内で使用されます。ノード（PLR）はオリジナルの発信元ではなく、それ自身の IP アドレスを使用するという点のみが、これらのオブジェクトとオリジナル（障害前）のオブジェクトとは異なります。たとえば、path メッセージおよび pathTear メッセージには、新しい SENDER_TEMPLATE が含まれます。Resv メッセージおよび resvTear メッセージには、新しい FILTERSPEC オブジェクトが含まれます。この LSP がアクティブにバックアップ トンネルの使用を開始する場合、表示が変化します。

フィールド	説明
Bkup FilerSpec	発信 FRR 状態が Ready または Active の場合、SENDER_TEMPLATE および FILTERSPEC オブジェクトが表示されます。LSP がアクティブにバックアップ トンネルの使用を開始すると、これらのオブジェクトは、バックアップ トンネルから送信される RSVP メッセージ内で使用されます。ノード（PLR）はオリジナルの発信元ではなく、それ自身の IP アドレスを使用するという点のみが、これらのオブジェクトとオリジナル（障害前）のオブジェクトとは異なります。たとえば、path および pathTear メッセージには、新しい SENDER_TEMPLATE が含まれます。Resv および resvTear メッセージには、新しい FILTERSPEC オブジェクトが含まれます。この LSP がアクティブにバックアップ トンネルの使用を開始する場合、表示が変化します。
Path ID handle	保護スイッチ バイト（PSB）の識別子。
Incoming policy	LSP のポリシー判定。トンネルの着信 path メッセージに RSVP ポリシーが許可されていなかった場合、LSP はアップになりません。Accepted が表示されます。
Policy source(s)	FRR LSP の場合、ポリシー ソースの値は常に MPLS/TE です。
Status	FRR LSP の場合、有効な値は次のとおりです。 • Proxied：ヘッドエンド ルータ。 • Proxied Terminated：テールエンド ルータ。 ミッドポイント ルータの場合、このフィールドは常に空白です。

関連コマンド

コマンド	説明
mplstraffic-engfast-reroutebackup-prot-preemption	バックアップ保護プリエンプション アルゴリズムを変更して、有効に使用されていない帯域幅量を最小化します。

show ip rsvp fast-reroute

高速再ルーティング プライマリ トンネルと、これに対応して保護を提供するバックアップ トンネルの情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpfast-reroute** コマンドを使用します。

show ip rsvp fast-reroute [**filter** [**session-type** {*session-type-number*|**all**}]]

構文の説明

filter	（任意）表示するトンネルのサブネットを指定します。
session-type *session-type-number*	（任意）表示するトンネルのタイプを指定します。有効な値は次のとおりです。 • **7**（IPv4 ポイントツーポイント（P2P）トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）トンネル セッションの場合）。 • **13**（IPv4 ポイントツーマルチポイント（P2MP）TE LSP トンネル セッションの場合）
session-typeall	（任意）トンネル セッションのすべてのタイプを指定します。

コマンド デフォルト

引数を指定しない場合は、すべての高速再ルーティング プライマリ トンネルの情報が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(27)S	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
12.2(33)SRE	このコマンドが変更されました。**filter** キーワードが追加され、ポイントツーポイントとポイントツーマルチポイント別にトンネル情報が表示されるようになりました。出力が更新され、マルチプロトコル ラベル スイッチング（MPLS）TE P2MP の情報が表示されるようになりました。
15.0(1)M	このコマンドが変更されました。クラシック IP RSVP（セッション タイプ 1）のサポートが削除されました。

例

次は、高速再ルーティング プライマリ トンネルと、これに対応して保護を提供するバックアップ トンネルの出力例です。

```
Router# show ip rsvp fast-reroute
Primary                 Protect BW         Backup
Tunnel                  I/F     BPS:Type   Tunnel:Label  State  Level  Type
------                  ------- --------   ------------- ------ -----  ---
GSR1---R2---_t65336     PO1/0   0:G        Tu1002:0      Ready  any-unl Nhop
GSR1---R2---_t65338     PO4/0   0:G        Tu1004:0      Ready  any-unl Nhop
```

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 *92 : show ip rsvp fast-reroute* フィールドの説明

フィールド	説明
Primary Tunnel	ホスト名とトンネル ID。
Protect I/F	保護されているインターフェイス。
BW BPS:Type	帯域幅（bps）と帯域幅を供給するプール。有効な値は、G（グローバル プール）と S（サブプール）です。
Backup Tunnel:Label	バックアップ トンネル ID とラベル。
State	保護の状態。有効な値は、Ready、Active、および None です。
Level	帯域幅のレベル。有効な値は、any と unl（無制限）です。
Type	バックアップ トンネルのタイプ：Nhop（ネクスト ホップ）または NNhop（ネクスト ネクスト ホップ）。

次の例では、高速再ルーティング プライマリ トンネルと、これに対応するバックアップ トンネルを表示します。この情報は、P2P LSP と P2MP サブ LSP に分類されます。次の例では、6 つのサブ LSP（イーサネット インターフェイス 0/0 で保護される 3 つとイーサネット インターフェイス 0/1 で保護される 3 つ）が含まれる Tunnel 22 を表示します。

```
Router# show ip rsvp fast-reroute
P2P                         Protect BW         Backup
Protected LSP               I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------               ------- --------   ------------- ------ -----   ------
R201_t1                     Et0/1   500K:G     Tu777:16      Ready  any-lim Nhop
P2MP
Protected Sub-LSP                           Protect BW         Backup
src_lspid[subid]->dst_tunid                 I/F     BPS:Type   Tunnel:Label  State
---------------------------                 ------- --------   ------------- ------
10.1.1.201_1[1]->10.1.1.203_22                Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[2]->10.1.1.206_22                Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[3]->10.1.1.213_22                Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[4]->10.1.1.214_22                Et0/1   500K:G     None          None
10.1.1.201_1[5]->10.1.1.216_22                Et0/1   500K:G     None          None
10.1.1.201_1[6]->10.1.1.217_22                Et0/1   500K:G     None          None
```

次の例では、Cisco IOS Release 12.4(24)T 以前のリリースで、高速再ルーティング プライマリ トンネルと、これに対応するバックアップ トンネルの情報を表示します。出力は、セッション タイプ別に表示されます。

```
Rrouter# show ip rsvp fast-reroute filter session-type all

Session Type 1 (rsvp)
P2P                       Protect BW         Backup
Protected LSP             I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------             ------- --------   ------------- ------ -----   ------
Session Type 7 (te-p2p-lsp)
P2P                       Protect BW         Backup
Protected LSP             I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------             ------- --------   ------------- ------ -----   ------
R201_t1                   Et0/1   500K:G     Tu777:16      Ready  any-lim Nhop
Session Type 13 (te-p2mp-lsp)
P2MP
Protected Sub-LSP                          Protect BW         Backup
src_lspid[subid]->dst_tunid                I/F     BPS:Type   Tunnel:Label  State
---------------------------                ------- --------   ------------- ------
10.1.1.201_1[1]->10.1.1.203_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[2]->10.1.1.206_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[3]->10.1.1.213_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[4]->10.1.1.214_22               Et0/1   500K:G     None          None
10.1.1.201_1[5]->10.1.1.216_22               Et0/1   500K:G     None          None
10.1.1.201_1[6]->10.1.1.217_22               Et0/1   500K:G     None          None
```

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 *93 : show ip rsvp fast-reroute Point-to-Multipoint* フィールドの説明

フィールド	説明
Protected LSP	保護されている LSP とトンネル ID。
Protected Sub-LSP src_lspid[subid]->dst_tunid	保護されているサブ LSP の送信元と宛先アドレス。P2MP ID は、送信元アドレスに追加されます。トンネル ID は、宛先アドレスに追加されます。

次の例では、Cisco IOS Release 15.0(1)M 以降のリリースで、高速再ルーティング プライマリ トンネルと、これに対応して保護を提供するバックアップ トンネルの情報を表示します。

```
Rrouter# show ip rsvp fast-reroute filter session-type all

Session Type 7 (te-p2p-lsp)
P2P                       Protect BW         Backup
Protected LSP             I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------             ------- --------   ------------- ------ -----   ------
p2mp-2_t12                Se3/0   500K:G     Tu700:0       Ready  any-unl Nhop
p2mp-2_t13                Se3/0   500K:G     Tu700:0       Ready  any-unl Nhop
Session Type 13 (te-p2mp-lsp)
P2MP
*Protected Sub-LSP                         Protect BW         Backup
src_lspid[subid]->dst_tunid                I/F     BPS:Type   Tunnel:Label  State
---------------------------                ------- --------   ------------- ------
10.2.0.1_12[1]->10.1.0.1_1                 Se5/0   1M:G       None          None
```

```
10.2.0.1_12[3]->10.2.3.3_1              Se3/0   1M:G        Tu700:16      Ready
10.2.0.1_12[5]->10.3.0.1_1              Se3/0   1M:G        Tu700:16      Ready
10.2.0.1_12[6]->10.3.4.3_1              Se3/0   1M:G        Tu700:16      Ready
10.2.0.1_12[8]->10.2.5.3_1              Se6/0   1M:G        Tu100:17      Ready
```

関連コマンド

コマンド	説明
mplstraffic-engauto-tunnelprimaryconfig	明示的なアドレスを使用せずに IP 処理を有効にします。
mplstraffic-engauto-tunnelprimaryconfigmplsip	プライマリ自動トンネルで LDP をイネーブルにします。
mplstraffic-engauto-tunnelprimaryonehop	すべてのネクストホップへのプライマリ トンネルを自動的に作成します。
mplstraffic-engauto-tunnelprimarytimers	障害の発生したプライマリ自動トンネルの削除後の秒数を設定します。
mplstraffic-engauto-tunnelprimarytunnel-num	プライマリ自動トンネル用のトンネルインターフェイス番号の範囲を設定します。

show ip rsvp fast-reroute bw-protect

バックアップ帯域幅保護が有効かどうか、その保護を提供するために使用するバックアップ トンネルの状態を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpfast-reroutebw-protect** コマンドを使用します。

show ip rsvp fast-reroute bw-protect [detail] [**filter** [**session-type** {*session-type-number*|**all**}] [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]]

構文の説明

detail	（任意）追加の受信者情報を指定します。
filter	（任意）表示する受信者のサブネットを指定します。
session-type *session-type-number*	（任意）表示するリソース予約プロトコル（RSVP）セッションのタイプを指定します。有効な値は次のとおりです。 • **1**（IPv4 セッションの場合） • **7**（IPv4 ポイントツーポイント トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）トンネル セッションの場合） • **13**（IPv4 ポイントツーマルチポイント TE LSP トンネル セッションの場合）
all	（任意）RSVP セッションのすべてのタイプを指定します。
destination *ip-address*	（任意）受信者の宛先 IP アドレスを指定します。
hostname	（任意）受信者のホスト名を指定します。
dst-port *port-number*	（任意）宛先ポート番号を指定します。有効な宛先ポート番号は、0 ～ 65535 の範囲内の値です。
source *ip-address*	（任意）受信者の送信元 IP アドレスを指定します。
src-port *port-number*	（任意）送信元ポートの番号を指定します。有効な送信元ポート番号は、0 ～ 65535 の範囲内の値です。

コマンド デフォルト

バックアップ帯域幅保護およびバックアップ トンネル状態の情報は表示されません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(29)S	このコマンドが導入されました。

リリース	変更箇所
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。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
12.2(33)SRE	このコマンドが変更されました。**session-type** キーワードが追加され、指定したタイプのトンネルが表示されるようになりました。出力が変更され、マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）ポイントツーマルチポイント（P2MP）の情報が表示されるようになりました。

例

次は、**showiprsvpfast-reroutebw-protect** コマンドの出力例です。

```
Router# show ip rsvp fast-reroute bw-protect

Primary          Protect  BW         Backup
Tunnel           I/F      BPS:Type   Tunnel:Label  State   BW-P    Type
---------------  -------  ---------  -----------   -----   ----    ----
PRAB-72-5_t500   PO2/0    500K:S     Tu501:19      Ready   ON      Nhop
PRAB-72-5_t601   PO2/0    103K:S     Tu501:20      Ready   OFF     Nhop
PRAB-72-5_t602   PO2/0    70K:S      Tu501:21      Ready   ON      Nhop
PRAB-72-5_t603   PO2/0    99K:S      Tu501:22      Ready   ON      Nhop
PRAB-72-5_t604   PO2/0    100K:S     Tu501:23      Ready   OFF     Nhop
PRAB-72-5_t605   PO2/0    101K:S     Tu501:24      Ready   OFF     Nhop
```

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 *94 : show ip rsvp fast-reroute bw-protect* フィールドの説明

フィールド	説明
Primary Tunnel	保護されているトンネルの ID。
Protect I/F	インターフェイス名。
BW BPS:Type	帯域幅（bps）および帯域幅のタイプ。可能な値は次のとおりです。 • S：サブプール • G：グローバル プール
Backup Tunnel:Label	バックアップ トンネルの ID。

フィールド	説明
State	バックアップ トンネルの状態有効な値は次のとおりです。 • Ready：データはプライマリ トンネルを通過していますが、プライマリ トンネルがダウンした場合はバックアップ トンネルに切り替わります。 • Active：プライマリ トンネルがダウンしたため、バックアップ トンネルがトラフィックに使用されています。 • None：バックアップ トンネルはありません。
BW-P	バックアップ帯域幅保護の状態。有効な値は、ON または OFF です。
Type	バックアップ トンネルのタイプ。有効な値は次のとおりです。 • Nhop：ネクスト ホップ • NNHOP：ネクスト ネクスト ホップ

次の例では、高速再ルーティング プライマリ トンネルと、これに対応して保護を提供するバックアップ トンネルを表示します。この情報は、ポイントツーポイント（P2P）ラベル スイッチド パス（LSP）と P2MP サブ LSP に分類されます。次の例では、6 つのサブ LSP（イーサネット インターフェイス 0/0 で保護される 3 つとイーサネット インターフェイス 0/1 で保護される 3 つ）が含まれる Tunnel 22 を表示します。

```
Router# show ip rsvp fast-reroute bw-protect

P2P                          Protect BW          Backup
Protected LSP                I/F     BPS:Type    Tunnel:Label  State  BW-P    Type
-------------                ------- --------    ------------- ------ -----   ------
R201_t1                      Et0/1   500K:G      Tu777:16      Ready  ON      Nhop
P2MP
Protected Sub-LSP                              Protect BW          Backup
src_lspid[subid]->dst_tunid                    I/F     BPS:Type    Tunnel:Label  BW-P
---------------------------                    ------- --------    ------------- ------
10.1.1.201_1[1]->10.1.1.203_22                   Et0/0   500K:G      Tu666:20      ON
10.1.1.201_1[2]->10.1.1.206_22                   Et0/0   500K:G      Tu666:20      ON
10.1.1.201_1[3]->10.1.1.213_22                   Et0/0   500K:G      Tu666:20      ON
10.1.1.201_1[4]->10.1.1.214_22                   Et0/1   500K:G      None          None
10.1.1.201_1[5]->10.1.1.216_22                   Et0/1   500K:G      None          None
10.1.1.201_1[6]->10.1.1.217_22                   Et0/1   500K:G      None          None
```

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 *95 : show ip rsvp fast-reroute bw-protect Point-to-Multipoint* フィールドの説明

フィールド	説明
Protected LSP	保護されている LSP とトンネル ID。

フィールド	説明
Protected Sub-LSP src_lspid[subid]->dst_tunid	保護されているサブ LSP の送信元と宛先アドレス。P2MP ID は、送信元アドレスに追加されます。トンネル ID は、宛先アドレスに追加されます。

関連コマンド

コマンド	説明
tunnelmplstraffic-engfast-reroutebw-protect	MPLS TE トンネルが、リンクまたはノードの障害発生時に、確立されたバックアップ トンネルを使用できるようにします。

show ip rsvp fast-reroute detail

リソース予約プロトコル（RSVP）カテゴリ固有の情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpfast-reroutedetail** コマンドを使用します。

show ip rsvp fast-reroute detail [**filter** [**session-type** {*session-type-number*|**all**}] [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]]

構文の説明

filter	（任意）表示する受信者のサブネットを指定します。
session-type *session-type-number*	（任意）表示する RSVP セッションのタイプを指定します。有効な値は次のとおりです。 • **1**（IPv4 セッションの場合） • **7**（IPv4 ポイントツーポイント（P2P）トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）トンネル セッションの場合） • **13**（IPv4 ポイントツーマルチポイント（P2MP）TE LSP トンネル セッションの場合）
all	（任意）RSVP セッションのすべてのタイプを指定します。
destination *ip-address*	（任意）受信者の宛先 IP アドレスを指定します。
hostname	（任意）受信者のホスト名を指定します。
dst-port *port-number*	（任意）宛先ポート番号を指定します。有効な宛先ポート番号は、0 ～ 65535 の範囲内の値です。
source *ip-address*	（任意）受信者の送信元 IP アドレスを指定します。
src-port *port-number*	（任意）送信元ポートの番号を指定します。有効な送信元ポート番号は、0 ～ 65535 の範囲内の値です。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(24)S	このコマンドが導入されました。
12.0(29)S	必要な Bandwidth Prot がコマンド出力の Flag フィールドに追加されました。
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。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

リリース	変更箇所
12.2(33)SRE	このコマンドが変更されました。**session-type** キーワードが追加され、指定したタイプのトンネルが表示されるようになりました。出力が変更され、MPLS TE P2MP の情報が表示されるようになりました。

例

次に、**show ip rsvp fast-reroute detail** コマンドの出力例を示します。

```
Router# show ip rsvp fast-reroute detail

PATH:
  Tun Dest:   10.0.0.7  Tun ID: 500  Ext Tun ID: 10.0.0.5
  Tun Sender: 10.0.0.5  LSP ID: 8
  Path refreshes:
    sent:     to   NHOP 10.5.6.6 on POS2/0
  Session Attr:
    Setup Prio: 7, Holding Prio: 7
    Flags: Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
    Session Name: PRAB-72-5_t500
  ERO: (incoming)
    10.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.5.6 (Strict IPv4 Prefix, 8 bytes, /32)
    10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  ERO: (outgoing)
    10.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
    10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Fast-Reroute Backup info:
    Inbound  FRR: Not active
    Outbound FRR: Ready -- backup tunnel selected
      Backup Tunnel: Tu501      (label 19)
      Bkup Sender Template:
        Tun Sender: 10.5.6.5  LSP ID: 8
      Bkup FilerSpec:
        Tun Sender: 10.5.6.5, LSP ID: 8
  Path ID handle: 04000405.
  Incoming policy: Accepted. Policy source(s): MPLS/TE
  Status: Proxied
  Output on POS2/0. Policy status: Forwarding. Handle: 02000406
```

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 *96 : show ip rsvp fast-reroute detail* フィールドの説明

フィールド	説明
Tun Dest	受信者の IP アドレス。
Tun ID	トンネル ID 番号。
Ext Tun ID	拡張トンネル ID 番号。
Tun Sender	送信元の IP アドレス。

フィールド	説明
LSP ID	ラベル スイッチド パス ID 番号。
Setup Prio	確立プライオリティ。
Holding Prio	ホールディング プライオリティ。
Flags	バックアップ帯域幅保護がラベル スイッチドパスに設定されています。
Session Name	セッションの名前を指定します。
ERO (incoming)	着信 path メッセージの EXPLICIT_ROUTE オブジェクト。
ERO (outgoing)	発信 path メッセージの EXPLICIT_ROUTE オブジェクト。
Traffic params Rate	平均レート（ビット/秒）です。
Max. burst	最大バースト サイズ（バイト）。
Min Policed Unit	最小ポリシング単位（バイト）。
Max Pkt Size	最大パケット サイズ（バイト）。
Inbound FRR	着信 Fast Reroute（FRR）バックアップ トンネルの状態。このノードが再ルーティングされた LSP の下流にある（この LSP のマージ ポイントなど）場合、状態はアクティブです。
Outbound FRR	発信 FRR バックアップ トンネルの状態。このノードが、LSP のローカル修復点（PLR）である場合、次の 3 つの状態があります。 • Active：おそらくダウンストリーム障害があったため、この LSP はアクティブにバックアップ トンネルを使用しています。 • No Backup：この LSP にはローカルの（Fast Reroute）保護がありません。障害時に使用するためのバックアップ トンネルが選択されていません。 • Ready：この LSP は、ダウンストリーム リンクまたはノードの障害発生時にバックアップ トンネルが使用できます。障害時に使用するためのバックアップ トンネルが選択されています。
Backup Tunnel	発信 FRR 状態が Ready または Active の場合、このフィールドには次の内容が表示されます。 • 障害時に使用するためこの LSP に選択されているバックアップ トンネル。 • バックアップ トンネルテール（マージポイント）で受信するため、LSP のデータ パケットの先頭に追加される着信ラベル。

フィールド	説明
Bkup Sender Template	発信 FRR 状態が Ready または Active の場合、SENDER_TEMPLATE および FILTERSPEC オブジェクトが表示されます。LSP がアクティブにバックアップ トンネルの使用を開始すると、これらのオブジェクトは、バックアップ トンネルから送信される RSVP メッセージ内で使用されます。ノード（PLR）はオリジナルの発信元ではなく、それ自身の IP アドレスを使用するという点のみが、これらのオブジェクトとオリジナル（障害前）のオブジェクトとは異なります。たとえば、path および pathTear メッセージには、新しい SENDER_TEMPLATE が含まれます。Resv および resvTear メッセージには、新しい FILTERSPEC オブジェクトが含まれます。この LSP がアクティブにバックアップ トンネルの使用を開始する場合、表示が変化します。
Bkup FilerSpec	発信 FRR 状態が Ready または Active の場合、SENDER_TEMPLATE および FILTERSPEC オブジェクトが表示されます。LSP がアクティブにバックアップ トンネルの使用を開始すると、これらのオブジェクトは、バックアップ トンネルから送信される RSVP メッセージ内で使用されます。ノード（PLR）はオリジナルの発信元ではなく、それ自身の IP アドレスを使用するという点のみが、これらのオブジェクトとオリジナル（障害前）のオブジェクトとは異なります。たとえば、path および pathTear メッセージには、新しい SENDER_TEMPLATE が含まれます。Resv および resvTear メッセージには、新しい FILTERSPEC オブジェクトが含まれます。この LSP がアクティブにバックアップ トンネルの使用を開始する場合、表示が変化します。
Path ID handle	保護スイッチ バイト（PSB）の識別子。
Incoming policy	LSP のポリシー判定。トンネルの着信 path メッセージに RSVP ポリシーが許可されていなかった場合、LSP はアップになりません。Accepted が表示されます。
Policy source(s)	FRR LSP の場合、ポリシー ソースの値は常に MPLS/TE です。
Status	FRR LSP の場合、有効な値は次のとおりです。 • Proxied：ヘッドエンド ルータ。 • Proxied Terminated：テールエンド ルータ。 ミッドポイント ルータの場合、このフィールドは常に空白です。

次の例では、P2MP データを表示します。

```
Router# show ip rsvp fast-reroute detail

PATH:
  P2MP ID: 22  Tun ID: 22  Ext Tun ID: 10.1.1.201
  Tun Sender: 10.1.1.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
```

```
SubGroup ID: 2
S2L Destination : 10.1.1.206
Path refreshes:
  sent:     to   NHOP 10.0.0.205 on Ethernet0/0
Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0xF) Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
  Session Name: R201_t22
ERO: (incoming)
  10.1.1.201 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.201 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
  10.1.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
  10.1.0.206 (Strict IPv4 Prefix, 8 bytes, /32)
  10.1.1.206 (Strict IPv4 Prefix, 8 bytes, /32)
ERO: (outgoing)
  10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
  10.1.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
  10.1.0.206 (Strict IPv4 Prefix, 8 bytes, /32)
  1o.1.1.206 (Strict IPv4 Prefix, 8 bytes, /32)
Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
  Min Policed Unit: 1 bytes, Max Pkt Size 2147483647 bytes
Fast-Reroute Backup info:
  Inbound  FRR: Not active
  Outbound FRR: Ready -- backup tunnel selected
    Backup Tunnel: Tu666      (label 20)
    Bkup Sender Template:
      Tun Sender: 10.0.2.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
      SubGroup ID: 2
    Bkup FilerSpec:
      Tun Sender: 10.0.2.201, LSP ID: 1, SubGroup Orig: 10.1.1.201
      SubGroup ID: 2
Path ID handle: 01000417.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxied
```

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 *97 : show ip rsvp fast-reroute detail P2MP* フィールドの説明

フィールド	説明
P2MP ID	P2MP トンネルの宛先セットを指定する 32 ビットの番号。
Tun ID	トンネル ID 番号。
Ext Tun ID	拡張トンネル ID 番号。
Tun Sender	送信元の IP アドレス。
LSP ID	ラベル スイッチド パス ID 番号。
SubGroup Orig	LSP ヘッドエンド ルータ ID アドレス。
SubGroup ID	ヘッドエンド ルータからのシグナルを受ける各サブ LSP に割り当てられる増分番号。
S2L Destination	LSP テールエンド ルータ ID アドレス。

関連コマンド

コマンド	説明
mplstraffic-engfast-reroutebackup-prot-preemption	バックアップ保護プリエンプションアルゴリズムを変更して、有効に使用されていない帯域幅量を最小化します。

show ip rsvp hello

高速再ルーティング、再ルーティング（Hello ステート タイマー）、グレースフル リスタートに関する hello の状態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 **showiprsvphello** コマンドを使用します。

show ip rsvp hello

構文の説明

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	変更箇所
12.0(22)S	このコマンドが導入されました。
12.0(29)S	コマンド出力が変更され、グレースフル リスタート、再ルーティング（Hello ステート タイマー）、および Fast Reroute の情報が追加されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
12.2(33)SRA	コマンド出力が変更され、グレースフル リスタートが設定されているかどうか、フル モードが追加されているかどうかが表示されるようになりました。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SRC	コマンドの出力が、双方向フォワーディング検出（BFD）プロトコル情報も含むように変更されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

例

次は、**showiprsvphello** コマンドの出力例です。

```
Router# show ip rsvp hello
Hello:
 RSVP Hello for Fast-Reroute/Reroute: Enabled
  Statistics: Disabled
 BFD for Fast-Reroute/Reroute: Enabled
 RSVP Hello for Graceful Restart: Disabled
```

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。これらのフィールドは、hello が有効化または無効化されているプロセスに関する情報を表示します。

表 *98 : show ip rsvp hello* フィールドの説明

フィールド	説明
RSVP Hello for Fast-Reroute/Reroute	高速再ルーティング/再ルーティングの状態。 • Disabled：高速再ルーティングおよび再ルーティング（Hello ステート タイマー）は非アクティブ（無効）です。 • Enabled：高速再ルーティングおよび再ルーティング（Hello ステート タイマー）はアクティブ（有効）です。
Statistics	hello 統計の状態。 • Disabled：hello 統計は設定されていません。 • Enabled：統計が設定されています。hello パケットは、Hello インプット キューに到達すると、処理されるまでに要した時間を記録するためにタイムスタンプが付加されます。 • Shutdown：hello 統計は設定されていますが、動作していません。インプット キューが長すぎです（つまり、10,000 を超えるパケットがキュー内に滞留しています）。
BFD for Fast-Reroute/Reroute	高速再ルーティング/再ルーティングの BFD の状態。 • Disabled：BFD は設定されていません。 • Enabled：BFD が設定されています。
Graceful Restart	リスタート機能： • Disabled：リスタート機能は非アクティブです。 • Enabled：リスタート機能は、ルータ（フル モード）またはネイバー（ヘルプ ネイバー）でアクティブです。

関連コマンド

コマンド	説明
iprsvpsignallinghello(configuration)	ルータで Hello をグローバルに有効にします。
iprsvpsignallinghellostatistics	ルータで Hello 統計情報を有効にします。
showiprsvphellostatistics	hello パケットが hello 入力キューに入っていた時間を表示します。

show ip rsvp hello client lsp detail

ラベルスイッチド パス（LSP）のリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）クライアント Hello に関する詳細情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvphelloclientlspdetail** コマンドを使用します。

show ip rsvp hello client lsp detail [**filter** [**destination** *hostname*]]

構文の説明

filter	（任意）出力表示を限定するフィルタを指定します。
destination	（任意）接続先（トンネルテール）に設定されたフィルタを表示します。
hostname	（任意）接続先（トンネル テール）の IP アドレスまたは名前。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(33)S	このコマンドが導入されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。

使用上のガイドライン

LSP に関する情報（IP アドレス、タイプなど）を表示するには、**showiprsvphelloclientlspdetail** コマンドを使用します。

例

次は、**showiprsvphelloclientlspdetail** コマンドの出力例です。

```
Router# show ip rsvp hello client lsp detail
Hello Client LSPs (all lsp tree)
  Tun Dest: 10.0.1.1  Tun ID: 14  Ext Tun ID: 172.16.1.1
  Tun Sender: 172.16.1.1  LSP ID: 31
    Lsp flags: 0x32
    Lsp GR DN nbr: 192.168.1.1
    Lsp RR DN nbr: 10.0.0.3 HST
```

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 *99 : show ip rsvp hello client lsp detail* フィールドの説明

フィールド	説明
Hello Client LSPs	現在のクライアントには、グレースフル リスタート（GR）、再ルーティング（RR）（Hello ステート タイマー）、および Fast Reroute（FRR）が含まれます。
Tun Dest	宛先トンネルの IP アドレス。

フィールド	説明
Tun ID	トンネルの ID 番号。
Ext Tun ID	トンネルの拡張 ID 番号。通常、発信元アドレスと同じです。
Tun Sender	トンネル送信元の IP アドレス。
LSP ID	LSP の ID 番号。
Lsp flags	LSP データベースの情報。
Lsp GR DN nbr	LSP グレースフル リスタート ダウンストリーム ネイバーの IP アドレス。
Lsp RR DN nbr	LSP 再ルーティング ダウンストリーム ネイバーの IP アドレス（HST：Hello ステート タイマー）。

関連コマンド

コマンド	説明
showiprsvphello	Fast Reroute、再ルーティング（Hello ステート タイマー）、およびグレースフル リスタートについて、Hello の状態と統計情報を表示します。

show ip rsvp hello client lsp summary から show lane qos database

- show ip rsvp hello client lsp summary （1365 ページ）
- show ip rsvp hello client nbr detail （1367 ページ）
- show ip rsvp hello client neighbor detail （1369 ページ）
- show ip rsvp hello client neighbor summary （1371 ページ）
- show ip rsvp hello graceful-restart （1373 ページ）
- show ip rsvp hello instance detail （1375 ページ）
- show ip rsvp hello instance summary （1379 ページ）
- show ip rsvp hello statistics （1382 ページ）
- show ip rsvp high-availability counters （1384 ページ）
- show ip rsvp high-availability database （1390 ページ）
- show ip rsvp high-availability summary （1409 ページ）
- show ip rsvp host （1414 ページ）
- show ip rsvp host vrf （1418 ページ）
- show ip rsvp ingress （1420 ページ）
- show ip rsvp installed （1422 ページ）
- show ip rsvp interface （1432 ページ）
- show ip rsvp interface detail （1450 ページ）
- show ip rsvp listeners （1452 ページ）
- show ip rsvp neighbor （1455 ページ）
- show ip rsvp p2mp counters （1459 ページ）
- show ip rsvp policy （1461 ページ）
- show ip rsvp policy cops （1463 ページ）
- show ip rsvp policy identity （1464 ページ）
- show ip rsvp policy local （1467 ページ）
- show ip rsvp policy vrf （1475 ページ）
- show ip rsvp precedence （1478 ページ）
- show ip rsvp request （1480 ページ）
- show ip rsvp reservation （1489 ページ）

- show ip rsvp sbm （1501 ページ）
- show ip rsvp sender （1504 ページ）
- show ip rsvp signalling （1539 ページ）
- show ip rsvp signalling blockade （1542 ページ）
- show ip rsvp signalling fast-local-repair （1545 ページ）
- show ip rsvp signalling rate-limit （1551 ページ）
- show ip rsvp signalling refresh （1553 ページ）
- show ip rsvp snooping （1555 ページ）
- show ip rsvp tos （1556 ページ）
- show ip rsvp transport （1558 ページ）
- show ip rsvp transport sender （1560 ページ）
- show ip rtp header-compression （1563 ページ）
- show ip tcp header-compression （1566 ページ）
- show ip vrf （1569 ページ）
- show lane qos database （1574 ページ）

show ip rsvp hello client lsp summary

ラベルスイッチド パス（LSP）のリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）クライアント Hello に関する概要情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvphelloclientlspsummary** コマンドを使用します。

show ip rsvp hello client lsp 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 モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SB	このコマンドが導入されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。

使用上のガイドライン

LSP に関する情報（IP アドレス、ID 番号など）を表示するには、**showiprsvphelloclientlspsummary** コマンドを使用します。

例

次は、**showiprsvphelloclientlspsummary** コマンドの出力例です。

```
Router# show ip rsvp hello client lsp summary
Local           Remote          tun_id  lsp_id  FLAGS
10.1.1.1        172.16.1.1        14      31      0x32
```

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 *100 : show ip rsvp hello client lsp summary* フィールドの説明

フィールド	説明
Local	トンネル送信元の IP アドレス。
Remote	トンネルの宛先 IP アドレス
tun_id	トンネルの ID 番号。
lsp_id	LSP の ID 番号。
FLAGS	データベース情報。

関連コマンド

コマンド	説明
showiprsvphello	Fast Reroute、再ルーティング（Hello ステート タイマー）、およびグレースフル リスタートについて、Hello の状態と統計情報を表示します。

show ip rsvp hello client nbr detail

ネイバーのリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）クライアント Hello に関する詳細情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvphelloclientnbrdetail** コマンドを使用します。

show ip rsvp hello client nbr detail [**filter** [**destination** *hostname*]]

構文の説明

filter	（任意）出力表示を限定するフィルタを指定します。
destination	（任意）接続先（トンネルテール）に設定されたフィルタを表示します。
hostname	（任意）接続先（トンネル テール）の IP アドレスまたは名前。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(33)S	このコマンドが導入されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。

使用上のガイドライン

ネイバー（nbr）の情報を表示するには、**showiprsvphelloclientnbrdetail** コマンドを使用します。

例

次は、**showiprsvphelloclientnbrdetail** コマンドの出力例です。

```
Router# show ip rsvp hello client nbr detail
Hello Client Neighbors
  Remote addr 10.0.0.1,  Local addr  10.0.0.3
    Nbr State: Normal    Type: Reroute
    Nbr Hello State: Up
    LSPs protecting: 1
    I/F: Et1/3
  Remote addr 172.16.1.1,  Local addr  192.168.1.1
    Nbr State: Normal    Type: Graceful Restart
    Nbr Hello State: Lost
    LSPs protecting: 1
```

次の表に、出力で表示されるフィールドについて説明します。

表 *101 : show ip rsvp hello client nbr detail* フィールドの説明

フィールド	説明
Remote addr	リモート ネイバーの IP アドレス。グレースフル リスタートの場合は、ネイバー ルータの ID です。Fast Reroute および Hello ステート タイマー（再ルーティング）の場合は、ネイバーのインターフェイス アドレスのいずれかです。

フィールド	説明
Local addr	ローカル ネイバーの IP アドレス。グレースフル リスタートの場合は、ネイバー ルータの ID です。Fast Reroute および Hello ステート タイマー（再ルーティング）の場合は、ネイバーのインターフェイスアドレスのいずれかです。
Nbr state	ネイバーの状態。有効な値は次のとおりです。 • Normal：ネイバーは正常に機能しています。 • Restarting：ネイバーは再起動しています。 • Recover Nodal：ネイバーはノード障害から回復中です。 • HST_GR_LOST：HST（再ルーティングの Hello ステート タイマー）が失われました。GR（グレースフル リスタート）も失われたかどうかを確認するために待機中です。 • WAIT PathTear：パイプライン内のトラフィックが送信可能になるまで、PathTear メッセージは待機します。
Type	クライアントのタイプ：グレースフル リスタート（GR）、再ルーティング（RR）（Hello ステート タイマー）、または Fast Reroute（FRR）。
Nbr Hello State	ネイバーの Hello インスタンスの状態。表示される値は次のとおりです。 • Up：ノードはネイバーと通信しています。 • Lost：通信が切断されました。 • Init：通信を確立しています。
LSPs protecting	保護されている LSP の数。
I/F	Hello インスタンスに関連付けられたインターフェイス名と番号。

関連コマンド

コマンド	説明
showiprsvphello	Fast Reroute、再ルーティング（Hello ステート タイマー）、およびグレースフル リスタートについて、Hello の状態と統計情報を表示します。
showiprsvphelloclientneighborsummary	ネイバーの RSVP TE クライアント Hello に関する概要情報を表示します。

show ip rsvp hello client neighbor detail

ネイバーのリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）クライアント Hello に関する詳細情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvphelloclientneighbordetail** コマンドを使用します。

show ip rsvp hello client neighbor detail

構文の説明

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	変更箇所
12.0(29)S	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

Hello ネイバーに関する情報（状態、タイプなど）を表示するには、**showiprsvphelloclientneighbordetail** コマンドを使用します。

例

次は、**showiprsvphelloclientneighbordetail** コマンドの出力例です。

```
Router# show ip rsvp hello client neighbor detail
Hello Client Neighbors
  Remote addr 10.0.0.1,  Local addr  10.0.0.3
    Nbr State: Normal    Type: Reroute
    Nbr Hello State: Up
    LSPs protecting: 1
    I/F: Et1/3
  Remote addr 172.16.1.1,  Local addr  192.168.1.1
    Nbr State: Normal    Type: Graceful Restart
    Nbr Hello State: Lost
    LSPs protecting: 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。フィールドには、ネイバーを一意に識別する情報が表示されます。クライアントには、グレースフル リスタート、再ルーティング（Hello ステート タイマー）、および Fast Reroute が含まれます。

表 *102 : show ip rsvp hello client neighbor detail* フィールドの説明

フィールド	説明
Remote addr	リモート ネイバーの IP アドレス。グレースフル リスタートの場合は、ネイバー ルータの ID です。Fast Reroute および Hello ステート タイマー（再ルーティング）の場合は、ネイバーのインターフェイス アドレスのいずれかです。
Local addr	ローカル ネイバーの IP アドレス。グレースフル リスタートの場合は、ネイバー ルータの ID です。Fast Reroute および Hello ステート タイマー（再ルーティング）の場合は、ネイバーのインターフェイス アドレスのいずれかです。
Nbr State	ネイバーの状態。有効な値は次のとおりです。 • Normal：ネイバーは正常に機能しています。 • Restarting：ネイバーは再起動しています。 • Recover Nodal：ネイバーはノード障害から回復中です。 • HST_GR_LOST：HST（再ルーティングの Hello ステート タイマー）が失われました。グレースフル リスタート（GR）も失われたかどうかを確認するために待機中です。 • WAIT PathTear：パイプライン内のトラフィックが送信可能になるまで、PathTear メッセージは待機します。
Type	クライアントのタイプ：グレースフル リスタート、再ルーティング（Hello ステート タイマー）、または Fast Reroute。
Nbr Hello State	ネイバーの Hello の状態。表示される値は次のとおりです。 • Up：ノードはネイバーと通信しています。 • Lost：通信が切断されました。 • Init：通信を確立しています。
LSPs protecting	保護されている LSP の数。
I/F	Hello インスタンスに関連付けられたインターフェイス名と番号。

関連コマンド

コマンド	説明
showiprsvphello	Fast Reroute、再ルーティング（Hello ステート タイマー）、およびグレースフル リスタートについて、Hello の状態と統計情報を表示します。

show ip rsvp hello client neighbor summary

ネイバーのリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）クライアント Hello に関する概要情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvphelloclientneighborsummary** コマンドを使用します。

show ip rsvp hello client neighbor 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 モード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(29)S	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

ネイバーの情報（状態、タイプ、Hello インスタンスの状態など）を表示するには、**showiprsvphelloclientneighborsummary** コマンドを使用します。

例

次は、**showiprsvphelloclientneighborsummary** コマンドの出力例です。

```
Router# show ip rsvp hello client neighbor summary
Local Remote Type NBR_STATE HI_STATE LSPs
10.0.0.1 10.0.0.3 RR Normal Up 1
172.16.1.1 192.168.1.1 GR Normal Lost 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 *103 : show ip rsvp hello client neighbor summary* フィールドの説明

フィールド	説明
Local	トンネル送信元の IP アドレス。
Remote	トンネルの宛先 IP アドレス
Type	クライアントのタイプ：グレースフル リスタート（GR）、再ルーティング（RR）（Hello ステート タイマー）、または Fast Reroute（FRR）。

フィールド	説明
NBR_STATE	ネイバーの状態。有効な値は次のとおりです。 • Normal：ネイバーは正常に機能しています。 • Restarting：ネイバーは再起動しています。 • Recover Nodal：ネイバーはノード障害から回復中です。 • HST_GR_LOST：HST（再ルーティングの Hello ステート タイマー）が失われました。グレースフル リスタート（GR）も失われたかどうかを確認するために待機中です。 • WAIT PathTear：パイプライン内のトラフィックが送信可能になるまで、PathTear メッセージは待機します。
HI_STATE	ネイバーの Hello インスタンスの状態。表示される値は次のとおりです。 • Up：ノードはネイバーと通信しています。 • Lost：通信が切断されました。 • Init：通信を確立しています。
LSP	ネイバーで送受信する LSP の数。

関連コマンド

コマンド	説明
showiprsvphello	Fast Reroute、再ルーティング（Hello ステート タイマー）、およびグレースフル リスタートについて、Hello の状態と統計情報を表示します。

show ip rsvp hello graceful-restart

リソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）グレースフル リスタート Hello に関する情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvphellograceful-restart** コマンドを使用します。

show ip rsvp hello graceful-restart

構文の説明

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	変更箇所
12.0(29)S	このコマンドが導入されました。
12.2(33)SRA	コマンド出力が変更され、グレースフル リスタートが設定されているかどうか、フル モードが追加されているかどうかが表示されるようになりました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

グレースフル リスタートの状態と関連する統計情報を表示するには、**showiprsvphellograceful-restart** コマンドを使用します。

例

次は、**showiprsvphellograceful-restart** コマンドの出力例です。

```
Router# show ip rsvp hello graceful-restart
Graceful Restart: Enabled (full mode)
  Refresh interval: 10000 msecs
  Refresh misses: 4
  DSCP: 0x30
  Advertised restart time: 30000 msecs
  Advertised recovery time: 120000 msecs
  Maximum wait for recovery: 3600000 msecs
```

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 *104 : show ip rsvp hello graceful-restart* フィールドの説明

フィールド	説明
Graceful Restart	リスタート機能： • Enabled：リスタート機能は、ルータ（フル モード）またはネイバー（ヘルプ ネイバー）でアクティブです。 • Disabled：リスタート機能は非アクティブです。
Refresh interval	ノードが Hello メッセージをネイバーに送信する頻度（ミリ秒（ms））。
Refresh misses	ステートフル スイッチオーバー（SSO）処理が開始されるネイバー ダウン イベントをトリガーする消失 Hello メッセージの数。
DSCP	Hello メッセージの IP ヘッダーの DiffServ コード ポイント（DSCP）。
Advertised restart time	送信元が障害後に RSVP-TE コンポーネントを再起動し、Hello メッセージを交換するために必要な時間（ms）。
Advertised recovery time	SSO 後にネイバー ルータが RSVP またはマルチプロトコル ラベル スイッチング（MPLS）転送状態を再同期する場合に、回復中のノードが要求する時間（ms）。 （注） ゼロ値は、RSVP または MPLS 転送状態が SSO 後に保持されないことを示します。
Maximum wait for recovery	ルータがネイバーの回復を待機する最大時間（ms）。

関連コマンド

コマンド	説明
clearip rsvp high-availability counters	RP によって保持されている RSVP-TE HA カウンタをクリア（0 に設定）します。
ip rsvp signalling hello graceful-restart mode	RP で RSVP-TE グレースフル リスタート サポート機能を有効にします。
ip rsvp signalling hello graceful-restart neighbor	隣接ルータで RSVP-TE グレースフル リスタート サポート機能を有効にします。
show ip rsvp hello	Fast Reroute、再ルーティング（Hello ステート タイマー）、およびグレースフル リスタートについて、Hello の状態と統計情報を表示します。

show ip rsvp hello instance detail

Hello インスタンスの詳細情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvphelloinstancedetail** コマンドを使用します。

show ip rsvp hello instance detail [**filter destination** *ip-address*]

構文の説明

filterdestination *ip-address*	（任意）ネイバー ノードの IP アドレス。

コマンド モード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.0(29)S	コマンド出力が変更され、グレースフル リスタート、Hello ステート タイマー（再ルーティング）、および Fast Reroute の情報が追加されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

現在設定されているプロセス（クライアント）の情報を表示するには、**showiprsvphelloinstancedetail** コマンドを使用します。

例

次は、**showiprsvphelloinstancedetail** コマンドの出力例です。

```
Router# show ip rsvp hello instance detail
Neighbor 10.0.0.3  Source  10.0.0.2
    Type: Active    (sending requests)
    I/F:  Serial2/0
    State:   Up        (for 2d19h2d19h)
    Clients: ReRoute
    LSPs protecting: 1
    Missed acks: 4, IP DSCP: 0x30
    Refresh Interval (msec)
      Configured: 6000
      Statistics: (from 40722 samples)
        Min:      6000
        Max:      6064
        Average:  6000
        Waverage: 6000 (Weight = 0.8)
        Current:  6000
```

```
  Last sent Src_instance: 0xE617C847
  Last recv nbr's Src_instance: 0xFEC28E95
  Counters:
    Communication with neighbor lost:
      Num times:                    0
      Reasons:
        Missed acks:                0
        Bad Src_Inst received:      0
        Bad Dst_Inst received:      0
        I/F went down:              0
        Neighbor disabled Hello:    0
    Msgs Received:   55590
         Sent:       55854
         Suppressed: 521
Neighbor 10.0.0.8 Source  10.0.0.7
  Type: Passive   (responding to requests)
  I/F:  Serial2/1
  Last sent Src_instance: 0xF7A80A52
  Last recv nbr's Src_instance: 0xD2F1B7F7
  Counters:
    Msgs Received:   199442
         Sent:       199442
```

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 *105 : show ip rsvp hello instance detail* フィールドの説明

フィールド	説明
Neighbor	隣接ノードの IP アドレス。
Source	Hello メッセージを送信中のノードの IP アドレス。
Type	値は、Active（ノードはリクエストを送信中）および Passive（ノードはリクエストに応答中）です。
I/F	このインスタンスに送信される Hello の送信元インターフェイス。any は Hello がどのインターフェイスからも送信可能であることを示します。
State	通信の状態。表示される値は次のとおりです。 • Up：ノードはネイバーと通信しています。 • Lost：通信が切断されました。 • Init：通信を確立しています。
Clients	この Hello インスタンスを作成したクライアント。グレースフル リスタート、再ルーティング（Hello ステート タイマー）、および Fast Reroute が含まれます。
LSPs protecting	この Hello インスタンスが保護している LSP の数。
Missed acks	確認応答（ACK）の消失が原因で通信が切断された回数。

フィールド	説明
IP DSCP	Hello IP ヘッダーで使用される IP DiffServ コードポイント（DSCP）値。
Refresh Interval (msec)	ノードが、状態が追跡されているネイバーそれぞれについて Hello リクエスト オブジェクトを含む Hello メッセージを生成する頻度（ms）。
Configured	設定されている更新間隔。
Statistics	指定されたサンプル数（パケット数）の更新間隔の統計情報。
Min	最小更新間隔。
Max	最大更新間隔。
Average	平均更新間隔。
Waverage	加重平均更新間隔。
Current	現在の更新間隔。
Last sent Src_instance	ネイバーへ最後に送信された送信元インスタンス。
Last recv nbr's Src_instance	ネイバーから最後に受信した送信元インスタンス フィールド値。（0 は受信なしを意味します）。
Counters	ネイバーとの通信に関連する増分情報。
Num times	ネイバーとの通信が切断した回数の合計。
Reasons	以下のフィールドは、ネイバーとの通信が切断した理由を示します。
Missed acks	ACK 消失が原因で通信が切断した回数。
Bad Src_Inst received	不正な送信元インスタンス フィールドが原因で通信が切断した回数。
Bad Dst_Inst received	不正な接続先インスタンス フィールドが原因で通信が切断した回数。
I/F went down	インターフェイスが動作不能になった回数。
Neighbor disabled Hello	ネイバーが Hello メッセージを無効にした回数。
Msgs Received	受信したメッセージの数。
Sent	送信されたメッセージの数。

フィールド	説明
Suppressed	最適化によって削減されたメッセージの数。

関連コマンド

コマンド	説明
iprsvpsignallinghello(configuration)	ルータで Hello をグローバルに有効にします。
iprsvpsignallinghellostatistics	ルータで Hello 統計情報を有効にします。
showiprsvphello	Fast Reroute、再ルーティング（Hello ステート タイマー）、およびグレースフル リスタートについて、Hello の状態と統計情報を表示します。
showiprsvphelloinstancesummary	Hello インスタンスの概要情報を表示します。

show ip rsvp hello instance summary

Hello インスタンスの概要情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvphelloinstancesummary** コマンドを使用します。

show ip rsvp hello instance 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 モード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.0(29)S	コマンド出力が変更され、グレースフル リスタート、再ルーティング（Hello ステート タイマー）、および Fast Reroute の情報が追加されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

例

次は、**showiprsvphelloinstancesummary** コマンドの出力例です。

```
Router# show ip rsvp hello instance summary
Active Instances:
  Client  Neighbor        I/F        State      LostCnt  LSPs Interval
  RR      10.0.0.3        Se2/0      Up               0     1 6000
  GR      10.1.1.1        Any        Up              13     1 10000
  GR      10.1.1.5        Any        Lost             0     1 10000
  GR      10.2.2.1        Any        Init             1     0 5000
Passive Instances:
  Neighbor        I/F
  10.0.0.1        Se2/1
Active = Actively tracking neighbor state on behalf of clients:
         RR = ReRoute, FRR = Fast ReRoute, or GR = Graceful Restart
Passive = Responding to hello requests from neighbor
```

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 *106 : show ip rsvp hello instance summary* フィールドの説明

フィールド	説明
Active Instances	Hello リクエストを送信中のアクティブなノード。
Client	Helloが代わりに送信されるクライアント。GR（グレースフル リスタート）、RR（再ルーティング＝Hello ステート タイマー）、およびFRR（Fast Reroute）が含まれます。
Neighbor	隣接ノードのIPアドレス。グレースフル リスタートの場合は、ネイバー ルータのIDです。Fast RerouteおよびHello ステート タイマー（再ルーティング）の場合は、ネイバーのインターフェイス アドレスのいずれかです。
I/F	このインスタンスに送信されるHelloの送信元インターフェイス。anyはHelloがどのインターフェイスからも送信可能であることを示します。
State	通信の状態。表示される値は次のとおりです。 • Up：ノードはネイバーと通信しています。 • Lost：通信が切断されました。 • Init：通信を確立しています。
LostCnt	ネイバーとの通信が切断した回数。
LSP	このHelloインスタンスによって保護されているラベルスイッチドパス（LSP）の数。
Interval	Hello 更新間隔（ミリ秒）。
Passive Instances	Hello リクエストに応答中のパッシブ ノード。
Neighbor	隣接ノードのIPアドレス。グレースフル リスタートの場合は、ネイバー ルータのIDです。Fast RerouteおよびHello ステート タイマー（再ルーティング）の場合は、ネイバーのインターフェイス アドレスのいずれかです。
I/F	このインスタンスに送信されるHelloの送信元インターフェイス。anyはHelloがどのインターフェイスからも送信可能であることを示します。

関連コマンド

コマンド	説明
iprsvpsignallinghello(configuration)	ルータで Hello をグローバルに有効にします。
iprsvpsignallinghellostatistics	ルータで Hello 統計情報を有効にします。

コマンド	説明
showiprsvphello	Fast Reroute、再ルーティング（Hello ステート タイマー）、およびグレースフル リスタートについて、Hello の状態と統計情報を表示します。
showiprsvphelloinstancedetail	Hello インスタンスの詳細情報を表示します。

show ip rsvp hello statistics

hello パケットの Hello インプット キュー内滞留時間を表示するには、特権 EXEC モードで **showiprsvphellostatistics** コマンドを使用します。

show ip rsvp hello 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

hello パケットの Hello インプット キュー内滞留時間に関する情報は表示されません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T 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、Hello 更新間隔が小さすぎないか判断することができます。間隔が小さすぎると、実際にはそうでないにもかかわらず、通信が失われたという宣言がなされる場合があります。

例

次は、**showiprsvphellostatistics** コマンドの出力例です。

```
Router# show ip rsvp hello statistics

Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:4
    Current length: 0 (max:500)
  Number of samples taken: 2398525
```

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 *107 : show ip rsvp hello statistics* フィールドの説明

フィールド	説明
Status	Hello がルータ上でグローバルに有効化されているかどうかを示すインジケータ。
Current	現在の hello パケットの Hello インプット キュー内滞留時間（ミリ秒単位）。
Average	hello パケットの Hello インプット キュー内滞留時間の平均（ミリ秒単位）。
Max	hello パケットの最長の Hello インプット キュー内滞留時間（ミリ秒単位）。
Current length	hello パケットの現在の Hello インプット キュー内滞留時間（ミリ秒単位）。
Number of samples taken	これらの統計情報の作成対象となったパケットの数。

関連コマンド

コマンド	説明
clearIprsvphelloinstancestatistics	インスタンスの Hello 統計をクリアします。
clearIprsvphellostatistics	Hello 統計情報をグローバルにクリアします。
iprsvpsignallinghellorefreshinterval	Hello 要求間隔を設定します。
iprsvpsignallinghellostatistics	ルータで Hello 統計情報を有効にします。

show ip rsvp high-availability counters

ルートプロセッサ（RP）によって維持されているすべてのリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）高可用性（HA）カウンタを表示するには、ユーザEXECモードまたは特権 EXEC モードで **show ip rsvp high-availability counters** コマンドを使用します。

show ip rsvp high-availability 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 モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRA	このコマンドが導入されました。
12.2(33)SRB	インサービス ソフトウェア アップグレード（ISSU）のサポートが追加されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
15.0(1)S	このコマンドが変更されました。出力が、ポイントツーポイント（P2P）およびポイントツーマルチポイント（P2MP）のトラフィック エンジニアリング カウンタの情報を表示するように更新されました。
15.2(2)S	このコマンドが変更されました。出力が、MPLS トラフィック エンジニアリング自動トンネルおよび自動メッシュ ステートフル スイッチオーバー（SSO）トンネルのチェックポイント情報を表示するように拡張されました。
Cisco IOS XE Release 3.6S	このコマンドが変更されました。出力が、MPLS トラフィック エンジニアリング自動トンネルおよび自動メッシュ ステートフル スイッチオーバー（SSO）トンネルのチェックポイント情報を表示するように拡張されました。

使用上のガイドライン

HA カウンタを表示するには、**show ip rsvp high-availability counters** コマンドを使用します。表示には、状態、ISSU、チェックポイント メッセージ、リソース障害、およびエラーが含まれます。

コマンドの出力は、RP がアクティブであるかスタンバイであるかによって異なります（詳細については、「例」の項を参照してください）。

すべてのカウンタをクリアするには、**clear ip rsvp high-availability counters** コマンドを使用します。

例

次に、アクティブ RP に対して **show ip rsvp high-availability counters** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability counters

State: Active
P2P LSPs for which recovery:
  Attempted: 1
  Succeeded: 1
  Failed:    0
P2MP subLSPs for which recovery:
  Attempted: 2
  Succeeded: 2
  Failed:    0
Bulk sync
  initiated: 1
Send timer
  started: 2
Checkpoint Messages (Items) Sent
  Succeeded:      2  (8)
    Acks accepted:2  (8)
    Acks ignored:     (0)
    Nacks:        0  (0)
  Failed:         0  (0)
  Buffer alloc:   2
  Buffer freed:   4
ISSU:
  Checkpoint Messages Transformed:
    On Send:
      Succeeded:         2
      Failed:            0
      Transformations:   0
    On Recv:
      Succeeded:         2
      Failed:            0
      Transformations:   0
  Negotiation:
    Started:              2
    Finished:             2
    Failed to Start:      0
    Messages:
      Sent:
        Send succeeded:   14
        Send failed:      0
        Buffer allocated:        14
        Buffer freed:            0
        Buffer alloc failed:     0
      Received:
        Succeeded:        10
        Failed:           0
        Buffer freed:     10
  Init:
    Succeeded:            1
    Failed:               0
  Session Registration:
    Succeeded:            1
    Failed:               0
  Session Unregistration:
    Succeeded:            1
    Failed:               0
Errors:
  None
```

```
Historical: (When Active was Standby)
Checkpoint Messages (Items) Received
  Valid:        2  (11)
  Invalid:      0  (0)
Buffer freed: 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 *108 : show ip rsvp high-availability counters*：アクティブ *RP* フィールドの説明

フィールド	説明
State	RP の状態。 • Active：アクティブ RP。
Bulk sync	スタンバイ RP がアクティブ RP に対して行った、すべての書き込みデータベース エントリの再送信要求の件数。 • Initiated：再起動以降にスタンバイ RP が開始したバルク同期操作の回数。
Send timer	書き込みデータベースのタイマー。
Checkpoint Messages (Items) Sent	起動以降に送信されたバンドル メッセージまたはアイテムの詳細。
Succeeded	起動以降にアクティブ RP からスタンバイ RP に送信されたバンドル メッセージまたはアイテムの数。値は次のとおりです。 • Acks accepted：アクティブ RP からスタンバイ RP に送信されたバンドル メッセージまたはアイテムの数。 • Acks ignored：アクティブ RP から送信されたもののスタンバイ RP によって拒否されたバンドル メッセージまたはアイテムの数。 • Nacks：スタンバイ RP への転送のためにアクティブ RP 上のチェックポインティング ファシリティ（CF）に与えられたものの、転送が失敗したバンドル メッセージまたはアイテムの数。
Failed	送信タイマーの更新時にアクティブ RP がスタンバイ RP へと送信しようとしたものの、CF からエラーが返されたバンドル メッセージまたはアイテムの数。
Buffer alloc	割り当て済みのストレージ スペース。
Buffer freed	使用可能なストレージ スペース。
ISSU	インサービス ソフトウェア アップグレード（ISSU）カウンタ。

フィールド	説明
Checkpoint Messages Transformed	起動以降に、アクティブ RP とスタンバイ RP が相互運用できるように変換された（互換性のためにアップグレードまたはダウングレードされた）バンドル メッセージまたはアイテムの詳細。
On Send	成功もしくは失敗した、または変換されたアクティブ RP からの送信メッセージの数。
On Recv	成功もしくは失敗した、または変換されたアクティブ RP による受信メッセージの数。
Negotiation	アクティブ RP とスタンバイ RP が相互運用性パラメータのネゴシエーションを行った回数。
Started	開始されたネゴシエーションの回数。
Finished	完了したネゴシエーションの回数。
Failed to Start	開始に失敗したネゴシエーションの回数。
Messages	送受信されたネゴシエーション メッセージの数。これらのメッセージは、成功または失敗のいずれかです。 • Send succeeded：送信に成功したメッセージの数。 • Send failed：送信に失敗したメッセージの数。 • Buffer allocated：許可されているストレージ スペース。 • Buffer freed：使用可能なストレージ スペース。 • Buffer alloc failed：使用可能なストレージ スペースがありません。
Init	RSVP ISSU クライアントによる初期化の成功および不成功（失敗）の回数。
Session Registration	スタンバイ RP が再起動されるたびにアクティブ RP が実行し、成功および失敗したセッション登録の回数。
Session Unregistration	スタンバイ RP がリセットされる前の、成功および失敗したセッション登録解除の回数。
Errors	エラーまたは警告の詳細。

次に、スタンバイ RP に対して **show ip rsvp high-availability counters** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability counters

State: Standby
```

```
Checkpoint Messages (Items) Received
  Valid:        1  (2)
  Invalid:      0  (0)
  Buffer freed: 1

ISSU:
  Checkpoint Messages Transformed:
    On Send:
      Succeeded:         0
      Failed:            0
      Transformations:   0
    On Recv:
      Succeeded:         1
      Failed:            0
      Transformations:   0

  Negotiation:
    Started:              1
    Finished:             1
    Failed to Start:      0
    Messages:
      Sent:
        Send succeeded:   5
        Send failed:      0
        Buffer allocated:        5
        Buffer freed:            0
        Buffer alloc failed:     0
      Received:
        Succeeded:        7
        Failed:           0
        Buffer freed:     7

  Init:
    Succeeded:            1
    Failed:               0

  Session Registration:
    Succeeded:            0
    Failed:               0

  Session Unregistration:
    Succeeded:            0
    Failed:               0

Errors:
  None
```

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 *109 : show ip rsvp high-availability counters*：スタンバイ *RP* フィールドの説明

フィールド	説明
状態	RP の状態。 • Standby：スタンバイ（バックアップ）RP。

フィールド	説明
Checkpoint Messages (Items) Received	スタンバイ RP が受け取ったメッセージまたはアイテムの詳細。値は次のとおりです。 • Valid：スタンバイ RP が受け取った有効なメッセージまたはアイテムの数。 • Invalid：スタンバイ RP が受け取った無効なメッセージまたはアイテムの数。 • Buffer freed：使用可能なストレージ スペースの量。
ISSU	ISSU カウンタ。 （注） ISSU フィールドの詳細については、上記の表を参照してください。
Errors	エラーまたは警告の詳細。

関連コマンド

コマンド	説明
clear ip rsvp high-availability counters	RP によって保持されている RSVP-TE HA カウンタをクリア（0 に設定）します。
show ip rsvp high-availability database	TE SSO で使用される RSVP-TE HA 読み取り/書き込みデータベースの内容を表示します。
show ip rsvp high-availability summary	RSVP-TE HA RP の概要情報を表示します。

show ip rsvp high-availability database

トラフィック エンジニアリング（TE）で使用されるリソース予約プロトコル（RSVP）高可用性（HA）読み取り/書き込みデータベースの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip rsvp high-availability database** コマンドを使用します。

show ip rsvp high-availability database {**hello**|**if-autotun**|**link-management** {**interfaces** [{**fixed**|**variable**}]|**system**}|**lsp** [{**filter** [{**destination** *ip-address*}]|[{**lsp-id** *lsp-id*}]|[{**source** *ip-address*}]|[{**tunnel-id** *tunnel-id*}]}]|**lsp-head** [**filter** *number*]|**summary**}

構文の説明

hello	読み取り/書き込みデータベース内の hello エントリに関する情報を表示します。
if-autotun	読み取り/書き込みデータベース内の TE HA 自動トンネル インターフェイス エントリに関する情報を表示します。
link-management	読み取り/書き込みデータベース内のリンク管理エントリに関する情報を表示します。
interfaces	読み取り/書き込みデータベース内のリンク管理インターフェイスに関する情報を表示します。
fixed	（オプション）読み取り/書き込みデータベース内のリンク管理固定インターフェイスに関する情報を表示します。
variable	（オプション）読み取り/書き込みデータベース内のリンク管理変動インターフェイスに関する情報を表示します。
system	読み取り/書き込みデータベース内のリンク管理システムに関する情報を表示します。
lsp	読み取り/書き込みデータベース内のラベル スイッチド パス（LSP）エントリに関する情報を表示します。
filter destination *ip-address*	（オプション）宛先（トンネル テール）の IP アドレスについて、フィルタ処理された情報を表示します。
filter lsp-id *lsp-id*	（オプション）0 から 65535 までの番号で指定された特定の LSP ID について、フィルタ処理された情報を表示します。
filter source *ip-address*	（オプション）送信元（トンネル ヘッド）の IP アドレスについて、フィルタ処理された情報を表示します。
filter tunnel-id *tunnel-id*	（オプション）0 から 65535 までの番号で指定された特定のトンネル ID について、フィルタ処理された情報を表示します。
lsp-head	読み取り/書き込みデータベース内の LSP ヘッド エントリに関する情報を表示します。

filter *number*	（オプション）0 から 65535 までの番号で指定された特定の LSP ヘッド ルータ について、フィルタ処理された情報を表示します。
summary	読み取り/書き込みデータベース内のエントリに関する累積情報を表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRA	このコマンドが導入されました。
12.2(33)SRB	コマンドの出力が、ルータによって実行されるルーズ ホップ展開の結果を表示するように変更されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。コマンドの出力が、**lsp-head** キーワードによって指定されたパス保護情報を含むように変更されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
15.0(1)S	このコマンドは、Cisco IOS リリース 15.0(1)S に統合されました。コマンドの出力が、ポイントツーポイント（P2P）トンネルのデータベース エントリ情報をポイントツーマルチポイント（P2MP）トンネルのデータベース エントリ情報から区別するように、また、エラー データベースの情報を表示するように変更されました。
12.2(50)SY	このコマンドが、Cisco IOS Release 12.2(50)SY に統合されました。
Cisco IOS XE リリース 3.5S	このコマンドが、Cisco IOS XE Release 3.5S に統合されました。
15.2(2)S	このコマンドが変更されました。**if-autotun** キーワードが追加されました。**show ip rsvp high-availability database lsp** コマンド、**show ip rsvp high-availability database lsp-head** コマンド、および **show ip rsvp high-availability database summary** コマンドの出力が、MPLS TE 自動トンネルおよび自動メッシュ ステートフル スイッチオーバー（SSO）トンネルのチェックポイント情報を表示するように拡張されました。

リリース	変更箇所
Cisco IOS XE Release 3.6S	このコマンドが変更されました。**if-autotun** キーワードが追加されました。**show ip rsvp high-availability database lsp** コマンド、**show ip rsvp high-availability database lsp-head** コマンド、および **show ip rsvp high-availability database summary** コマンドの出力が、MPLS TE 自動トンネルおよび自動メッシュ ステートフル スイッチオーバー（SSO）トンネルのチェックポイント情報を表示するように拡張されました。

使用上のガイドライン

読み取り/書き込みデータベース内のエントリに関する情報を表示するには、**show ip rsvp high-availability database** コマンドを使用します。

ルーズ ホップの情報を表示するには、**show ip rsvp high-availability database lsp** コマンドを使用します。ルーズ ホップ展開は、ルータが受信パス メッセージの明示ルート オブジェクト（ERO）を処理するときに、そのルータ上で実行できます。ルータは、受信 ERO からすべてのローカル IP アドレスを削除した後、ネクスト ホップを検索します。ネクスト ホップは厳格ではなくルーズであることが ERO によって指定されている場合、ルータは、TE トポロジデータベースおよびルーティングを参照し、パス メッセージを転送するためのネクスト ホップと出力インターフェイスを決定します。計算の結果は、ホップのリストです。このリストは発信 ERO 内に配置され、LSP データを使用して、ルーズ ホップ情報としてチェックポインティングされます。

Cisco IOS リリース 15.0(1)S およびそれ以降のリリースでは、**show ip rsvp high-availability database lsp** コマンドは Sub-LSP 情報を表示します。（P2MP、P2P のいずれの場合でも）Sub-LSP がステートフル スイッチオーバー（SSO）後に回復できなかった場合は、障害がエラー データベースに記録され、トラブルシューティングに使用されます。エラー データベースのエントリは、**show ip rsvp high-availability database lsp** コマンドを使用すると表示できます。

show ip rsvp high-availability database lsp-head コマンドはヘッドエンド ルータに対してのみ使用でき、それ以外のルータの情報は提供しません。

例

アクティブ RP での hello の例

次に、アクティブ ルート プロセッサ（RP）に対して **show ip rsvp high-availability database hello** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability database hello

HELLO WRITE DB
   Header:
     State: Checkpointed     Action: Add
     Seq #: 1                Flags: 0x0
   Data:
     Last sent Src_instance: 0xDE435865
HELLO READ DB
```

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 *110 : show ip rsvp high-availability database hello* : アクティブ *RP* フィールドの説明

フィールド	説明
HELLO WRITE DB	アクティブ RP hello データ（スタンバイ RP がアクティブ RP になり、LSP を回復する必要があるときにスタンバイ RP に送信される、チェックポインティングされた RSVP-TE 情報で構成される）のストレージ エリア。このフィールドは、スタンバイ RP の場合は空白です。
Header	ヘッダー情報。
State	エントリのステータス。表示される値は次のとおりです。 • Ack-Pending：エントリは送信されていますが、確認応答されていません。 • Checkpointed：エントリは送信済みで、スタンバイ RP による確認応答済みです。 • Send-Pending：エントリは送信待ちの状態です。
Action	実行されるアクション。表示される値は次のとおりです。 • Add：スタンバイ RP にアイテムを追加します。 • Delete：スタンバイ RP からアイテムを削除します。これは、アクティブ RP が削除操作の確認応答（ACK）を待っている間に行われる一時的なアクションです。 • Modify：スタンバイ RP 上のアイテムを変更します。 • Remove：スタンバイ RP からアイテムを削除します。
Seq #	メッセージの確認応答（ACK）と送信されたメッセージに対する否定確認応答（NACK）を同期するためにアクティブ RP およびスタンバイ RP が使用する番号。
Flags	データを特定または追跡するために使用される属性。
Data	最後の伝送に関する情報。
Last sent Src_instance	最後に送信された送信元インスタンスの識別子。
HELLO READ DB	スタンバイ RP hello データ用のストレージ エリア。このフィールドは、アクティブ RP の場合は、回復モード中を除いて空白です。

スタンバイ RP での hello の例

次に、スタンバイ RP に対して **show ip rsvp high-availability database hello** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability database hello

HELLO WRITE DB
HELLO READ DB
   Header:
     State: Checkpointed     Action: Add
     Seq #: 1                Flags: 0x0
   Data:
     Last sent Src_instance: 0xDE435865
```

これらのフィールドは、スタンバイ RP の場合は読み取りデータベース内のフィールドであることを除き、表に記載したアクティブ RP のフィールドと同じです。

アクティブ RP での自動トンネル インターフェイスの例

次に、アクティブ RP に対して **show ip rsvp high-availability database if-autotun** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability database if-autotun
IF_AUTOTUN WRITE DB

  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
    Tunnel ID: 1000 (if_handle: 85), prot_if_handle: 14
    template_unit: n/a, dest: 22.22.22.22, flags=0x0

  Header:
    State: Checkpointed     Action: Add
    Seq #: 61               Flags: 0x0
  Data:
    Tunnel ID: 2000 (if_handle: 86), prot_if_handle: 14
    template_unit: n/a, dest: 22.22.22.22, flags=0x1

  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
    Tunnel ID: 3000 (if_handle: 87), prot_if_handle: 0
    template_unit: 1, dest: 22.22.22.22, flags=0x2

  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
    Tunnel ID: 3001 (if_handle: 88), prot_if_handle: 0
    template_unit: 1, dest: 172.16.255.128, flags=0x2

  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
```

```
    Tunnel ID: 3002 (if_handle: 89), prot_if_handle: 0
    template_unit: 1, dest: 200.0.0.0, flags=0x2


IF_AUTOTUN READ DB
```

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 *111 : show ip rsvp high-availability database if-autotun*：アクティブ *RP* フィールドの説明

フィールド	説明
IF_AUTOTUN WRITE DB	アクティブ RP 自動トンネル インターフェイス情報用のストレージ エリア。このフィールドは、スタンバイ RP の場合は空白です。
Header	ヘッダー情報。
State	エントリのステータス。表示される値は次のとおりです。 • Ack-Pending：エントリは送信されていますが、確認応答されていません。 • Checkpointed：エントリは送信済みで、スタンバイ RP による確認応答済みです。 • Send-Pending：エントリはまだ送信待ちの状態です。
Action	実行されるアクション。表示される値は次のとおりです。 • Add：スタンバイ RP にアイテムを追加します。 • Delete：スタンバイ RP からアイテムを削除します。このアクションは、アクティブ RP が削除操作の ACK を待っている間に一時的に表示されます。 • Modify：スタンバイ RP 上のアイテムを変更します。 • Remove：スタンバイ RP からアイテムを削除します。
Seq #	メッセージの ACK と送信されたメッセージに対する NACK を同期するためにアクティブ RP およびスタンバイ RP が使用する番号。

フィールド	説明
Flags	データを特定または追跡するために使用される属性。
Data	最後の伝送に関する情報。
Tunnel ID	トンネル識別子。
if_handle	自動トンネル インターフェイスを表す内部番号。同じトンネルIDに対し、スタンバイ読み取り DB 内のレコードのこの if_handle の値は、アクティブ書き込み DB 内のレコードの値と常に同じである必要があります。
prot_if_handle	自動トンネル メッシュ トンネルの場合、この値は常にゼロである必要があります。自動トンネル プライマリ トンネルの場合、この値は、自動トンネル プライマリの出力インターフェイスを表す内部番号です。自動トンネル バックアップ トンネルの場合、この値は、バックアップによって保護されているインターフェイスを表す内部番号です。上記の 3 つのケースすべてにおいて、同じトンネルIDに対し、スタンバイ読み取り DB 内のレコードのこの値は、アクティブ書き込み DB 内のレコードの値と常に同じである必要があります。
template_unit	自動トンネル メッシュの場合、メッシュ トンネルの作成元である自動テンプレート インターフェイス番号を表します。自動トンネル プライマリおよび自動トンネル バックアップの場合、この値は「n/a」である必要があります。
dest	自動トンネルの宛先 IP アドレス。
flags	エンコーディングされた値は、以下のとおりです。 • 0 = 自動トンネル プライマリ • 1 = 自動トンネル バックアップ • 2 = 自動トンネル メッシュ
IF_AUTOTUN READ DB	スタンバイ RP 自動トンネル インターフェイス情報用のストレージ エリア。このフィールドは、アクティブ RP の場合は空白です。

スタンバイ RP のフィールドは、アクティブ RP によって使用されるインターフェイス自動トンネル書き込みデータベース内ではなくインターフェイス自動トンネル読み取りデータベース内にあることを除き、表に記載したものと同じです。

アクティブ RP でのリンク管理インターフェイスの例

次に、アクティブ RP に対して **show ip rsvp high-availability database link-management interfaces** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability database link-management interfaces

TE LINK WRITE DB
Flooding Protocol: ospf  IGP Area ID: 0  Link ID: 0 (GigabitEthernet3/2)
  Header:
    State: Checkpointed     Action: Add
    Seq #: 4                Flags: 0x0
  Data:
        Ifnumber: 5  Link Valid Flags: 0x193B
        Link Subnet Type: Broadcast
        Local Intfc ID: 0  Neighbor Intf ID: 0
        Link IP Address: 172.16.3.1
        Neighbor IGP System ID: 172.16.3.2  Neighbor IP Address: 10.0.0.0
        IGP Metric: 1  TE Metric: 1
        Physical Bandwidth: 1000000 kbits/sec
        Res. Global BW: 3000 kbits/sec
        Res. Sub BW: 0 kbits/sec
        Upstream::
                                 Global Pool   Sub Pool
                                 -----------   ----------
        Reservable Bandwidth[0]:           0            0 kbits/sec
        Reservable Bandwidth[1]:           0            0 kbits/sec
        Reservable Bandwidth[2]:           0            0 kbits/sec
        Reservable Bandwidth[3]:           0            0 kbits/sec
        Reservable Bandwidth[4]:           0            0 kbits/sec
        Reservable Bandwidth[5]:           0            0 kbits/sec
        Reservable Bandwidth[6]:           0            0 kbits/sec
        Reservable Bandwidth[7]:           0            0 kbits/sec
        Downstream::
                                 Global Pool   Sub Pool
                                 -----------   ----------
        Reservable Bandwidth[0]:        3000            0 kbits/sec
        Reservable Bandwidth[1]:        3000            0 kbits/sec
        Reservable Bandwidth[2]:        3000            0 kbits/sec
        Reservable Bandwidth[3]:        3000            0 kbits/sec
        Reservable Bandwidth[4]:        3000            0 kbits/sec
        Reservable Bandwidth[5]:        3000            0 kbits/sec
        Reservable Bandwidth[6]:        3000            0 kbits/sec
        Reservable Bandwidth[7]:        2900            0 kbits/sec
        Affinity Bits: 0x0
        Protection Type: Capability 0,  Working Priority 0
        Number of TLVs: 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 *112 : show ip rsvp high-availability database link-management interfaces* : アクティブ *RP* フィールドの説明

フィールド	説明
TE LINK WRITE DB	アクティブ TE RP リンク データ用のストレージ エリア。このフィールドは、スタンバイ RP の場合は空白です。
Flooding Protocol	対象のエリアの情報をフラッディングしているプロトコル。OSPF = Open Shortest Path First
IGP Area ID	フラッディングされているエリアの内部ゲートウェイ プロトコル（IGP）識別子。
Link ID	フラッディングされているエリアのリンク識別子とインターフェイス。
ヘッダー	ヘッダー情報。
State	エントリのステータス。表示される値は次のとおりです。 • Ack-Pending：エントリは送信されていますが、確認応答されていません。 • Checkpointed：エントリは送信済みで、スタンバイ RP による確認応答済みです。 • Send-Pending：エントリは送信待ちの状態です。
Action	実行されるアクション。表示される値は次のとおりです。 • Add：スタンバイ RP にアイテムを追加します。 • Delete：スタンバイ RP からアイテムを削除します。このアクションは、アクティブ RP が削除操作の ACK を待っている間に一時的に表示されます。 • Modify：スタンバイ RP 上のアイテムを変更します。 • Remove：スタンバイ RP からアイテムを削除します。
Seq #	メッセージの ACK と送信されたメッセージに対する NACK を同期するためにアクティブ RP およびスタンバイ RP が使用する番号。
Flags	データを特定または追跡するために使用される属性。
Data	最後の伝送に関する情報。
Ifnumber	インターフェイス番号。
Link Valid Flags	リンクを特定または追跡するために使用される属性。

フィールド	説明
Link Subnet Type	リンクのサブネット タイプ。表示される値は次のとおりです。 • Broadcast：複数の受信者に向けたデータ。 • Nonbroadcast Multiaccess：データが仮想回路またはスイッチング ファブリックを経由して1台のコンピュータから別のコンピュータへと直接送信されるネットワーク。 • Point-to-Multipoint：単一の送信元エンド システム（ルート ノードと呼ばれる）が複数の宛先エンド システム（リーフと呼ばれる）に接続する一方向接続。 • Point-to-Point：2 つのエンド システム間の一方向または双方向の接続。 • Unknown subnet type：サブネット タイプが識別されない場合。
Local Intfc ID	ローカル インターフェイスの識別子。
Neighbor Intf ID	ネイバー インターフェイスの識別子。
Link IP Address	リンクの IP アドレス。
Neighbor IGP System ID	IGP を使用して設定されているネイバー システムの識別子。
Neighbor IP Address	ネイバーの IP アドレス。
IGP Metric	IGP を使用して設定されている TE リンクのメトリック値。
TE Metric	マルチプロトコル ラベル スイッチング（MPLS）TE を使用して設定されている TE リンクのメトリック値。
Physical Bandwidth	リンクの帯域幅容量（キロビット/秒（kb/s）単位）。
Res.Global BW	このリンク上で予約可能なグローバル プール帯域幅の量（kb/s 単位）。
Res.Sub BW	このリンク上で予約可能なサブプール帯域幅の量（kb/s 単位）。
Upstream	次の、帯域幅の値を示すセクションのヘッダー。
Global Pool	このリンク上のグローバル プール帯域幅（kb/s 単位）。
Sub Pool	このリンク上のサブプール帯域幅（kb/s 単位）。
Reservable Bandwidth [1]	グローバル TE トポロジおよびサブプールにおける予約可能な帯域幅の量（kb/s 単位）。
Downstream	次の、帯域幅の値を示すセクションのヘッダー。

フィールド	説明
Affinity Bits	トンネルに必要なリンク属性。
Protection Type	高速再ルーティング（FRR）によって保護されている LSP。 • Capability = FRR を使用できる LSP。 • Working Priority = FRR を実際に使用している LSP。
Number of TLVs	タイプ、長さ、値（TLV）の数。

スタンバイ RP のフィールドは、アクティブ RP によって使用される TE リンク書き込みデータベース内ではなく TE リンク読み取りデータベース内にあることを除き、表に記載したものと同じです。

アクティブ RP でのリンク管理システムの例

次に、アクティブ RP に対して **show ip rsvp high-availability database link-management system**コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability database link-management system

TE SYSTEM WRITE DB
Flooding Protocol: OSPF  IGP Area ID: 0
  Header:
    State: Checkpointed     Action: Modify
    Seq #: 4                Flags: 0x0
  Data:
    LM Flood Data::
      LSA Valid flags: 0x0  Node LSA flag: 0x0
      IGP System ID: 172.16.3.1  MPLS TE Router ID: 10.0.0.3
      Flooded links: 1  TLV length: 0 (bytes)
      Fragment id: 0
TE SYSTEM READ DB
```

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 *113 : show ip rsvp high-availability database link-management system*：アクティブ *RP* フィールドの説明

フィールド	説明
TE SYSTEM WRITE DB	アクティブ TE RP システムデータ用のストレージエリア。このフィールドは、スタンバイ RP の場合は空白です。
Flooding Protocol	対象のエリアの情報をフラッディングしているプロトコル。OSPF = Open Shortest Path First
IGP Area ID	フラッディングされているエリアの IGP 識別子。
Header	ヘッダー情報。

フィールド	説明
State	エントリのステータス。表示される値は次のとおりです。 • Ack-Pending：エントリは送信されていますが、確認応答されていません。 • Checkpointed：エントリは送信済みで、スタンバイ RP による確認応答済みです。 • Send-Pending：エントリは送信待ちの状態です。
Action	実行されるアクション。表示される値は次のとおりです。 • Add：スタンバイ RP にアイテムを追加します。 • Delete：スタンバイ RP からアイテムを削除します。このアクションは、アクティブ RP が削除操作の ACK を待っている間に一時的に表示されます。 • Modify：スタンバイ RP 上のアイテムを変更します。 • Remove：スタンバイ RP からアイテムを削除します。
Seq #	メッセージの ACK と送信されたメッセージに対する NACK を同期するためにアクティブ RP およびスタンバイ RP が使用する番号。
Flags	データを特定または追跡するために使用される属性。
Data	最後の伝送に関する情報。
LM Flood Data	リンク管理（LM）フラッディング データ。
LSA Valid flags	リンクステート アドバタイズメント（LSA）属性。
Node LSA flag	ルータによって使用される LSA 属性。
IGP System ID	IGP フラッディングで対象エリアの対象ノードを識別するために使用される識別情報（IP アドレス）。
MPLS TE Router ID	MPLS TE ルータの識別子（IP アドレス）。
Flooded links	フラッディングされているリンクの数。
TLV length	TLV の長さ（バイト単位）。
Fragment id	このリンクのフラグメント識別子。
TE SYSTEM READ DB	スタンバイ TE RP システム データ用のストレージエリア。このフィールドは、スタンバイ RP の場合は空白です。

スタンバイ RP のフィールドは、アクティブ RP によって使用される TE システム書き込みデータベース内ではなく TE システム読み取りデータベース内にあることを除き、表に記載したものと同じです。

P2P トンネル用アクティブ RP での LSP の例

次に、P2P トンネルのアクティブ RP に対して **show ip rsvp high-availability database lsp** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability database lsp

Tun ID: 0   LSP ID: 10   (P2P)
  SubGrp ID:   -
  SubGrp Orig: -
  Dest:   10.3.0.1
  Sender: 10.1.0.1     Ext. Tun ID: 10.1.0.1
  Header:
    State: Checkpointed     Action: Add
    Seq #: 2                Flags: 0x0
  Data:
    PathSet ID: -
    Lspvif if_num: -
    InLabel: -
    Out I/F: Se2/0
    Next-Hop: 10.1.3.2
    OutLabel: 16
    Loose hop info: None (0)
```

P2MP トンネル用アクティブ RP での LSP の例

次に、P2MP トンネルのアクティブ RP に対して **show ip rsvp high-availability database lsp** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability database lsp

Tun ID: 1   LSP ID: 127   (P2MP)
  SubGrp ID:   1
  SubGrp Orig: 10.1.0.1
  Dest:   10.2.0.1
  Sender: 10.1.0.1     Ext. Tun ID: 10.1.0.1
  Header:
    State: Checkpointed     Action: Add
    Seq #: 30               Flags: 0x0
  Data:
    PathSet ID: 0x1A000003
    Lspvif if_num: 35 (Lspvif0)
    InLabel: 19
    Out I/F: None
    Next-Hop: -
    OutLabel: -
    Loose hop info: None (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 *114 : show ip rsvp high-availability database lsp* : アクティブ *RP* フィールドの説明

フィールド	説明
P2P/P2MP	トンネルのタイプ。
Subgrp ID	サブグループの識別子（P2MP TE LSP の場合のみ有効）。
Subgrp Orig	サブグループの送信元 IP アドレス（P2MP TE LSP の場合のみ有効）。
Lspvif if_num	LSPVIF のインターフェイス番号（P2MP TE テールエンドの場合のみ有効）。
PathSet ID	パス セットの識別子（P2MP TE LSP の場合のみ有効）。
LSP WRITE DB	アクティブ RP LSP データ用のストレージ エリア。このフィールドは、スタンバイ RP の場合は空白です。
Tun ID	トンネル識別子。
LSP ID	LSP ID。
Dest	トンネルの宛先 IP アドレス。
Sender	トンネルの送信者 IP アドレス。
Ext.Tun ID	拡張トンネル識別子。通常、0 または送信者の IP アドレスに設定します。
Header	ヘッダー情報。
State	エントリのステータス。表示される値は次のとおりです。 • Ack-Pending：エントリは送信されていますが、確認応答されていません。 • Checkpointed：エントリは送信済みで、スタンバイ RP による確認応答済みです。 • Send-Pending：エントリは送信待ちの状態です。
Action	実行されるアクション。表示される値は次のとおりです。 • Add：スタンバイ RP にアイテムを追加します。 • Delete：スタンバイ RP からアイテムを削除します。このアクションは、アクティブ RP が削除操作の ACK を待っている間に一時的に表示されます。 • Modify：スタンバイ RP 上のアイテムを変更します。 • Remove：スタンバイ RP からアイテムを削除します。
Seq #	メッセージの ACK と送信されたメッセージに対する NACK を同期するためにアクティブ RP およびスタンバイ RP が使用する番号。

フィールド	説明
Flags	データを特定または追跡するために使用される属性。
Data	最後の伝送に関する情報。
InLabel	着信ラベルの識別子。
Out I/F	発信インターフェイス。
Next-Hop	ネクスト ホップの IP アドレス。
OutLabel	送信ラベルの識別子。
Loose hop info	ルータ上で実行されたルーズ ホップ展開を一覧表示するか、「None」を指定します。
LSP READ DB	スタンバイ RP LSP データ用のストレージ エリア。このフィールドは、アクティブ RP の場合は空白です。

スタンバイ RP のフィールドは、アクティブ RP によって使用される LSP 書き込みデータベース内ではなく LSP 読み取りデータベース内にあることを除き、表に記載したものと同じです。

P2P トンネル用アクティブ RP での LSP ヘッドの例

次に、P2P トンネルのアクティブ RP に対して **show ip rsvp high-availability database lsp-head** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability database lsp-head

LSP_HEAD WRITE DB
  Tun ID: 0  (P2P)
  Header:
    State: Checkpointed     Action: Add
    Seq #: 2                Flags: 0x0
  Data:
    lsp_id: 10, bandwidth: 5, thead_flags: 0x1, popt: 1
    feature flags: none
    output_if_num: 11, output_nhop: 10.1.3.2
    RRR path setup info
      Destination: 10.3.0.1, Id: 10.3.0.1 Router Node (ospf) flag:0x0
      IGP: ospf, IGP area: 0, Number of hops: 3, metric: 128
      Hop 0: 10.1.3.2, Id: 10.2.0.1 Router Node (ospf), flag:0x0
      Hop 1: 10.2.3.3, Id: 10.3.0.1 Router Node (ospf), flag:0x0
      Hop 2: 10.3.0.1, Id: 10.3.0.1 Router Node (ospf), flag:0x0
```

P2MP トンネル用アクティブ RP での LSP ヘッドの例

次に、P2MP トンネルのアクティブ RP に対して **show ip rsvp high-availability database lsp-head** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability database lsp-head

LSP_HEAD WRITE DB
Tun ID: 1  (P2MP)
  Destination: 10.2.0.1
  Header:
    State: Checkpointed     Action: Add
    Seq #: 3                Flags: 0x0
  Data:
    lsp_id: 11, bandwidth: 100, thead_flags: 0x1, popt: 1
    Subgrp_id: 1
    feature flags: none
    output_if_num: 3, output_nhop: 10.1.2.2
    RRR path setup info
      Destination: 10.2.0.1, Id: 10.2.0.1 Router Node (ospf) flag:0x0
      IGP: ospf, IGP area: 0, Number of hops: 3, metric: 10
      Hop 0: 10.1.2.1, Id: 10.1.0.1 Router Node (ospf), flag:0x0
      Hop 1: 10.1.2.2, Id: 10.2.0.1 Router Node (ospf), flag:0x0
      Hop 2: 10.2.0.1, Id: 10.2.0.1 Router Node (ospf), flag:0x0
```

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 *115 : show ip rsvp high-availability database lsp-head* : アクティブ *RP* フィールドの説明

フィールド	説明
LSP_HEAD WRITE DB	アクティブ RP LSP ヘッド データ用のストレージ エリア。このフィールドは、スタンバイ RP の場合は空白です。
P2P/P2MP	トンネルのタイプ。
Tun ID	トンネル識別子。
Header	ヘッダー情報。
State	エントリのステータス。表示される値は次のとおりです。 • Ack-Pending：エントリは送信されていますが、確認応答されていません。 • Checkpointed：エントリは送信済みで、スタンバイ RP による確認応答済みです。 • Send-Pending：エントリは送信待ちの状態です。
Action	実行されるアクション。表示される値は次のとおりです。 • Add：スタンバイ RP にアイテムを追加します。 • Delete：スタンバイ RP からアイテムを削除します。これは、アクティブ RP が削除操作の ACK を待っている間に行われる一時的なアクションです。 • Modify：スタンバイ RP 上のアイテムを変更します。 • Remove：スタンバイ RP からアイテムを削除します。

フィールド	説明
Seq #	メッセージの ACK と送信されたメッセージに対する NACK を同期するためにアクティブ RP およびスタンバイ RP が使用する番号。
Flags	データを特定または追跡するために使用される属性。
Data	最後の伝送に関する情報。
lsp_id	LSP ID。
bandwidth	LSP 上の帯域幅（kb/s 単位）。
thead_flags	データを特定または追跡するために使用されるトンネルヘッド属性。
popt	解析オプションの番号。
feature_flags	トラフィックの転送に使用されている LSP がパス保護のパス オプションを使用するセカンダリ LSP であるかどうかを示します。有効な値は、次のとおりです。 • none • path protection active
output_if_num	出力インターフェイスの番号。
output_nhop	出力ネクスト ホップの IP アドレス。
RRR path setup info	リソース予約ルーティング（RRR）のパス情報。
Destination	宛先の IP アドレス。
ID	ルーティング ノードの IP アドレスとプロトコル。表示される値は次のとおりです。 • ISIS = Intermediate System-to-Intermediate System • OSPF = Open Shortest Path First
flag	データを追跡するために使用される属性。
IGP	Interior Gateway Protocol。OSPF = Open Shortest Path First
IGP area	IGP エリアの識別子。
Number of hops	接続またはルータの数。
metric	ルーティング コスト。
Hop	ホップの番号と IP アドレス。

フィールド	説明
LSP_HEAD READ DB	スタンバイ RP LSP ヘッド データ用のストレージ エリア。このフィールドは、アクティブ RP の場合は空白です。

スタンバイ RP のフィールドは、アクティブ RP によって使用される LSP ヘッド書き込みデータベース内ではなく LSP ヘッド読み取りデータベース内にあることを除き、表に記載したものと同じです。

アクティブ RP でのサマリーの例

次に、アクティブ RP に対して **show ip rsvp high-availability database summary**コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability database summary

Write DB:
  Send-Pending:     0
  Ack-Pending :     0
  Checkpointed:    10
  Total       :    10
Read DB:
  Total       :     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 *116 : show ip rsvp high-availability database summary* : アクティブ *RP* フィールドの説明

フィールド	説明
Write DB	アクティブ RP サマリー データ用のストレージ エリア。このフィールドは、スタンバイ RP の場合は空白です。
Send-Pending	エントリは送信待ちの状態です。
Ack-Pending	エントリは送信済みですが、確認応答待ちの状態です。
Checkpointed	エントリは、送信済みかつ確認応答済みです。
Total	書き込みデータベース内のエントリの総数。
Total	読み取りデータベース内のエントリの総数。

スタンバイ RP でのサマリーの例

次に、スタンバイ RP に対して **show ip rsvp high-availability database summary** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability database summary
```

```
Write DB:
  Send-Pending:     0
  Ack-Pending :     0
  Checkpointed:     0
  Total       :     0
Read DB:
  Total       :    10
```

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 *117 : show ip rsvp high-availability database summary* : スタンバイ *RP* フィールドの説明

フィールド	説明
Write DB	アクティブ RP サマリーデータ用のストレージエリア。
Send-Pending	エントリは送信待ちの状態です。
Ack-Pending	エントリは送信済みですが、確認応答待ちの状態です。
Checkpointed	エントリは、送信済みかつ確認応答済みです。
Total	書き込みデータベース内のエントリの総数。
Total	読み取りデータベース内のエントリの総数。

関連コマンド

コマンド	説明
show ip rsvp high-availability counters	RP によって維持されているすべての RSVP HA カウンタを表示します。
show ip rsvp high-availability summary	RSVP HA RP の概要情報を表示します。

show ip rsvp high-availability summary

リソース予約プロトコル（RSVP）トラフィックエンジニアリング（TE）高可用性（HA）ルートプロセッサ（RP）の概要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 rsvp high-availability summary** コマンドを使用します。

show ip rsvp high-availability 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 モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRA	このコマンドが導入されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
15.2(2)S	このコマンドが変更されました。出力が、MPLS TE 自動トンネルおよび自動メッシュ ステートフル スイッチオーバー（SSO）トンネルのチェックポイント情報を表示するように拡張されました。
Cisco IOS XE Release 3.6S	このコマンドが変更されました。出力が、MPLS TE 自動トンネルおよび自動メッシュ ステートフル スイッチオーバー（SSO）トンネルのチェックポイント情報を表示するように拡張されました。

使用上のガイドライン

RP 上に現在設定されている HA パラメータに関する情報を表示するには、**show ip rsvp high-availability summary** コマンドを使用します。

コマンドの出力は、RP がアクティブであるかスタンバイであるかによって異なります

例

次に、アクティブ RP に対して **show ip rsvp high-availability summary**コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability summary

State:
Graceful-Restart: Enabled, mode: full
HA state: Active
Checkpointing: Allowed
Messages:
Send timer: not running (Interval: 1000 msec)
Items sent per Interval: 200
CF buffer size used: 2000
```

（注） スタンバイ RP の場合は、出力の最初の 3 行のみが表示されます。アクティブ RP の場合は、すべての行が表示されます。

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 *118 : show ip rsvp high-availability summary*：フィールドの説明

フィールド	説明
State	グレースフル リスタートおよび HA の状態。
Graceful Restart	リスタート機能： • Enabled：ルータ（フル モード）またはそのネイバー（ヘルプネイバー）では、リスタート機能がアクティブ化されています。 • Disabled：リスタート機能はアクティブ化されていません。
HA state	RP の状態。以下のいずれかです。 • Active：アクティブ RP。 • Standby：スタンバイ（バックアップ）RP。 • Recovering：アクティブ RP が回復期間中です。
Checkpointing	アクティブ RP からスタンバイ RP に状態の情報（書き込みデータベース エントリ）をコピーする機能。値は次のとおりです。 • Allowed：正常に機能しています。 • Not Allowed：チェックポインティングは許可されていません。理由として、RP が存在していないか、RP の準備ができていない可能性があります。
Messages	指定された間隔中にアクティブ RP がスタンバイ RP に送信した、チェックポインティングされたメッセージ。

フィールド	説明
Send timer	書き込みデータベースのタイマー。値は次のとおりです。 • running：エントリは送信保留中の状態で書き込みデータベース内に存在しており、チェックポインティングは許可されています。 • not running：チェックポインティングが許可されていないか、書き込みデータベースが空です。 （注） 書き込みデータベース内のエントリは、以下のいずれかの状態です。 • Send-Pending：エントリはまだスタンバイ RP に送信されていません。 • Ack-Pending：エントリはスタンバイ RP に送信されましたが、スタンバイ RP からの確認応答はまだ受信されていません。 • Checkpointed：アクティブ RP への通知を行うチェックポインティング機能（CF）メッセージは、スタンバイ RP によって確認されています。
Interval	アクティブ RP がスタンバイ RP にメッセージを送信するまでの時間（ミリ秒単位）。
Items sent per Interval	書き込みデータベース タイマーがアクティブ化するたびにアクティブ RP がスタンバイ RP に送信するデータベース エントリ（書き込みデータベースから取得され、バンドル メッセージ内にパックされてスタンバイ RP に転送されるデータ）の数。
CF buffer size used	チェックポインティング機能によって使用されるストレージスペースの量（バイト単位）。

場合によっては、Checkpointing フィールドに「Not Allowed」と表示されることがあります。次に、出力例の抜粋を示します。

```
Checkpointing: Not Allowed
Peer RP Present : No
RF Comm. Up : No
Flow Control On : No
CF Comm. Up : No
RF Ready to Recv: No
```

（注） チェックポインティングが許可されている場合、出力例に表示されている属性は表示されません。詳細については、アクティブ RP に対して **show ip rsvp high-availability summary** コマンドを実行した場合の出力を参照してください。

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 *119 : show ip rsvp high-availability summary* : *Checkpointing* フィールドの説明

フィールド	説明
Peer RP Present : No	アクティブ RP はいずれのピア RP とも通信できません。 （注） これは、スタンバイ RP が削除されている場合、またはスタンバイ RP が再起動中などで一時的に使用できなくなっている場合に発生します。
RF Comm.Up : No	アクティブ RP 上の冗長性機能（RF）は、スタンバイ RP 上の RF と通信できません。
Flow Control On : No	フロー制御がオフのため、アクティブ RP は、スタンバイ RP にインターネット プロトコル通信（IPC）メッセージを（チェックポインティングを使用して）送信することができません。
CF Comm.Up : No	アクティブ RP 上の TE CF クライアントは、スタンバイ RP 上の TE CF クライアントと通信することができません。
RF Ready to Recv : No	スタンバイ RP 上の RF は、チェックポイント メッセージを受信する準備ができていません。

次に、ステートフル スイッチオーバー（SSO）が発生した後に **show ip rsvp high-availability summary** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp high-availability summary

State:
 Graceful-Restart: Enabled
 HA state: active
Checkpointing: Allowed
Recovery Time (msec)
 Advertised:    120000 msec
 Last recorded: 75012 msec
Messages:
 Send timer: not running (Interval:1000)
 Items sent per Interval: 200
```

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 *120 : show ip rsvp high-availability summary* : *SSO* 発生後のフィールドの説明

フィールド	説明
Advertised	アドバタイズされた回復時間（ミリ秒単位）。
Last recorded	最後に記録された回復時間（ミリ秒単位）。

関連コマンド

コマンド	説明
clear ip rsvp high-availability counters	RP によって保持されている RSVP-TE HA カウンタをクリア（0 に設定）します。
show ip rsvp high-availability counters	RP によって維持されているすべての RSVP-TE HA カウンタを表示します。
show ip rsvp high-availability database	TE SSO で使用される RSVP-TE HA 読み取り/書き込みデータベースの内容を表示します。

show ip rsvp host

リソース予約プロトコル（RSVP）ホストの具体的な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 **showiprsvphost** コマンドを使用します。

show ip rsvp host {**receivers**|**senders**} [{*hostnamegroup-address*}]

構文の説明

senders	現在データベースに格納されている RSVP 関連の送信側情報。
receivers	現在データベースに格納されている RSVP 関連の受信側情報。
hostname	（オプション）送信元または宛先のホスト名。
group-address	（オプション）送信元または宛先の IP アドレス。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
12.4(6)T	このコマンドが変更されました。コマンドの出力が、RSVP 識別情報が設定されている場合はその情報を表示するように拡張されました。
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。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

静的な RSVP 送信者および受信者を表示するには、**showiprsvphost** コマンドを使用します。ルータに RSVP 識別情報を持つローカル ホスト受信者または送信者が設定されている場合は、それらが使用するアプリケーション ID も表示されます。

例

次の **showiprsvphostsenders** コマンドの出力例では、ローカル送信者に対して RSVP 識別情報が設定されていません。

```
Router# show ip rsvp host senders
To              From            Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.3 192.168.104.1 UDP 1     1                              10K
  Mode(s): Host CLI
```

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 *121 : show ip rsvp host senders* フィールドの説明（*RSVP* 識別情報が設定されていない場合）

フィールド	説明
To	受信者の IP アドレス。
From	送信元の IP アドレス。
Pro	プロトコル コード。TCP や UDP などの IP プロトコル。
DPort	宛先ポート番号。コード 1 は、TCP や UDP などの IP プロトコルを示します。
Sport	送信元ポート番号です。コード 1 は、TCP や UDP などの IP プロトコルを示します。
Prev Hop	前のホップの IP アドレス。空白は、前のホップがないことを意味します。
I/F	前のホップのインターフェイス。
BPS	予約レート（1 秒あたりのビット数（bps）単位）。
Mode(s)	次の文字列のいずれか。 • Host：ルータは、この予約のホスト システムまたは RSVP エンドポイントとして機能しています。 • LSP-Tunnel：この予約は、トラフィック エンジニアリング（TE）トンネルの予約です。 • MIB：この予約は、リモート管理ステーションからの Simple Network Management Protocol（SNMP）SET ディレクティブを介して作成されています。 • CLI：この予約は、ローカル RSVP コマンドを介して作成されています。 • Host CLI：表示されている静的な送信者が **iprsvpsender-host** コマンドによって作成されていることを意味する、「Host」およびコマンドライン インターフェイスを表す「CLI」という文字列の組み合わせ。

次の **showiprsvphostsenders** コマンドの出力例では、ローカル送信者に対して RSVP 識別情報が設定されています。

```
Router# show ip rsvp host senders
To              From            Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.3 192.168.104.1 UDP 1     1                           10K
  Mode(s): Host CLI
  Identity: voice100
    Locator: GUID=www.cisco.com,APP=voice,VER=100.0
    ID Type: Application
```

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 *122 : show ip rsvp host senders* フィールドの説明（*RSVP* 識別情報が設定されている場合）

フィールド	説明
To	受信者の IP アドレス。
From	送信元の IP アドレス。
Pro	プロトコル コード。TCP や UDP などの IP プロトコル。
DPort	宛先ポート番号。コード 1 は、TCP や UDP などの IP プロトコルを示します。
Sport	送信元ポート番号です。コード 1 は、TCP や UDP などの IP プロトコルを示します。
Prev Hop	前のホップの IP アドレス。空白は、前のホップがないことを意味します。
I/F	前のホップのインターフェイス。
BPS	予約レート（1 秒あたりのビット数（bps）単位）。
Mode(s)	次の文字列のいずれか。 • CLI：この予約は、ローカル RSVP コマンドを介して作成されています。 • Host：ルータは、この予約のホスト システムまたは RSVP エンドポイントとして機能しています。 • Host CLI：表示されている静的な送信者が **iprsvpsender-host** コマンドによって作成されていることを意味する、「Host」および「CLI」という文字列の組み合わせ。 • LSP-Tunnel：この予約は、トラフィック エンジニアリング（TE）トンネルの予約です。 • MIB：この予約は、リモート管理ステーションからの SNMP SET ディレクティブを介して作成されています。
アイデンティティ	RSVP アプリケーション ID のエイリアス文字列。
ロケータ	この静的に設定されている送信者に対し、RSVP PATH メッセージで伝送されるアプリケーション ID。
ID Type	識別情報のタイプ。RSVP では、アプリケーション ID（アプリケーション）とユーザ ID（ユーザ）という 2 つのタイプが定義されています。Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアでは、アプリケーション ID のみをサポートしています。

関連コマンド

コマンド	説明
iprsvpsender-host	ルータで RSVP PATH メッセージを生成するホストをシミュレートできるようにします。

show ip rsvp host vrf

Virtual Routing and Forwarding（VRF）インスタンスとともに設定されているリソース予約プロトコル（RSVP）ホストの具体的な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 **showiprsvphostvrf** コマンドを使用します。

show ip rsvp host vrf {******vrf-name*} {**receivers|senders**} [{*group-namegroup-address*}]

構文の説明

*	すべての VRF を表示します。
vrf-name	指定した VRF の名前です。
receivers	現在データベースに格納されているRSVP関連の受信側情報を表示します。
senders	現在データベースに格納されているRSVP関連の送信側情報を表示します。
group-name	（オプション）送信元または宛先のホスト名。
group-address	（オプション）送信元または宛先の IP アドレス。

コマンド モード

ユーザ EXEC（<）
特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.0(1)M	このコマンドが導入されました。

使用上のガイドライン

VRF および静的な RSVP 送信者および受信者を表示するには、**showiprsvphostvrf** コマンドを使用します。

例

次の **showiprsvphostvrf*senders** コマンドの出力例では、ローカル送信者について VRF が表示されています。

```
Router# show ip rsvp host vrf * senders
VRF: vrf2
To                  From                Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.4       198.168.104.12      UDP 10    10    none          none     10K
  Mode(s): Host CLI
VRF: vrf1
To                  From                Pro DPort Sport Prev Hop      I/F      BPS
192.168.105.4       198.168.105.12      UDP 10    10    none          none     10K
  Mode(s): Host CLI
```

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 *123 : show ip rsvp host vrf senders* フィールドの説明

フィールド	説明
VRF	VRF の名前。
To	受信者の IP アドレス。
From	送信元の IP アドレス。
Pro	プロトコル コード。TCP や UDP などの IP プロトコル。
DPort	宛先ポート番号。コード 1 は、TCP や UDP などの IP プロトコルを示します。
Sport	送信元ポート番号です。コード 1 は、TCP や UDP などの IP プロトコルを示します。
Prev Hop	前のホップの IP アドレス。空白は、前のホップがないことを意味します。
I/F	前のホップのインターフェイス。
BPS	予約レート（1 秒あたりのビット数（bps）単位）。
Mode(s)	次の文字列のいずれか。 • Host：ルータは、この予約のホスト システムまたは RSVP エンドポイントとして機能しています。 • LSP-Tunnel：この予約は、トラフィック エンジニアリング（TE）トンネルの予約です。 • MIB：この予約は、リモート管理ステーションからの SNMP SET ディレクティブを介して作成されています。 • CLI：この予約は、ローカル RSVP CLI コマンドを介して作成されています。 • Host CLI：表示されている静的な送信者が CLI コマンド **iprsvpsender-host** によって作成されていることを意味する、「Host」および「CLI」という文字列の組み合わせ。

関連コマンド

コマンド	説明
showiprsvphost	RSVP ホストに固有の情報を表示します。

show ip rsvp ingress

インターフェイス上に設定されているリソース予約プロトコル（RSVP）入力帯域幅の情報を表示するには、特権 EXEC モードで **showiprsvpingress** コマンドを使用します。

show ip rsvp ingress interface [detail] [*type number*]

構文の説明

interface	インターフェイスを指定します。
type number	（オプション）インターフェイスのタイプと、インターフェイスまたはサブインターフェイスの番号。
detail	（オプション）入力帯域幅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	変更箇所
15.1(3)T	このコマンドが導入されました。
15.1(1)S	このコマンドが、Cisco IOS Release 15.1(1)S に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

特定のインターフェイスまたはすべてのインターフェイスに設定されている RSVP 入力帯域幅に関する情報を表示するには、**showiprsvpingress** コマンドを使用します。このコマンドでは、オプションのキーワードまたは引数を指定しないと、すべてのインターフェイスに設定されている RSVP 入力帯域幅に関する情報が表示されます。特定のインターフェイスまたはすべてのインターフェイスに設定されている入力帯域幅に関する詳細情報を表示するには、**detail** キーワードを使用します。

例

次は、**showiprsvpingressdetailethernet1/0** コマンドの出力例です。

```
Device# show ip rsvp ingress interface detail ethernet 1/0
interface    rsvp  in-allocated  in-i/f max  in-flow max  VRF
Et1/0        ena   0             7500K       7500K        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 *124 : show ip rsvp ingress* フィールドの説明

フィールド	説明
interface	入力帯域幅が設定されているインターフェイスを表示します。
rsvp	RSVP の状態。値は、enabled（アクティブ化されている）または disabled（非アクティブ化されている）のいずれかです。 （注） このフィールドが disabled になるのは、ルーティング情報ベース（RIB）への登録時に内部エラーが発生した場合のみです。
in-allocated	現在割り当てられている帯域幅の量（1 秒あたりのビット数単位）。
in-i/f max	予約可能な入力帯域幅（kb/s 単位）。
in-flow max	RSVP 入力帯域幅として設定されているインターフェイス帯域幅の割合。
VRF	VRF 名。

関連コマンド

コマンド	説明
iprsvpbandwidth	インターフェイスで IP 用 RSVP をイネーブルにします。
maximumbandwidthingress	入力ポリシープールの帯域幅パラメータを設定します。

show ip rsvp installed

リソース予約プロトコル（RSVP）に関連してインストールされているフィルタと、対応する帯域幅の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 **showiprsvpinstalled** コマンドを使用します。

show ip rsvp installed [**vrf** {******vrf-name*}] [*interface-type interface-number*] **[detail]**

構文の説明

vrf *	（任意）設定された Virtual Routing and Forwarding（VRF）インスタンスをすべて表示します。
vrf *vrf-name*	（オプション）指定された VRF の名前。
interface-type	（オプション）インターフェイスのタイプ。
interface-number	（オプション）インターフェイスの番号。
detail	（オプション）インターフェイスと、それらの予約に関する追加情報を表示します。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
12.2(2)T	このコマンドが Cisco IOS Release 12.2(2)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(15)T	このコマンドが変更されました。コマンドの出力が、圧縮が考慮された後でトラフィック制御ステートブロック（TCSB）に必要となるリソースを表示するように変更されました。
12.2(18)SXF2	このコマンドが、Cisco IOS Release 12.2(18)SXF2 に統合されました。
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。
12.2(33)SRC	このコマンドが変更されました。コマンドの出力が、RSVP集約の情報を表示するように変更されました。
15.0(1)M	このコマンドが変更されました。キーワード **vrf** および ***** と、引数 *vrf-name* が追加されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

（注） コマンドの構文は、プラットフォームとリリースによって異なります。キーワード **vrf** と引数 *vrf-name* の組み合わせは、Cisco ASR 1000 シリーズのルータではサポートされていません。

showiprsvpinstalled コマンドは、インターフェイスとそれらの予約に関する情報を表示します。予約のトラフィック パラメータ、ダウンストリーム ホップ、圧縮、VRF、および対象の予約のサービス品質（QoS）を保証するために RSVP によって使用されるリソースなどの追加情報を表示するには、オプションの **detail** キーワードを使用します。

例

この項では、**showiprsvpinstalled** コマンドの出力例を示します。使用されているインターフェイスまたはプラットフォーム、および、イネーブルにされているオプションによって、表示される出力は次に示すものと若干異なります。

インストールされている IP RSVP：例

次は、**showiprsvpinstalled** コマンドの出力例です。

```
Router# show ip rsvp installed
RSVP: Ethernet1: has no installed reservations
RSVP: Serial0:
     kbps   To              From      Protocol DPort Sport Weight Conversation
     0      192.168.0.0     172.16.2.28     UDP 20    30    128   270
     150    192.168.0.1     172.16.2.1      UDP 20    30    128   268
     100    192.168.0.1     172.16.1.1      UDP 20    30    128   267
     200    192.168.0.1     172.16.1.25     UDP 20    30    256   265
     200    192.168.0.2     172.16.1.25     UDP 20    30    128   271
     0      192.168.0.2     172.16.2.28     UDP 20    30    128   269
     150    192.168.0.2     172.16.2.1      UDP 20    30    128   266
     350    192.168.0.3     172.16.0.0      UDP 20    30    128   26
```

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 *125 : show ip rsvp installed* フィールドの説明

フィールド	説明
kbps	予約されているレート（キロビット/秒単位）。
To	送信元デバイスの IP アドレス。
From	宛先デバイスの IP アドレスを指定します。
Protocol	プロトコル コード。コードは、TCP、User Datagram Protocol（UDP）などの IP プロトコルを示します。
DPort	宛先ポート番号。

フィールド	説明
Sport	送信元ポート番号です。
Weight	重み付け均等化キューイング（WFQ）で使用される重み付け。
Conversation	WFQ カンバセーションの番号。 （注） インターフェイスに WFQ が設定されていない場合、Weight と Conversation はゼロになります。

RSVP 圧縮方式の予測：例

次の **showiprsvpinstalled** detail コマンドの出力例では、圧縮方式、圧縮コンテキスト ID、および 1 パケットあたりの削減されるバイト数など、実行中のシリアル インターフェイス 3/0 上の圧縮パラメータが表示されています。

```
Router# show ip rsvp installed detail
RSVP:Ethernet2/1 has no installed reservations
RSVP:Serial3/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2. Source is 10.1.1.1,
  Protocol is UDP, Destination port is 18054, Source port is 19156
  Compression:(method rtp, context ID = 1, 37.98 bytes-saved/pkt avg)
  Admitted flowspec:
    Reserved bandwidth:65600 bits/sec, Maximum burst:328 bytes, Peak rate:80K bits/sec
    Min Policed Unit:164 bytes, Max Pkt Size:164 bytes
  Admitted flowspec (as required if compression were not applied):
    Reserved bandwidth:80K bits/sec, Maximum burst:400 bytes, Peak rate:80K bits/sec
    Min Policed Unit:200 bytes, Max Pkt Size:200 bytes
  Resource provider for this flow:
    WFQ on FR PVC dlci 101 on Se3/0: PRIORITY queue 24.  Weight:0, BW 66 kbps
  Conversation supports 1 reservations [0x1000405]
  Data given reserved service:3963 packets (642085 bytes)
  Data given best-effort service:0 packets (0 bytes)
  Reserved traffic classified for 80 seconds
  Long-term average bitrate (bits/sec):64901 reserved, 0 best-effort
  Policy:INSTALL. Policy source(s):Default
```

次の **showiprsvpinstalled** detail コマンドの出力例では、圧縮コンテキスト ID が使用できないため、シリアル 3/0 インターフェイス上では圧縮が予測されていないことが表示されています。

```
Router# show ip rsvp installed detail
RSVP:Ethernet2/1 has no installed reservations
RSVP:Serial3/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2. Source is 10.1.1.1,
  Protocol is UDP, Destination port is 18116, Source port is 16594
  Compression:(rtp compression not predicted:no contexts available)
  Admitted flowspec:
    Reserved bandwidth:80K bits/sec, Maximum burst:400 bytes, Peak rate:80K bits/sec
    Min Policed Unit:200 bytes, Max Pkt Size:200 bytes
  Resource provider for this flow:
    WFQ on FR PVC dlci 101 on Se3/0: PRIORITY queue 24.  Weight:0, BW 80 kbps
  Conversation supports 1 reservations [0x2000420]
```

```
Data given reserved service:11306 packets (2261200 bytes)
Data given best-effort service:0 packets (0 bytes)
Reserved traffic classified for 226 seconds
Long-term average bitrate (bits/sec):79951 reserved, 0 best-effort
Policy:INSTALL. Policy source(s):Default
```

（注） 圧縮コンテキスト ID が使用できない場合は、**iprtpcompression-connections***number* コマンドを使用して、圧縮コンテキスト ID のプールを拡大します。

RSVP 集約：例

次に、RSVP 集約が設定されているときに **showiprsvpinstalled** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp installed

RSVP: Ethernet0/0 has no installed reservations
RSVP: Serial1/0
BPS    To              From            Protoc DPort  Sport
300K   192.168.50.1    192.168.40.1    0      46     0
RSVP: RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46)
BPS    To              From            Protoc DPort  Sport
80K    192.168.5.1     192.168.2.1     TCP    222    222
80K    192.168.6.1     192.168.2.1     TCP    223    223
```

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 *126 : show ip rsvp installed* フィールドの説明（*RSVP* 集約が設定されている場合）

フィールド	説明
RSVP	指定されたインターフェイスの予約情報。
BPS	予約されているレート（1 秒あたりのビット数（bps）単位）。
To	送信元デバイスの IP アドレス。
From	宛先デバイスの IP アドレスを指定します。
Protoc	プロトコル コード。 • コードは、エンドツーエンド（E2E）予約の IP プロトコル（TCP や User Datagram Protocol（UDP）など）を示します。 • 集約予約の場合、コードは 0 です。

フィールド	説明
DPort	宛先ポート番号。 • 番号は、E2E 予約のプロトコル宛先ポートを示します。 • 集約予約の場合、番号は Differentiated Services Code Point（DiffServ コード ポイント、DSCP）を示します。
Sport	送信元ポート番号です。 • 番号は、E2E 予約のプロトコル送信元ポートを示します。 • 集約予約の場合、番号は 0 です。
RSVP	集約にマッピングされている個々の E2E 予約。次の事項が表示されます。 • 集約の送信元の IP アドレス。 • 集約の宛先の IP アドレス。 • DiffServ コード ポイント（DSCP）値。

RSVP 集約の詳細：例

次に、RSVP 集約が設定されており、アグリゲータから見た集約予約全体にマッピングされた E2E 予約が存在するときに **showiprsvpinstalleddetail** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp installed detail
RSVP: Ethernet0/0 has no installed reservations
RSVP: Serial1/0 has the following installed reservations
RSVP Reservation. Destination is 192.168.50.1. Source is 192.168.40.1,
  Protocol is 0  , Destination port is 46, Source port is 0
  Traffic Control ID handle: 35000403
  Created: 20:27:14 EST Thu Nov 29 2007
  Admitted flowspec:
    Reserved bandwidth: 300K bits/sec, Maximum burst: 300K bytes, Peak rate: 300K bits/sec

     Min Policed Unit: 20 bytes, Max Pkt Size: 0 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations [0x3000408]
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 24558 seconds
  Long-term average bitrate (bits/sec): 0 reserved, 0 best-effort
  Policy: INSTALL. Policy source(s): Default
RSVP: RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46) has the following installed
reservations
RSVP Reservation. Destination is 192.168.5.1. Source is 192.168.2.1,
  Protocol is TCP, Destination port is 222, Source port is 222
  Traffic Control ID handle: 0500040B
  Created: 20:27:14 EST Thu Nov 29 2007
```

```
Admitted flowspec:
  Reserved bandwidth: 80K bits/sec, Maximum burst: 5K bytes, Peak rate: 80K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
Resource provider for this flow:
  QBM
Conversation supports 1 reservations [0x600040A]
Data given reserved service: 0 packets (0 bytes)
Data given best-effort service: 0 packets (0 bytes)
Reserved traffic classified for 24558 seconds
Long-term average bitrate (bits/sec): 0 reserved, 0 best-effort
Policy: INSTALL. Policy source(s):
```

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 *127 : show ip rsvp installed detail* フィールドの説明（*RSVP* 集約が設定されている場合）

フィールド	説明
RSVP	指定されたインターフェイスの予約情報。

フィールド	説明
RSVP Reservation	シリアル 1/0 インターフェイスの予約情報。次の情報が含まれます。 • 宛先の IP アドレス。 • 集約予約のデアグリゲータ。 • 発信元の IP アドレス。 • 集約予約のアグリゲータ。 • 使用されるプロトコル。 • 集約予約の場合、0 です。 • TCP/UDP または E2E 予約のプロトコル。 • 宛先ポート。 • 集約予約の DiffServ コード ポイント（DSCP）。 • E2E 予約のプロトコル ポート番号。 • 送信元ポート。 • 集約予約の場合、0 です。 • E2E 予約のプロトコル ポート番号。 • 記録を目的として RSVP によって割り当てられたトラフィック コントロール識別子。 • 作成日。 • 帯域幅、最大バースト、ピーク レート、ポリシング済みユニット サイズ、および最大パケット サイズなどの Flowspec 情報。 • リソース プロバイダー情報。 • 集約予約の場合は「None」。 • E2E 予約の場合は QoS 帯域幅マネージャ（BM）。 • Type of service provided：予約済みベスト エフォート型（RSVP/DiffServ ノードが常に 0 パケット）。 • トラフィックが分類される時間の長さ。 • ビットレート（RSVP/DiffServ ノードでは常に 0） • ポリシー。

フィールド	説明
RSVP	次を含む集約情報。 • 集約の送信元の IP アドレス。 • 集約の宛先の IP アドレス。 • DSCP。 （注） 上記以外のフィールドは、上記のフィールドで説明した値を使用して、集約の E2E 予約に関する情報を表示します。

VRF：例

次に、特定の VRF が設定されている場合の出力例を示します。

```
Router# show ip rsvp installed vrf myvrf detail
RSVP: FastEthernet2/0 has the following installed reservations
RSVP Reservation. Destination is 10.10.10.10. Source is 10.10.10.12,
  Protocol is UDP, Destination port is 10, Source port is 10
  Traffic Control ID handle: C8000407
  Created: 22:51:26 UTC Sun Feb 17 2008
  Admitted flowspec:
    Reserved bandwidth: 10K bits/sec, Maximum burst: 10K bytes, Peak rate: 10K bits/sec
    Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations [0xBF000406]
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 12783 seconds
  Long-term average bitrate (bits/sec): 0 reserved, 0 best-effort
  Policy: INSTALL. Policy source(s): Default
VRF : myvrf
```

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 *128 : show ip rsvp installed detail* フィールドの説明（*VRF* が設定されている場合）

フィールド	説明
RSVP	指定されたインターフェイスの予約情報。

フィールド	説明
RSVP 予約	シリアル 1/0 インターフェイスの予約情報。次の情報が含まれます。 • 宛先の IP アドレス。 • 集約予約のデアグリゲータ。 • 発信元の IP アドレス。 • 集約予約のアグリゲータ。 • 使用されるプロトコル。 • 集約予約の場合、0 です。 • TCP/UDP または E2E 予約のプロトコル。 • 宛先ポート。 • 集約予約の DiffServ コード ポイント（DSCP）。 • E2E 予約のプロトコル ポート番号。 • 送信元ポート。 • 集約予約の場合、0 です。 • E2E 予約のプロトコル ポート番号。 • 記録を目的として RSVP によって割り当てられたトラフィック コントロール識別子。 • 作成日。 • 帯域幅、最大バースト、ピーク レート、ポリシング済みユニット サイズ、および最大パケット サイズなどの Flowspec 情報。 • リソース プロバイダー情報。 • 集約予約の場合は「None」。 • E2E 予約の場合は QoS 帯域幅マネージャ（BM）。 • Type of service provided：予約済みベスト エフォート型（RSVP/DiffServ ノードが常に 0 パケット）。 • トラフィックが分類される時間の長さ。 • ビットレート（RSVP/DiffServ ノードでは常に 0） • ポリシー。

フィールド	説明
RSVP	次を含む集約情報。 • 集約の送信元の IP アドレス。 • 集約の宛先の IP アドレス。 • DSCP。 （注） 上記以外のフィールドは、上記のフィールドで説明した値を使用して、集約の E2E 予約に関する情報を表示します。
VRF	VRF の名前。

関連コマンド

コマンド	説明
iprtpcompression-connections	インターフェイス上に存在できる RTP ヘッダー圧縮接続数の合計数を指定します。
showiprsvpinterface	RSVP 関連情報を表示します。
showqueueinginterface	データプレーン情報に関するインターフェイス キューイング統計を表示します。

show ip rsvp interface

リソース予約プロトコル（RSVP）に関連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 rsvp interface** コマンドを使用します。

show ip rsvp interface [**vrf** {******vrf-name*}] **[detail]** [*interface-type interface-number*]

構文の説明

vrf *	（オプション）設定された Virtual Routing and Forwarding（VRF）インスタンスをすべて表示します。
vrf *vrf-name*	（オプション）指定された VRF を表示します。
detail	（オプション）インターフェイスに関する追加情報を表示します。
interface-type	（オプション）インターフェイスのタイプ。
interface-number	（オプション）インターフェイスの番号。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
12.2(2)T	このコマンドが変更されました。**detail** キーワードが追加されました。
12.2(4)T	このコマンドが変更されました。このコマンドは、Cisco 7500 シリーズおよび ATM 相手先固定接続（PVC）インターフェイスに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(13)T	このコマンドが変更されました。このコマンドに対して行われた変更は、次のとおりです。 • レート制限およびリフレッシュ削減の情報が出力の表示に追加されました。 • キーワードまたは引数が入力されていない場合は RSVP グローバル設定が表示されるようになりました。

リリース	変更箇所
12.2(15)T	このコマンドが変更されました。このコマンドに対して行われた変更は、次のとおりです。 • アドミッション コントロールに対する圧縮の影響と、RSVP 帯域幅制限のカウンタが表示に追加されました。 • 暗号化認証パラメータが表示に追加されました。
12.2(18)SFX2	このコマンドが、Cisco IOS Release 12.2(18)SFX2 に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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。
12.2(33)SRB	このコマンドが変更されました。コマンドの出力が、高速ローカル修復（FLR）の情報を表示するように拡張されました。
12.2(33)SRC	このコマンドが変更されました。コマンドの出力が、RSVP集約の情報を表示するように拡張されました。
12.4(20)T	このコマンドが変更されました。コマンドの出力が、指定されたインターフェイスで設定されている RSVP 送信元アドレスを表示するように拡張されました。
15.0(1)M	このコマンドが変更されました。**vrf** および ***** キーワードと *vrf-name* 引数が追加されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。
15.1(3)S1	このコマンドが変更されました。**show ip rsvp interface** コマンドの出力が、すべてのインターフェイスで設定されている RSVP の状態を表示するように拡張されました。

使用上のガイドライン

現在割り当て済みとなっている帯域幅や使用可能な最大帯域幅など、RSVP が有効化されているインターフェイスに関する情報を表示するには、**show ip rsvp interface** コマンドを使用します。帯域幅およびシグナリングのパラメータや遮断の状態を表示するには、オプションの **detail** キーワードを使用します。

インターフェイスに関連付けられているRSVPパラメータの情報を表示するには、**show ip rsvp interface detail** コマンドを使用します。これらのパラメータには、次のものがあります。

- 合計 RSVP 帯域幅。
- 既存のフローに割り当てられている RSVP 帯域幅。
- 単一のフローに割り当て可能な最大の RSVP 帯域幅。
- サポートされているアドミッション コントロールのタイプ（ヘッダー圧縮方式）。

- RSVP 圧縮予測によってサポートされている圧縮方式。
- RSVP 集約。
- RSVP 送信元アドレス。
- VRF。

例

このセクションでは、**show ip rsvp interface** コマンドの出力例を示します。使用されているインターフェイスまたはプラットフォーム、および、イネーブルにされているオプションによって、表示される出力は次に示すものと若干異なります。

RSVP インターフェイス情報：例

次の **show ip rsvp interface** コマンドの出力例では、RSVP が有効になっている各インターフェイスの情報が表示されています。

```
Router# show ip rsvp interface
interface    rsvp       allocated  i/f max  flow max sub max  VRF
Et0/0        ena        300K       1M       1M       0
Et0/1        ena        100K       1M       1M       0
Et1/0        ena        200K       1M       1M       0
Et1/1        ena        0          1M       1M       0
Et1/2        ena        0          1M       1M       0
```

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。

表 *129 : show ip rsvp interface* 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。
rsvp	RSVP の状態。有効であるか無効であるかを示します。
allocated	現在割り当て済みの帯域幅。
i/f max	割り当て可能な最大帯域幅。
flow max	このインターフェイスで割り当て可能な最大の単一フロー。
sub max	このインターフェイスで許可される最大のサブプール値。

RSVP 詳細情報：例

次の **show ip rsvp interfacedetail** コマンドの出力例では、RSVP が有効になっている各インターフェイスの詳細な RSVP 情報が表示されています。

```
Router# show ip rsvp interface detail
```

```
PO0/0:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):200M bits/sec
     Max. allowed (per flow):200M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
 PO1/0:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
     Max. allowed (per flow):50M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
PO1/1:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
     Max. allowed (per flow):50M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
 PO1/2:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
     Max. allowed (per flow):50M bits/secMax. allowed for LSP tunnels using sub-pools:0
 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
 PO1/3:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
     Max. allowed (per flow):50M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
 Lo0:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):200M bits/sec
```

```
    Max. allowed (per flow):200M bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs:0x3F
    Number of refresh intervals to enforce blockade state:4
    Number of missed refresh messages:4
    Refresh interval:30
```

次の表で、POインターフェイス0/0の場合にこの詳細な出力に表示される重要なフィールドを説明します。その他のインターフェイスの場合も、フィールドは同様です。

表 *130 : show ip rsvp interface detail* フィールドの説明：詳細な *RSVP* 情報の例

フィールド	説明
PO0/0	インターフェイス名。
Bandwidth	有効な RSVP 帯域幅パラメータは次のとおりです。 • Curr allocated：現在割り当てられている帯域幅の量（1秒あたりのビット数単位）。 • Max. allowed (total)：許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed (per flow)：1 フローに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed for LSP tunnels using sub-pools：ラベル スイッチド パス（LSP）トンネルに対して許可される帯域幅の最大量（1秒あたりのビット数単位）。 • Set aside by policy (total)：ローカル ポリシーによって確保される帯域幅の量（1 秒あたりのビット数単位）。
Signalling	有効な RSVP シグナリング パラメータは次のとおりです。 • DSCP value used in RSVP msgs：RSVP メッセージで使用されている DiffServ コード ポイント（DSCP）。 • Number of refresh intervals to enforce blockade state：遮断が有効になるまでの時間（ミリ秒単位）。 • Number of missed refresh messages：ルータの状態が期限切れになるまでのリフレッシュ メッセージの件数。 • Refresh interval：リフレッシュ メッセージが送信されるまでの時間（ミリ秒単位）。

RSVP 圧縮方式の予測：例

次の **show ip rsvp interface detail** コマンドの出力例では、RSVP が設定されている各インターフェイスの RSVP の圧縮方式の予測の設定が表示されています。

```
Router# show ip rsvp interface detail
 Et2/1:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):1158K bits/sec
     Max. allowed (per flow):128K bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Admission Control:
     Header Compression methods supported:
       rtp (36 bytes-saved), udp (20 bytes-saved)
   Neighbors:
     Using IP encap:0.  Using UDP encap:0
   Signalling:
     Refresh reduction:disabled
   Authentication:disabled
 Se3/0:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):1158K bits/sec
     Max. allowed (per flow):128K bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Admission Control:
     Header Compression methods supported:
       rtp (36 bytes-saved), udp (20 bytes-saved)
   Neighbors:
     Using IP encap:1.  Using UDP encap:0
   Signalling:
     Refresh reduction:disabled
   Authentication:disabled
```

次の表で、イーサネット インターフェイス 2/1 の場合にこの出力に表示される重要なフィールドを説明します。シリアル インターフェイス 3/0 の場合も、フィールドは同様です。

表 *131 : show ip rsvp interface detail* フィールドの説明：*RSVP* 圧縮方式の予測の例

フィールド	説明
Et2/1	インターフェイス名および番号

フィールド	説明
Bandwidth	有効な RSVP 帯域幅パラメータは次のとおりです。 • Curr allocated：現在割り当てられている帯域幅の量（1 秒あたりのビット数単位）。 • Max. allowed (total)：許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed (per flow)：1 フローに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed for LSP tunnels using sub-pools：LSP トンネルに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Set aside by policy (total)：ローカル ポリシーによって確保される帯域幅の量（1 秒あたりのビット数単位）。
Admission Control	有効なアドミッション コントロールのタイプは次のとおりです。 • Header Compression methods supported: • Real-Time Transport Protocol（RTP）または User Datagram Protocol（UDP）圧縮方式と、1 パケットあたりの削減されるバイト数。
Neighbors	IP および UDP カプセル化を使用するネイバーの数。
シグナリング	有効なシグナリングのタイプ。refresh reduction は「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。
Authentication	Authentication は「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。

RSVP 暗号化認証：例

次の **show ip rsvp interface detail** コマンドの出力例では、ルータ上の RSVP が設定されているすべてのインターフェイスについて、暗号化認証パラメータなどの詳細情報が表示されています。

```
Router# show ip rsvp interface detail
 Et0/0:
   Bandwidth:
    Curr allocated: 0 bits/sec
    Max. allowed (total): 7500K bits/sec
    Max. allowed (per flow): 7500K bits/sec
    Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
    Set aside by policy (total):0 bits/sec
   Neighbors:
    Using IP encap: 0.  Using UDP encap: 0
   Signalling:
```

```
   Refresh reduction: disabled
 Authentication: enabled
   Key:           11223344
   Type:          sha-1
   Window size:   2
   Challenge:     enabled
```

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 *132 : show ip rsvp interface detail* フィールドの説明：暗号化認証の例

フィールド	説明
Et0/0	インターフェイス名および番号
Bandwidth	有効な RSVP 帯域幅パラメータは次のとおりです。 • Curr allocated：現在割り当てられている帯域幅の量（1 秒あたりのビット数単位）。 • Max. allowed (total)：許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed (per flow)：1 フローに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed for LSP tunnels using sub-pools：LSP トンネルに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Set aside by policy (total)：ローカル ポリシーによって確保される帯域幅の量（1 秒あたりのビット数単位）。
Neighbors	IP および UDP カプセル化を使用するネイバーの数。
Signalling	有効なシグナリングのタイプ。refresh reduction は「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。
Authentication	Authentication は「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。パラメータは次のとおりです。 • Key：クリア テキストで表示される RSVP 認証アルゴリズムのキー（文字列）（例：11223344）または <encrypted>。 • Type：RSVP メッセージ内の暗号署名を生成するアルゴリズム。可能な値は「md5」および「sha-1」です。 • Window size：順番に関係なく受信できる RSVP 認証済みメッセージの最大数。 • Challenge：ネットワークで検出された新しい RSVP ネイバーに対して実行されるチャレンジ レスポンス ハンドシェイク。可能な値は「enabled」（アクティブ）または「disabled」（非アクティブ）です。

RSVP FLR：例

次の **show ip rsvp interface detail** コマンドの出力例では、FLR が有効になっているイーサネット 1/0 インターフェイスの詳細情報が表示されています。

```
Router# show ip rsvp interface detail ethernet1/0
  Et1/0:
    RSVP: Enabled
    Interface State: Up
    Bandwidth:
      Curr allocated: 9K bits/sec
      Max. allowed (total): 300K bits/sec
      Max. allowed (per flow): 300K bits/sec
      Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
      Set aside by policy (total): 0 bits/sec
    Traffic Control:
      RSVP Data Packet Classification is ON via CEF callbacks
    Signalling:
      DSCP value used in RSVP msgs: 0x30
      Number of refresh intervals to enforce blockade state: 4
    FLR Wait Time (IPv4 flows):
      Repair is delayed by 500 msec.
    Authentication: disabled
      Key chain:   <none>
      Type:        md5
      Window size: 1
      Challenge:   disabled
    Hello Extension:
      State: Disabled
```

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 *133 : show ip rsvp interface detail* フィールドの説明：*FLR* の例

フィールド	説明
Et1/0	インターフェイス名および番号
RSVP	「enabled」はアクティブであること、「disabled」は非アクティブであることを意味します。
Interface State	「up」はインターフェイスが設定されていること、「down」はインターフェイスが設定されていないことを意味します。

フィールド	説明
Bandwidth	有効な RSVP 帯域幅パラメータは次のとおりです。 • Curr allocated：現在割り当てられている帯域幅の量（1 秒あたりのビット数単位）。 • Max. allowed (total)：許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed (per flow)：1 フローに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed for LSP tunnels using sub-pools：LSP トンネルに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Set aside by policy (total)：ローカル ポリシーによって確保される帯域幅の量（1 秒あたりのビット数単位）。
Traffic Control	「RSVP Data Packet Classification is ON via CEF callbacks」は、すべてのパケットが RSVP によって処理されているわけではないため、過剰なオーバーヘッドが回避され、ネットワークのパフォーマンスが向上していることを意味します。
Signalling	有効なシグナリング パラメータは次のとおりです。 • DSCP value used in RSVP msgs：RSVP メッセージで使用されている DiffServ コード ポイント（DSCP）値。 • Number of refresh intervals to enforce blockade state：遮断が有効になるまでの時間（ミリ秒単位）。
FLR Wait Time (IPv4 flows)	「Repair is delayed by 500 msec」は、指定されたインターフェイスで FLR プロシージャが開始するまでの時間（ミリ秒単位）を示しています。
認証	Authentication は「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。パラメータは次のとおりです。 • Key chain：クリア テキストで表示される RSVP 認証アルゴリズムのキー（文字列）（例：11223344）または <encrypted>。 • Type：RSVP メッセージ内の暗号署名を生成するアルゴリズム。可能な値は「md5」および「sha-1」です。 • Window size：順番に関係なく受信できる RSVP 認証済みメッセージの最大数。 • Challenge：ネットワークで検出された新しい RSVP ネイバーに対して実行されるチャレンジ レスポンス ハンドシェイク。可能な値は「enabled」（アクティブ）または「disabled」（非アクティブ）です。

フィールド	説明
Hello Extension	ネイバー ノードが到達不能になった場合に RSVP ノードでそのことを検出できるようにします。状態は、「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。

RSVP 集約：例

次の **show ip rsvp interface detail** コマンドの出力例では、RSVP が設定されている各インターフェイスの集約パラメータが表示されています。

```
Router# show ip rsvp interface detail
Se1/0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 300K bits/sec
     Max. allowed (total): 400K bits/sec
     Max. allowed (per flow): 400K bits/sec
     Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
     Set aside by policy (total): 0 bits/sec
   Traffic Control:
     RSVP Data Packet Classification is OFF
     RSVP resource provider is: none
   Signalling:
     DSCP value used in RSVP msgs: 0x3F
     Number of refresh intervals to enforce blockade state: 4
   Authentication: disabled
     Key chain:   <none>
     Type:        md5
     Window size: 1
     Challenge:   disabled
   FRR Extension:
     Backup Path: Not Configured
   BFD Extension:
     State: Disabled
     Interval: Not Configured
   RSVP Hello Extension:
     State: Disabled
   RFC 3175 Aggregation: Enabled
     Role: interior
```

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 *134 : show ip rsvp interface detail* フィールドの説明：*RSVP* 集約の例

フィールド	説明
Se1/0	インターフェイス名および番号
RSVP	「enabled」はアクティブであること、「disabled」は非アクティブであることを意味します。
Interface State	「up」はインターフェイスが設定されていること、「down」はインターフェイスが設定されていないことを意味します。

フィールド	説明
Bandwidth	有効な RSVP 帯域幅パラメータは次のとおりです。 • Curr allocated：現在割り当てられている帯域幅の量（1 秒あたりのビット数単位）。 • Max. allowed (total)：許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed (per flow)：1 フローに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed for LSP tunnels using sub-pools：LSP トンネルに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Set aside by policy (total)：ローカル ポリシーによって確保される帯域幅の量（1 秒あたりのビット数単位）。
Traffic Control	RSVP Data Packet Classification Is OFF：データ パケット分類をディセーブルにすると、RSVP は各パケットの処理はしなくなり、アドミッション コントロールのみを実行するようになります。 RSVP Resource Provider is None：リソース プロバイダーを **none** に設定すると、RSVP は、重み付け均等化キューイング（WFQ）や帯域幅などのリソースを予約と関連付けなくなります。 RSVP 集約は RSVP スケーラビリティ拡張をコントロール プレーンの集約のみに使用するため、これらの設定が必要です。トラフィック制御は、クラスベース均等化キューイング（CBWFQ）によって実行されます。
Signalling	有効なシグナリング パラメータは次のとおりです。 • DSCP value used in RSVP msgs：RSVP メッセージの IP ヘッダーで使用されている DiffServ コード ポイント（DSCP）値。 • Number of refresh intervals to enforce blockade state：遮断が有効になるまでの時間（ミリ秒単位）。

フィールド	説明
Authentication	Authentication は「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。パラメータは次のとおりです。 • Key chain：クリアテキストで表示される RSVP 認証アルゴリズムのキー（文字列）（例：11223344）または <encrypted>。 • Type：RSVP メッセージ内の暗号署名を生成するアルゴリズム。可能な値は「md5」および「sha-1」です。 • Window size：順番に関係なく受信できる RSVP 認証済みメッセージの最大数。 • Challenge：ネットワークで検出された新しい RSVP ネイバーに対して実行されるチャレンジ レスポンス ハンドシェイク。可能な値は「enabled」（アクティブ）または「disabled」（非アクティブ）です。
FRR Extension	高速再ルーティング バックアップ パスが設定されているかどうか。
BFD Extension	双方向フォワーディング検出。値は次のとおりです。 • State：「enabled」（アクティブ）または「disabled」（非アクティブ）。 • Interval：値が設定されているか、または「Not Configured」。
RSVP Hello Extension	ネイバー ノードが到達不能になった場合に RSVP ノードでそのことを検出できるようにします。状態は、「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。
RFC 3175 Aggregation	RFC 3175（*AggregationofRSVPforIPv4andIPv6Reservations*）に定義された集約の状態。値は次のとおりです。 • Enabled：アクティブ。 • Disabled：非アクティブ。 Role • Interior：インターフェイスは集約領域に面しています。 • Exterior：インターフェイスは従来の RSVP 領域に面しています。

RSVP 送信元アドレス：例

次の **showiprsvpinterface detail ethernet1/0** コマンドの出力例では、当該のインターフェイスに設定されている送信元アドレスが表示されています。

```
Router# show ip rsvp interface detail ethernet1/0
 Et1/0:
```

```
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 0 bits/sec
     Max. allowed (total): 7500K bits/sec
     Max. allowed (per flow): 7500K bits/sec
     Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
     Set aside by policy (total): 0 bits/sec
   Traffic Control:
     RSVP Data Packet Classification is ON via CEF callbacks
   Signalling:
     DSCP value used in RSVP msgs: 0x3F
     Number of refresh intervals to enforce blockade state: 4
     Ip address used in RSVP objects: 10.1.3.13 <----------source address for Ethernet
0/1
   Authentication: disabled
     Key chain:   <none>
     Type:        md5
     Window size: 1
     Challenge:   disabled
   Hello Extension:
     State: Disabled
```

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 *135 : show ip rsvp interface detail* フィールドの説明：*RSVP* 送信元アドレスの例

フィールド	説明
Et1/0	インターフェイス名および番号
RSVP	「enabled」はアクティブであること、「disabled」は非アクティブであることを意味します。
Interface State	「up」はインターフェイスが設定されていること、「down」はインターフェイスが設定されていないことを意味します。
Bandwidth	有効な RSVP 帯域幅パラメータは次のとおりです。 • Curr allocated：現在割り当てられている帯域幅の量（1 秒あたりのビット数単位）。 • Max. allowed (total)：許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed (per flow)：1 フローに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed for LSP tunnels using sub-pools：LSP トンネルに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Set aside by policy (total)：ローカル ポリシーによって確保される帯域幅の量（1 秒あたりのビット数単位）。

フィールド	説明
Traffic Control	「RSVP Data Packet Classification is ON via CEF callbacks」は、すべてのパケットがRSVPによって処理されているわけではないため、過剰なオーバーヘッドが回避され、ネットワークのパフォーマンスが向上していることを意味します。
Signalling	有効なシグナリング パラメータは次のとおりです。 • DSCP value used in RSVP msgs：RSVP メッセージの IP ヘッダーで使用されている DiffServ コード ポイント（DSCP）値。 • Number of refresh intervals to enforce blockade state：遮断が有効になるまでの時間（ミリ秒単位）。 • IP address used in RSVP objects：指定されたインターフェイスの RSVP 送信元アドレス。
Authentication	Authenticationは「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。パラメータは次のとおりです。 • Key chain：クリア テキストで表示される RSVP 認証アルゴリズムのキー（文字列）（例：11223344）または <encrypted>。 • Type：RSVP メッセージ内の暗号署名を生成するアルゴリズム。可能な値は「md5」および「sha-1」です。 • Window size：順番に関係なく受信できる RSVP 認証済みメッセージの最大数。 • Challenge：ネットワークで検出された新しいRSVPネイバーに対して実行されるチャレンジ レスポンス ハンドシェイク。可能な値は「enabled」（アクティブ）または「disabled」（非アクティブ）です。
Hello Extension	ネイバー ノードが到達不能になった場合に RSVP ノードでそのことを検出できるようにします。状態は、「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。

RSVP VRF：例

次の **show ip rsvp interface vrf my vrf detail** コマンドの出力例では、myvrf という名前のVRFに関連付けられているすべてのインターフェイスに関する情報が表示されています。

```
Router# show ip rsvp interface vrf myvrf detail
Se1/0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
```

```
    Curr allocated: 300K bits/sec
    Max. allowed (total): 400K bits/sec
    Max. allowed (per flow): 400K bits/sec
    Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
    Set aside by policy (total): 0 bits/sec
  Traffic Control:
    RSVP Data Packet Classification is OFF
    RSVP resource provider is: none
  Signalling:
    DSCP value used in RSVP msgs: 0x3F
    Number of refresh intervals to enforce blockade state: 4
  Authentication: disabled
    Key chain:   <none>
    Type:        md5
    Window size: 1
    Challenge:   disabled
  FRR Extension:
    Backup Path: Not Configured
  BFD Extension:
    State: Disabled
    Interval: Not Configured
  RSVP Hello Extension:
    State: Disabled
  RFC 3175 Aggregation: Enabled
    Role: interior
  VRF: myvrf
```

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 *136 : show ip rsvp interface detail* フィールドの説明：*RSVP VRF* の例

フィールド	説明
Se1/0	インターフェイス名および番号
RSVP	「enabled」はアクティブであること、「disabled」は非アクティブであることを意味します。
Interface State	「up」はインターフェイスが設定されていること、「down」はインターフェイスが設定されていないことを意味します。
Bandwidth	有効な RSVP 帯域幅パラメータは次のとおりです。 • Curr allocated：現在割り当てられている帯域幅の量（1 秒あたりのビット数単位）。 • Max. allowed (total)：許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed (per flow)：1 フローに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Max. allowed for LSP tunnels using sub-pools：LSP トンネルに対して許可される帯域幅の最大量（1 秒あたりのビット数単位）。 • Set aside by policy (total)：ローカル ポリシーによって確保される帯域幅の量（1 秒あたりのビット数単位）。

フィールド	説明
Traffic Control	RSVP Data Packet Classification Is OFF：データ パケット分類をディセーブルにすると、RSVP は各パケットの処理はしなくなり、アドミッション コントロールのみを実行するようになります。 RSVP Resource Provider is None：リソース プロバイダーを **none** に設定すると、RSVP は、重み付け均等化キューイング（WFQ）や帯域幅などのリソースを予約と関連付けなくなります。 RSVP 集約は RSVP スケーラビリティ拡張をコントロール プレーンの集約のみに使用するため、これらの設定が必要です。トラフィック制御は、クラスベース均等化キューイング（CBWFQ）によって実行されます。
Signalling	有効なシグナリング パラメータは次のとおりです。 • DSCP value used in RSVP msgs：RSVP メッセージの IP ヘッダーで使用されている DiffServ コード ポイント（DSCP）値。 • Number of refresh intervals to enforce blockade state：遮断が有効になるまでの時間（ミリ秒単位）。
Authentication	Authentication は「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。パラメータは次のとおりです。 • Key chain：クリア テキストで表示される RSVP 認証アルゴリズムのキー（文字列）（例：11223344）または <encrypted>。 • Type：RSVP メッセージ内の暗号署名を生成するアルゴリズム。可能な値は「md5」および「sha-1」です。 • Window size：順番に関係なく受信できる RSVP 認証済みメッセージの最大数。 • Challenge：ネットワークで検出された新しい RSVP ネイバーに対して実行されるチャレンジ レスポンス ハンドシェイク。可能な値は「enabled」（アクティブ）または「disabled」（非アクティブ）です。
FRR Extension	高速再ルーティング バックアップ パスが設定されているかどうか。
BFD Extension	双方向フォワーディング検出。値は次のとおりです。 • State：「enabled」（アクティブ）または「disabled」（非アクティブ）。 • Interval：値が設定されているか、または「Not Configured」。
RSVP Hello Extension	ネイバー ノードが到達不能になった場合に RSVP ノードでそのことを検出できるようにします。状態は、「enabled」（アクティブ）または「disabled」（非アクティブ）のいずれかです。

フィールド	説明
RFC 3175 Aggregation	RFC 3175（*AggregationofRSVPforIPv4andIPv6Reservations*）に定義された集約の状態。値は次のとおりです。 • Enabled：アクティブ。 • Disabled：非アクティブ。 Role • Interior：インターフェイスは集約領域に面しています。 • Exterior：インターフェイスは従来の RSVP 領域に面しています。
VRF	VRF の名前。

関連コマンド

コマンド	説明
showiprsvpinstalled	RSVP 関連のインストールされているフィルタと対応する帯域幅情報を表示します。
showiprsvpneighbor	現在の RSVP ネイバーを表示します。

show ip rsvp interface detail

すべてのインターフェイス タイプについて hello 設定を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip rsvp interface detail** コマンドを使用します。

show ip rsvp interface detail [*type number*]

構文の説明

type number	（オプション）hello設定の表示対象とするインターフェイスのタイプと番号。

コマンド デフォルト

すべてのインターフェイスの hello 設定が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
12.2(33)SRE	このコマンドが変更されました。出力が、PHOP アドレス フィールドで使用されている送信元アドレスを表示するように更新されました。
15.1(2)T	このコマンドが変更されました。出力が、オーバーヘッドの割合を表示するように更新されました。
15.1(1)S	このコマンドが、Cisco IOS Release 15.1(1)S に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズの集約サービス ルータに実装されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

特定のインターフェイスについて hello 設定を表示するには、**show ip rsvp interface detail** コマンドで引数 *type* および *number* を使用します。

例

次に、**show ip rsvp interface detail** コマンドの出力例を示します。

```
Router# show ip rsvp interface detail GigabitEthernet 9/47
```

```
Tu0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 10K bits/sec
     Max. allowed (total): 75K bits/sec
     Max. allowed (per flow): 75K bits/sec
     Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
     Set aside by policy (total): 0 bits/sec
   Admission Control:
     Header Compression methods supported:
       rtp (36 bytes-saved), udp (20 bytes-saved)
     Tunnel IP Overhead percent:
       4
     Tunnel Bandwidth considered:
       Yes
   Traffic Control:
     RSVP Data Packet Classification is ON via CEF callbacks
   Signalling:
     DSCP value used in RSVP msgs: 0x3F
     Number of refresh intervals to enforce blockade state: 4
   Authentication: disabled
     Key chain:   <none>
     Type:        md5
     Window size: 1
     Challenge:   disabled
   Hello Extension:
     State: Disabled
```

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 *137 : show ip rsvp interface detail* フィールドの説明

フィールド	説明
RSVP	リソース予約プロトコル（RSVP）の状態（Enabled または Disabled）。
Interface State	インターフェイスの状態（Up または Down）。
Curr allocated	現在割り当てられている帯域幅の量（1 秒あたりのビット数（b/s）単位）。
Max. allowed (total)	許可される帯域幅の合計最大量（b/s 単位）。
Max. allowed (per flow)	1 フローに対して許可される帯域幅の最大量（b/s 単位）。
Max. allowed for LSP tunnels using sub-pools	帯域幅をサブプールから取得するラベル スイッチド パス（LSP）トンネルに対して許可される帯域幅の最大量。
Tunnel IP Overhead percent	RSVPの帯域幅を手動でオーバーライドするためのオーバーヘッドの割合。
Tunnel Bandwidth considered	トンネルの帯域幅が考慮されているかどうかを示します。
DSCP value used in RSVP msgs	RSVP メッセージ内の DiffServ コード ポイント（DSCP）値。

show ip rsvp listeners

指定されたポートまたはプロトコルのリソース予約プロトコル（RSVP）リスナーを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showiprsvplisteners** コマンドを使用します。

show ip rsvp listeners [{*ip-address*|**any**|**vrf** {***vrf-name***}}] [{**udp**|**tcp**|**any***protocol*}] [{*dst-port*|**any**}]

構文の説明

ip-address	（オプション）RSVP メッセージの特定の IP アドレス。
any	（オプション）RSVP メッセージの任意の IP アドレス宛先。
vrf *	（任意）設定された Virtual Routing and Forwarding（VRF）インスタンスをすべて表示します。
vrf *vrf-name*	（オプション）指定された VRF の情報を表示します。
udp	（オプション）受信インターフェイスで使用される User Datagram Protocol（UDP）と、UDP 送信元ポート番号。
tcp	（オプション）受信インターフェイスで使用される TCP と、TCP 送信元ポート番号。
any	（オプション）受信インターフェイスで使用される任意のプロトコルと、UDP または TCP 送信元ポート番号。
protocol	（オプション）受信インターフェイスで使用されるプロトコルと、UDP または TCP 送信元ポート番号。 （注） *protocol* 引数を選択する場合、範囲は 0 から 255 までで、使用されるプロトコルは IP です。
dst-port	（オプション）RSVP メッセージ用の特定の宛先ポート（0 から 65535 まで）。
any	（オプション）RSVP メッセージの任意の宛先。

コマンド デフォルト

showiprsvplisteners コマンドをキーワードまたは引数なしで入力すると、RSVP が設定されている各インターフェイスで送受信されたすべてのリスナーが表示されます。

コマンド モード

ユーザ EXEC（<）
特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。

リリース	変更箇所
15.0(1)M	このコマンドが変更されました。キーワード **vrf** および ***** と、引数 *vrf-name* が追加されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

（注） コマンドの構文は、プラットフォームとリリースによって異なります。キーワード **vrf** および ***** と引数 *vrf-name* は、ASR 1000 シリーズ アグリゲーション サービス ルータではサポートされていません。

RSVP が設定されている各インターフェイスで送受信されたリスナーの数を表示するには、**showiprsvplisteners** コマンドを使用します。

例

次の例では、myvrf1 という名前の VRF のリスナーが表示されています。

```
Router# show ip rsvp listeners vrf myvrf1
VRF : myvrf1
```

To Protocol DPort Description Action OutIf

10.0.2.1 any any RSVP Proxy reply

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 *138 : show ip rsvp listeners* コマンド フィールドの説明

フィールド	説明
VRF	リスナーの表示対象とする VRF の名前。
To	受信インターフェイスの IP アドレスです。
Protocol	使用されるプロトコル。
DPort	受信側ルータ上の宛先ポート。
Description	RSVP にリスニングを行うように要求した Cisco IOS コンポーネント。たとえば RSVP プロキシおよびラベル スイッチド パス（LSP）トンネル シグナリングなどです。

フィールド	説明
Action	フローがその宛先に到達したときに実行されるアクション。値は次のとおりです。 • announce：フローの到達がアナウンスされます。 • reply：フローが宛先に到達すると、送信者は応答を受信します。
OutIf	受信側ルータの発信インターフェイス。 （注） このフィールドが空白の場合、リスナーはグローバル設定モードで設定されており、特定のインターフェイスに関連付けられていないことを意味します。インターフェイス名が表示される場合、リスナーはインターフェイス設定モードで設定されており、そのインターフェイスに関連付けられています。

関連コマンド

コマンド	説明
iprsvplisteneroutbound	RSVP ルータを、特定のインターフェイス経由で送信される PATH メッセージをリッスンするように設定します。

show ip rsvp neighbor

現在のリソース予約プロトコル（RSVP）ネイバーを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showiprsvpneighbor** コマンドを使用します。

show ip rsvp neighbor [{**detail**|**inactive [detail]**|**vrf** {***vrf-name***}}]

構文の説明

detail	（オプション）RSVP ネイバーに関する追加情報を表示します。
inactive	（オプション）1 時間を超えてアクティビティがなかった RSVP ネイバーを表示します。
detail	（オプション）非アクティブな RSVP ネイバーに関する追加情報を表示します。
vrf *	（任意）設定された Virtual Routing and Forwarding（VRF）インスタンスをすべて表示します。
vrf *vrf-name*	（オプション）指定された VRF の名前。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
12.2(13)T	引数 *interface-typeinterface-number* が削除されました。コマンドに detail キーワードが追加され、出力にレート制限およびリフレッシュ削減の情報が追加されました。
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。
15.0(1)M	このコマンドが変更されました。キーワード **vrf** および ***** と、引数 *vrf-name* が追加されました。

使用上のガイドライン

現在の RSVP ネイバーの IP アドレスを表示するには、**showiprsvpneighbor** コマンドを使用します。RSVP ネイバーのレート制限およびリフレッシュ削減の情報と VRF 情報を表示するには、**detail** キーワードを入力します。

例

RSVP ネイバーの例

次のコマンドは、現在の RSVP ネイバーを表示します。

```
Router# show ip rsvp neighbor
 10.0.0.1        RSVP
 10.0.0.2        RSVP
```

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。

表 *139 : show ip rsvp neighbor* フィールドの説明

フィールド	説明
10.0.0.1	隣接ルータの IP アドレス。
RSVP	使用されているカプセル化のタイプ。

rate-limiting パラメータおよび refresh-reduction パラメータの例

次のコマンドは、現在の RSVP ネイバーの rate-limiting パラメータおよび refresh-reduction パラメータを表示します。

```
Router# show ip rsvp neighbor detail
Neighbor:10.0.0.1
    Encapsulation:RSVP
    Rate-Limiting:
      Dropped messages:0
Refresh Reduction:
      Remote epoch:0x1BFEA5
      Out of order messages:0
      Retransmitted messages:0
      Highest rcvd message id:1059
      Last rcvd message:00:00:04
Neighbor:10.0.0.2
    Encapsulation:RSVP
    Rate-Limiting:
      Dropped messages:0
    Refresh Reduction:
      Remote epoch:0xB26B1
      Out of order messages:0
      Retransmitted messages:0
      Highest rcvd message id:945
      Last rcvd message:00:00:05
```

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。

表 *140 : show ip rsvp neighbor detail* フィールドの説明

フィールド	説明
Neighbor	近接ルータの IP アドレス。

フィールド	説明
Encapsulation	使用されているカプセル化のタイプ。 （注） RSVP メッセージが IP アドレスに送信されているものの、その IP アドレスから RSVP メッセージが受信されてない場合、「Unknown」と表示されます。これは、エラー状態ではありません。単に、どの RSVP カプセル化（IP または User Datagram Protocol（UDP））が優先されるか、RSVP メッセージの送信にはどの RSVP カプセル化を使用すべきかをルータがまだ認識していないことを意味します。
Rate-Limiting	有効な rate-limiting パラメータは次のとおりです。 • Dropped messages：ネイバーによってドロップされたメッセージの数。
Refresh Reduction	有効な refresh-reduction パラメータは次のとおりです。 • Remote epoch：RSVP メッセージの番号空間識別子（ID）。ノードが再起動するたび、または RSVP プロセスが再起動するたびにランダムに生成されます。 • Out of order messages：順番に従っていないためにドロップされたメッセージの数。 • Retransmitted messages：ネイバーによって再送信されたメッセージの数。 • Highest rcvd message id：ネイバーによって送信されたメッセージ ID のうち、最大の番号。 • Last rcvd message：ネイバーによる最後のメッセージの受信以降の経過時間（時間、分、および秒単位）。

VRF の例

次のコマンドは、myvrf という名前の VRF を表示します。

```
Router# show ip rsvp neighbor vrf myvrf
VRF: myvrf
Neighbor        Encapsulation  Time since msg rcvd/sent
10.10.15.3         Raw IP         00:00:14   00:00:06
10.10.16.2         Raw IP         00:00:29   00:00:15
```

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。

表 *141 : show ip rsvp neighbor vrf* フィールドの説明

フィールド	説明
VRF	VRF の名前。

フィールド	説明
Neighbor	隣接ルータの IP アドレス。
Encapsulation	使用されているカプセル化のタイプ。
Time since msg rcvd/sent	ネイバーによるメッセージ送受信以降の経過時間（hh:mm:ss 形式）。

関連コマンド

コマンド	説明
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。

show ip rsvp p2mp counters

マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）ポイントツーマルチポイント（P2MP）サブラベル スイッチド パス（Sub-LSP）の設定および操作に関連するエラーを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showiprsvpp2mpcounters** コマンドを使用します。

show ip rsvp p2mp 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 モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRE	このコマンドが導入されました。

例

次の例では、MPLS TE P2MP Sub-LSP のエラー カウンタが表示されています。

```
Router# show ip rsvp p2mp counters
RSVP P2MP Error counters
Missing S2L_SUB_LSP object: 1
Multiple S2L_SUB_LSP objects: 1
Session's required bits are not zero: 1
Signalling attributes inconsistent: 1
IP header's destination is different from S2L_SUB_LSP destination: 1
Failed to enqueue S2L_SUB_LSP object into tmb: 1
Illegal Resv style: 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 *142 : show ip rsvp p2mp counters* フィールドの説明

フィールド	説明
Missing S2L_SUB_LSP object	S2L_SUB_LSP オブジェクトには、Sub-LSP の宛先が含まれています。S2L_SUB_LSP オブジェクトが使用できない場合はエラーが発生し、そのエラーはこのフィールドにカウントされます。
Multiple S2L_SUB_LSP objects	S2L_SUB_LSP オブジェクトには、Sub-LSP の宛先が含まれています。S2L_SUB_LSP オブジェクトが複数存在する場合はエラーが発生し、そのエラーはこのフィールドにカウントされます。
Session’s required bits are not zero	セッション オブジェクトの protocol フィールドは 0 である必要があります。そうでない場合はエラーが発生し、そのエラーはこのフィールドにカウントされます。

フィールド	説明
Signalling attributes inconsistent	ルータが P2MP LSP を伝送する場合は、すべての Sub-LSP が同じ属性を伝送する必要があります。そうでない場合はエラーが発生し、そのエラーはこのフィールドにカウントされます。
IP header's destination is different from S2L_SUB_LSP destination	パスに S2L_SUB_LSP オブジェクトのアドレスとは異なる IP ヘッダー宛先アドレスがある場合、そのIPヘッダー内の宛先アドレスは無視され、S2L_SUB_LSP オブジェクト内の宛先アドレスが使用されます。パス内の宛先アドレスがパス独自のアドレスの 1 つである場合、リソース予約プロトコル（RSVP）はそのパスを終了します。このイベントは、このフィールドにカウントされます。
Failed to enqueue S2L_SUB_LSP object into tmb	Sub-LSP がタイマー管理ブロック（TMB）へ送信されない場合はエラーが発生し、そのエラーはこのフィールドにカウントされます。
Illegal Resv style	すべての P2MP Resv メッセージの予約スタイルは、Shared Explicit（SE）です。異なる予約が使用されている場合はエラーが発生し、そのエラーはこのフィールドにカウントされます。

関連コマンド

コマンド	説明
showmplstraffic-engforwardingstatistics	MPLS TE P2MP パスと Sub-LSP に関する情報を表示します。

show ip rsvp policy

現在設定されているポリシーを表示するには、ユーザ EXEC モードまたは特権モードで **showiprsvppolicy** コマンドを使用します。

show ip rsvp policy [{**cops**|**local** [*acl*]}]

構文の説明

cops | **local**	（オプション）設定されている Common Open Policy Service（COPS）サーバまたはローカル ポリシーのいずれかが表示されます。
acl	（オプション）セッションが COPS サーバまたはローカル ポリシーによって管理されているアクセス コントロール リスト（ACL）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	変更箇所
12.1(1)T	このコマンドは、**showiprsvppolicycops** として導入されました。
12.2(13)T	このコマンドは、**local** キーワードを含むように変更されました。**keyword**このコマンドで **showiprsvppolicycops** コマンドが置き換えられます。
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

現在のローカル ポリシー、設定されている COPS サーバ、デフォルト ポリシー、および preemption パラメータ（「disabled」または「enabled」）を表示するには、**showiprsvppolicy** コマンドを使用します。

例

次に、**showiprsvppolicy** コマンドの出力例を示します。

```
Router# show ip rsvp policy
Local policy:
    A=Accept    F=Forward
    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:104
    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:None [Default policy]
COPS:
Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

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。

表 *143 : show ip rsvp policy* コマンド フィールドの説明

フィールド	説明
Local policy	現在設定されているローカル ポリシー。 A = メッセージを受け入れます。 F = メッセージを転送します。 空白（--）は、そのタイプのメッセージは受け入れられず、転送もされないことを意味します。
COPS	現在実行中の COPS サーバ。
Generic policy settings	COPS またはローカル ポリシーに固有ではないポリシー設定。 Default policy：「Accept all」は、すべての RSVP メッセージが受け入れられ、転送されることを意味します。「Reject all」は、すべての RSVP メッセージが拒否されることを意味します。 Preemption：「Disabled」は、特定のローカル ポリシーまたはリモート ポリシーによってプリエンプションの決定が要求される場合、RSVP はそれを実行しないことを意味します。「Enabled」は、特定のローカル ポリシーまたはリモート ポリシーによってプリエンプションの決定が要求される場合、RSVP はそれを実行する必要があることを意味します。

関連コマンド

コマンド	説明
iprsvpsignallinginitial-retransmit-delay	ネットワーク内の RSVP リソースの使用を決定するローカル プロシージャを作成します。

show ip rsvp policy cops

showiprsvppolicycops コマンドは、**showiprsvppolicy** コマンドに置き換えられました。詳細については、**showiprsvppolicy** コマンドを参照してください。

show ip rsvp policy identity

ルータ設定内の特定のリソース予約プロトコル（RSVP）識別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 **showiprsvppolicyidentity** コマンドを使用します。

show ip rsvp policy identity [*regular-expression*]

構文の説明

regular-expression	（オプション）表示される RSVP 識別情報のエイリアス文字列に対してパターン マッチングを行うことを可能にするテキストの文字列。

コマンド デフォルト

設定されているすべての RSVP 識別情報が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(6)T	このコマンドが導入されました。
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。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

表示される RSVP 識別情報のエイリアス文字列に対しパターン マッチングを実行するには、**showiprsvppolicyidentity** コマンドで、オプションの *regular-expression* 引数を使用します。このフィルタリング機能は、多数の識別情報がある設定において RSVP 識別情報の細かいサブセットを検索するのに使用します。

regular-expression 引数を省略すると、設定されているすべての識別子が表示されます。

例

次の **showiprsvppolicyidentity** コマンドの出力例では、設定されているすべての識別情報が表示されています。

```
Router# show ip rsvp policy identity
Alias: voice1
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=1.0
Alias: voice10
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=10.0
Alias: voice100
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=100.0
Alias: voice1000
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=1000.0
```

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 *144 : show ip rsvp policy identity* フィールドの説明

フィールド	説明
Alias	エイリアス文字列の名前。文字列には、印刷可能文字（0x20 ～ 0x7E の範囲）を 64 文字まで使用できます。 文字列の長さに上限はなく、印刷可能文字（0x20 ～ 0x7E の範囲）を含める必要があります。 （注） 空白文字または疑問符（?）を、文字列自体の一部として使用する場合、空白文字または疑問符を入力する前に、CTRL-V キー シーケンスを入力する必要があります。エイリアスが他のルータに送信されることはありません。
Type	識別情報のタイプ。RSVP では、アプリケーション ID（アプリケーション）とユーザ ID（ユーザ）という 2 つのタイプが定義されています。Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアでは、アプリケーション ID のみをサポートしています。
Locator	アプリケーション ID を含む RSVP メッセージに適用する適切なポリシーを検出するためにルータによって使用される情報。

次の **showiprsvppolicyidentity** コマンドの出力例では、エイリアスに voice100 が含まれるすべての識別情報が表示されています。

```
Router# show ip rsvp policy identity voice100
Alias: voice100
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=100.0
Alias: voice1000
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=1000.0
```

次の **showiprsvppolicyidentity** コマンドの出力例では、エイリアスに voice100 に対する完全一致が含まれるすべての識別情報が表示されています。

```
Router# show ip rsvp policy identity ^voice100$
Alias: voice100
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=100.0
```

関連コマンド

コマンド	説明
iprsvplistener	PATH メッセージを受信する RSVP ルータを設定します。
iprsvppolicyidentity	RSVP アプリケーション ID を定義します。
iprsvppolicylocal	RSVP 要求に対する認証の実行方法を決定します。

コマンド	説明
iprsvpreservation	ルータが RSVP RESV メッセージの受信をシミュレートできるようにします。
iprsvpsender	ルータが RSVP PATH メッセージの受信をシミュレートできるようにします。

show ip rsvp policy local

現在設定されているローカル ポリシーを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showiprsvppolicylocal** コマンドを使用します。

show ip rsvp policy local [detail] [**interface** *type number*] [{**acl** *acl-number*|**dscp-ip** *value*|**default**|**identity** *alias*|**origin-as** これを次のように更新します。}]

構文の説明

detail	（オプション）preempt-priority および local-override など、設定されているローカル ポリシーに関する追加情報を表示します。
interface *typenumber*	（任意）インターフェイスを指定します。
acl *acl-number*	（オプション）アクセス コントロール リスト（ACL）を指定します。範囲は 1 ～ 199 です。
dscp-ip *value*	（オプション）集約予約の DiffServ コード ポイント（DSCP）を指定します。有効な値は次のとおりです。 • 0 ～ 63：DSCP の数値。デフォルト値は 0 です。 • af11 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）プレシデンス値。 • default：デフォルト DSCP 値。 • ef：Expedited Forwarding（EF; 完全優先転送）DSCP 値。
default	（オプション）デフォルト ポリシーに関する情報を表示します。
identity *alias*	（オプション）アプリケーション識別情報（ID）のエイリアスを指定します。
origin-as *as*	（オプション）自律システムを指定します。値は 1 ～ 65535 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	変更箇所
12.2(13)T	このコマンドが導入されました。
12.0(29)S	このコマンドが変更されました。**origin-as** キーワードと *as* 引数の組み合わせが追加され、*acl-number* 引数がオプションになりました。

リリース	変更箇所
12.4(6)T	このコマンドが変更されました。**identity***alias* および **interface***typenumber* がキーワードと引数の組み合わせとして追加され、出力がアプリケーション ID の情報を含むように変更されました。
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。
12.2(33)SRC	このコマンドが変更されました。キーワード **dscp-ip** と引数 *value* の組み合わせが追加され、出力が RSVP 集約の情報を含むように変更されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

現在設定されている特定のローカルポリシーに関する情報を表示するには、**showiprsvppolicylocal** コマンドを使用します。**default** キーワードまたは **interface** キーワードと *typenumber* 引数の組み合わせは、1 つまたは複数の一致基準と一緒に使用できます。

次のキーワードと引数の組み合わせを省略すると、現在設定されているすべてのローカルポリシーが表示されます。**acl***acl-number*、**origin-as***as*、**identity***alias*、または**dscp-ip***value*。

一致基準としては、ACL、自律システム、アプリケーションID、またはDSCPというオプションの中から1つだけ指定できます。ただしそのパラメータには、作成済みのローカルポリシーのどの ACL、自律システム、アプリケーション ID、または DSCP でも設定できます。複数のローカルポリシーがあり、それらの一致基準が共通している場合は、そのパラメータを使用すると、一致基準を満たすすべてのローカルポリシーが表示されます。複数のローカルポリシーを作成しており、それぞれが一致基準としての ACL、自律システム、アプリケーション ID、またはDSCPを複数持っている場合、そのパラメータを使用して特定のポリシーのみを表示することはできません。一致基準を省略してすべてのローカルポリシーを表示する必要があります。

例

アプリケーション ID ローカル ポリシーの例

次の **showiprsvppolicylocal** コマンドの出力例では、設定されている、RSVP 識別情報（アプリケーション ID）に基づくグローバル ローカル ポリシーおよびインターフェイスごとのローカル ポリシーが表示されています。**displays**

```
Router# show ip rsvp policy local
  A=Accept    F=Forward
  Global:
    Path:AF Resv:AF PathErr:AF ResvErr:AF ACL(s):101
    Path:AF Resv:AF PathErr:AF ResvErr:AF AS(es):3
```

```
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:voice
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:video

  Serial2/0/0:
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:voice
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:video
  Serial2/0/1:
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:conference
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:iptv
    Path:-- Resv:-- PathErr:-- ResvErr:-- Default

Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

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 *145 : show ip rsvp policy local* フィールドの説明

フィールド	説明
A=Accept F=Forward	RSVP メッセージの状態。 • Accept：受け入れられているメッセージ。 • Forward：転送されているメッセージ。
Global	ローカル ポリシーの場所。Global：ルータ全体に対して設定されているローカル ポリシー。
Path、Resv、PathErr、ResvErr、ACL(s)、AS(es)、ID、Default	受け入れられ、転送されている RSVP メッセージのタイプと、設定されているローカル ポリシーに対する一致基準。空白（--）は、そのタイプのメッセージは受け入れられず、転送もされないことを意味します。
Serial2/0/0、Serial2/0/1	ルータ上の特定のインターフェイスに対して設定されているローカル ポリシー。
Path、Resv、PathErr、ResvErr、ACL(s)、AS(es)、ID	受け入れられ、転送されている RSVP メッセージのタイプと、設定されているローカル ポリシーのタイプ。空白（--）は、そのタイプのメッセージは受け入れられず、転送もされないことを意味します。

フィールド	説明
Generic policy settings	いずれのローカル ポリシーまたはリモート ポリシーにも固有ではないポリシー設定。 • Default policy：「Accept all」は、すべての RSVP メッセージが受け入れられ、転送されることを意味します。「Rejectall」は、すべての RSVP メッセージが拒否されることを意味します。 • Preemption：「Disabled」は、特定のローカル ポリシーまたはリモートポリシーによってプリエンプションの決定が要求される場合、RSVP はそれを実行しないことを意味します。「Enabled」は、特定のローカル ポリシーまたはリモート ポリシーによってプリエンプションの決定が要求される場合、RSVP はそれを実行する必要があることを意味します。

DSCP-IP ローカル ポリシーの例

次の **showiprsvppolicylocal** コマンドの出力例では、設定されている、DSCP EF に基づくグローバル ローカル ポリシーが表示されています。**displaysa**

```
Router# show ip rsvp policy local dscp-ip ef

    A=Accept    F=Forward
    Global:
      Path:AF Resv:AF PathErr:AF ResvErr:AF DSCP(s): ef
Generic policy settings:
    Default policy: Accept all
    Preemption:     Enabled
```

各フィールドの説明については、後述の表を参照してください。

show ip rsvp policy local detail の例

次の **showiprsvppolicylocaldetail** コマンドの出力例では、ローカル ポリシーの場所（ポリシーはグローバルに設定されているか、または特定のインターフェイスに対して設定されているかなど）と、プリエンプションの範囲および最大帯域幅の設定が表示されています。**shows**プリエンプションの優先度と、送信者および受信者の制限も表示されます。これらは、デフォルトに設定されている場合であっても表示されます。

```
Router# show ip rsvp policy local detail
Global:
  Policy for ID: voice
    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           02000409.
                           Accept               Forward
    Path:                  Yes                  Yes
    Resv:                  Yes                  Yes
```

```
    PathError:             Yes                  Yes
    ResvError:             Yes                  Yes
                           Setup Priority       Hold Priority
    TE:                    N/A                  N/A
    Non-TE:                N/A                  N/A
                           Current              Limit
    Senders:               0                    40
    Receivers:             0                    N/A
    Conversations:         0                    N/A
    Group bandwidth (bps): 0                    200K
    Per-flow b/w (bps):    N/A                  10M
  Policy for ID: video
    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           0200040A.

                           Accept               Forward
    Path:                  Yes                  Yes
    Resv:                  Yes                  Yes
    PathError:             Yes                  Yes
    ResvError:             Yes                  Yes
                           Setup Priority       Hold Priority
    TE:                    2                    2
    Non-TE:                5                    4
                           Current              Limit
    Senders:               2                    10
    Receivers:             2                    10
    Conversations:         2                    10
    Group bandwidth (bps): 100K                 200K
    Per-flow b/w (bps):    N/A                  10M
Ethernet2/1:
  Policy for ID: voice
    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           0200040B.

                           Accept               Forward
    Path:                  Yes                  Yes
    Resv:                  Yes                  Yes
    PathError:             Yes                  Yes
    ResvError:             Yes                  Yes
                           Setup Priority       Hold Priority
    TE:                    2                    2
    Non-TE:                5                    4
                           Current              Limit
    Senders:               2                    10
    Receivers:             2                    10
    Conversations:         2                    10
    Group bandwidth (bps): 100K                 200K
    Per-flow b/w (bps):    N/A                  10M
Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

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 *146 : show ip rsvp policy local detail* フィールドの説明

フィールド	説明
Global	ローカル ポリシーの場所。Global：ルータ全体に対して設定されているローカル ポリシー。
Policy for ID	「voice」という名前のアプリケーション ID エイリアスに対して定義されているグローバル ローカル ポリシー。
Preemption Scope	同じインターフェイス上では、RSVP サービス品質（QoS）予約のいずれのクラスが他の RSVP QoS 予約のクラスによってプリエンプション処理されうるかを示します。 「Unrestricted」は、「voice」などのアプリケーション ID を使用する予約は、他の「voice」以外の予約も含め、その予約と同じインターフェイス上の他のすべての予約クラスをプリエンプション処理できることを意味します。
Local Override	実行されているローカル ポリシーを適用することで、任意のリモート ポリシーをオーバーライドします。 • Disabled：非アクティブ。 • Enabled：アクティブ。
Fast ReRoute	マルチプロトコル ラベル スイッチング（MPLS）/トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）に対する高速再ルーティングの状態。 • Accept：受け入れられているメッセージ。 • Do not accept：高速再ルーティング サービスを要求するメッセージは受け入れられません。
Handle	経理目的で RSVP によってセキュリティ アソシエーションに割り当てられた内部データ ベース ID。
Accept、Forward	RSVP メッセージの状態。
Path、Resv、PathError、ResvError	受け入れられ、転送されている RSVP メッセージのタイプ。 • Yes：メッセージは受け入れられ、転送されています。 • No：メッセージは受け入れられておらず、転送もされていません。

フィールド	説明
Setup Priority、Hold Priority	プリエンプション優先度。「Setup Priority」は、予約が最初にインストールされたときの優先度を示します。「Hold Priority」は、予約がインストールされた後の優先度を示します。 「N/A」は、プリエンプション優先度が設定されていないことを示します。
TE	TE 予約のプリエンプション優先度。「Setup Priority」と「Hold Priority」の値は 0 から 7 までで、0 が最高の優先度と見なされます。
Non-TE	非 TE 予約のプリエンプション優先度。「Setup Priority」と「Hold Priority」の値は 0 から 65535 までで、65535 が最高の優先度と見なされます。
Current、Limit	次の許可されるパラメータの現在の数と最大数。
Senders	当該のポリシーによって受け入れおよび/または承認される現在の PATH 状態の数。
Receivers	当該のポリシーによって受け入れられる現在の RESV 状態の数。
Conversations	当該のローカル ポリシーで承認されるアクティブな帯域幅要求の数。
Group bandwidth (bps)	予約のクラスに対して設定されている帯域幅の量（1 秒あたりのビット数（bps）単位）。
Per-flow b/w (bps)	各予約に対して設定されている帯域幅の量（1 秒あたりのビット数（bps）単位）。
Ethernet2/1	ルータ上の特定のインターフェイスに対して設定されているローカル ポリシー。
Generic policy settings	当該のローカル ポリシーに固有ではないポリシー設定。 • Default policy：「Accept all」は、すべての RSVP メッセージが受け入れられ、転送されることを意味します。「Reject all」は、すべての RSVP メッセージが拒否されることを意味します。 • Preemption：「Disabled」は、特定のローカル ポリシーまたはリモート ポリシーによってプリエンプションの決定が要求される場合、RSVP はそれを実行しないことを意味します。「Enabled」は、特定のローカル ポリシーまたはリモート ポリシーによってプリエンプションの決定が要求される場合、RSVP はそれを実行する必要があることを意味します。

関連コマンド

コマンド	説明
iprsvppolicylocal	RSVP 要求に対する認証の実行方法を決定します。

show ip rsvp policy vrf

Virtual Routing and Forwarding（VRF）インスタンスとともに設定されているリソース予約プロトコル（RSVP）ポリシーの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 **showiprsvppolicyvrf** コマンドを使用します。

{**show ip rsvp policy vrf** {*****_vrf-name_} [**identity** [_alias_]]|**local** [{**acl** _acl_|**default**|**detail** [{**acl** _acl_|**default**|**identity** _alias_|**interface** _interface-type_|**origin-as** _as-number_}]}]}

構文の説明

*	すべての VRF を表示します。
vrf-name	指定した VRF の名前です。
ID	（オプション）RSVP メッセージの POLICY-DATA オブジェクトで伝達される一意の情報。
alias	（オプション）ルータ内でRSVP設定コマンド内の識別情報を参照および表示するために使用されている文字列を指定します。文字列には、引用符および正規表現を含む 64 の印刷可能文字（0x20 ～ 0x7E の範囲）を含めることができます。 （注） 空白文字または疑問符（?）を、エイリアスの一部またはロケータ文字列自体として使用する場合、空白文字または疑問符を入力する前に、CTRL/V キー シーケンスを入力する必要があります。エイリアスが他のルータに送信されることはありません。
local	（オプション）ローカル ポリシー。
acl	（オプション）ローカル ポリシーのアクセス コントロール リスト（ACL）。
acl	（オプション）ACL を指定します。各 ACL の値は 1 ～ 199 です。
default	（オプション）デフォルト ポリシー。
detail	（オプション）VRF の詳細情報。
acl	（オプション）ローカル ポリシーのアクセス コントロール リスト（ACL）。
acl	（オプション）ACL を指定します。各 ACL の値は 1 ～ 199 です。
default	（オプション）デフォルト ポリシー。
ID	（オプション）アプリケーション ID

alias	（オプション）ルータ内でRSVP設定コマンド内の識別情報を参照および表示するために使用されている文字列を指定します。文字列には、引用符および正規表現を含む 64 の印刷可能文字（0x20 ～ 0x7E の範囲）を含めることができます。 （注） 空白文字または疑問符（?）を、エイリアスの一部またはロケータ文字列自体として使用する場合、空白文字または疑問符を入力する前に、CTRL/V キー シーケンスを入力する必要があります。エイリアスが他のルータに送信されることはありません。
interface	（オプション）VRF のインターフェイス。
interface-type	（オプション）VRF のインターフェイス名。
origin-as	（オプション）VRF の自律システム（AS）。
as-number	（オプション）AS。各自律システムの値は 1 ～ 65535 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	変更箇所
15.0(1)M	このコマンドが導入されました。

使用上のガイドライン

VRF に対して設定されているポリシーを表示するには、**showiprsvppolicyvrf** コマンドを使用します。

例

次の例では、指定した VRF に対して設定されている ACL ローカル ポリシーが表示されています。

```
Router# show ip rsvp policy vrf myVrf1 local acl 101
    A=Accept    F=Forward
VRF: myVrf1
    Global:
      Path:AF Resv:AF PathErr:AF ResvErr:AF ACL(s): 101
    Ethernet0/0:
      Path:AF Resv:AF PathErr:AF ResvErr:AF ACL(s): 101
Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

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 *147 : show ip rsvp policy vrf* フィールドの説明

フィールド	説明
A=Accept	メッセージを受け入れます。

フィールド	説明
F=Forward	メッセージを転送します。
VRF	VRF の名前。 Global：VRF に対して設定されているグローバル ポリシー。 Path: AF：これらのメッセージを受け入れ、転送します。 Resv: AF：これらのメッセージを受け入れ、転送します。 PathErr：これらのメッセージを受け入れ、転送します。 ResvErr：これらのメッセージを受け入れ、転送します。 ACL(s)：アクセス コントロール リストの番号。 Ethernet0/0：VRF のために設定されているインターフェイス。
Generic policy settings	COPS またはローカル ポリシーに固有ではないポリシー設定。 Default policy：「Accept all」は、すべての RSVP メッセージが受け入れられ、転送されることを意味します。「Reject all」は、すべての RSVP メッセージが拒否されることを意味します。 Preemption：「Disabled」は、特定のローカル ポリシーまたはリモート ポリシーによってプリエンプションの決定が要求される場合、RSVP はそれを実行しないことを意味します。「Enabled」は、特定のローカル ポリシーまたはリモート ポリシーによってプリエンプションの決定が要求される場合、RSVP はそれを実行する必要があることを意味します。

関連コマンド

コマンド	説明
iprsvppolicyvrf	VRF に対する RSVP ポリシーを設定します。

show ip rsvp precedence

リソース予約プロトコル（RSVP）インターフェイスについてIPプレシデンスの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 **showiprsvpprecedence** コマンドを使用します。

show ip rsvp precedence [**type number**]

構文の説明

type	（任意）インターフェイスのタイプです。
number	（オプション）インターフェイスの番号。

コマンド モード

ユーザ EXEC モード（>）
特権 EXEC モード（#）

コマンド履歴

リリース	変更箇所
15.0(1)M	このコマンドが導入されました。

使用上のガイドライン

RSVPを使用するように設定されている特定のインターフェイスについてIPプレシデンスの情報を取得するには、show ip rsvp precedence コマンドでインターフェイス名を指定します。ルータ上の RSVP が有効になっているすべてのインターフェイスについて IP プレシデンスの情報を取得するには、show ip rsvp precedence コマンドをインターフェイス名を指定せずに使用します。

例

次の例では、RSVP が有効になっているインターフェイスの IP プレシデンスの情報が表示されています。

```
Router# show ip rsvp precedence ethernet 0/1
Interface name   Precedence  Precedence   TOS          TOS
                   conform     exceed     conform     exceed
Ethernet0/0          -           -          -           -
Ethernet0/1          -           -          -           -
Ethernet1/1          -           -          4           -
Ethernet1/2          3           -          -           -
```

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。

表 *148 : show ip rsvp precedence* フィールドの説明

フィールド	説明
Interface name	インターフェイスの詳細を表示します。

フィールド	説明
Precedence conform	インターフェイスでのIPプレシデンスの準拠に関する情報を表示します。 （注） 「Precedence conform」の値は、RSVP Flowspec に準拠するトラフィックに対し、0から7までの範囲のIPプレシデンス値を指定します。
Precedence exceed	インターフェイスでのIPプレシデンスの超過に関する情報を表示します。 （注） 「Precedence exceed」の値は、RSVP Flowspec を超過するトラフィックに対し、0から7までの範囲のIPプレシデンス値を指定します。
TOS conform	インターフェイスでの IP タイプ オブ サービス（ToS）の準拠に関する情報を表示します。 （注） 「TOS conform」の値は、RSVP Flowspec に準拠するトラフィックに対し、0 から 31 までの範囲の ToS 値を指定します。
TOS exceed	インターフェイスでの IP タイプ オブ サービス（ToS）の超過に関する情報を表示します。 （注） 「TOS exceed」の値は、RSVP Flowspec を超過するトラフィックに対し、0 から 31 までの範囲の ToS 値を指定します。

関連コマンド

コマンド	説明
show ip rsvp	RSVP 関連情報を表示します。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。
showiprsvptos	RSVPが有効なインターフェイスのIP TOS情報を表示します。

show ip rsvp request

現在データベース内にあるリソース予約プロトコル（RSVP）関連の要求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 **showiprsvprequest** コマンドを使用します。

T、12.2S、12.2SB、12.2(33)SRD、およびこれら以前のリリースでの構文
show ip rsvp request [detail] [**filter** [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]] [**vrf** {**vrf-name*}]

フィルタリング セッション タイプが「all」の場合の 12.2(33)SRE での構文
show ip rsvp request [detail] [**filter** [**session-type all**]]

フィルタリング セッション タイプが「1」の場合の 12.2(33)SRE での構文
show ip rsvp request [detail] [**filter** [**session-type** *session-type-number*]] [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]

フィルタリング セッション タイプが「7」または「13」の場合の 12.2(33)SRE での構文
show ip rsvp request [detail] [**filter** [**session-type** *session-type-number*]] [{**destination** *ip-addresshostname*}] [**lsp-id** *lsp-id*] [{**sender** *ip-addresshostname*}] [**tunnel-id** *tunnel-id*]

構文の説明

detail	（任意）追加の受信者情報を指定します。
filter	（任意）表示する受信者のサブネットを指定します。
session-type *session-type-number*	（任意）表示する RSVP セッションのタイプを指定します。有効な値は次のとおりです。 • **1** （IPv4 セッションの場合） • **7**（IPv4 ポイントツーポイント（P2P）トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）トンネル セッションの場合） • **13** （IPv4 ポイントツーマルチポイント（P2MP）TE LSP トンネル セッションの場合）
all	（任意）RSVP セッションのすべてのタイプを指定します。
destination *ip-address*	（オプション）宛先 IP アドレスを指定します。
hostname	（オプション）宛先のホスト名。
dst-port *port-number*	（任意）宛先ポート番号を指定します。有効な宛先ポート番号の範囲は 0 ～ 65535 です。
lsp-id *lsp-id*	（オプション）ラベル スイッチド パス ID を指定します。有効な番号の範囲は 0 ～ 65535 です。

sender *ip-address*	（オプション）トンネル ヘッドの IP アドレスを指定します。
hostname	（オプション）トンネル ヘッドのホスト名。
source *ip-address*	（オプション）送信元の送信元 IP アドレスを指定します。
hostname	（オプション）送信元のホスト名。
src-port *port-number*	（任意）送信元ポートの番号を指定します。有効な送信元ポート番号の範囲は 0 ～ 65535 です。
tunnel-id *tunnel-id*	（オプション）トンネルID番号を指定します。有効な番号の範囲は 0 ～ 65535 です。
vrf *	（任意）設定された Virtual Routing and Forwarding（VRF）インスタンスをすべて表示します。
vrf *vrf-name*	（オプション）指定された VRF の名前。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
12.2	このコマンドが Cisco IOS Release 12.2 に統合されました。追加の要求情報を表示するため、**detail** キーワードが追加されました。
12.0(22)S	このコマンドは Cisco IOS リリース 12.0(22)S に統合されました。このコマンドは、リンクステート パケット（LSP）がこのノードで終了するバックアップ トンネルをアクティブに使用している場合（つまり、このノードがマージポイントである場合）に高速再ルーティング情報を表示するように拡張されました。このコマンドは、Cisco 10000 シリーズ エッジ サービス ルータ（ESR）でサポートされています。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SRC	コマンドの出力が、RSVP 集約の情報を表示するように変更されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
15.0(1)M	このコマンドが変更されました。キーワード **vrf** および ***** と、引数 *vrf-name* が追加されました。

リリース	変更箇所
12.2(33)SRE	このコマンドが変更されました。特定のタイプのトンネルを表示するため、**session-type** キーワードが追加されました。出力が、マルチプロトコル（MPLS）TE P2MP 情報を表示するように変更されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

指定したインターフェイスまたはすべてのインターフェイスについてアップストリームに要求されている現在の RSVP 予約を表示するには、**showiprsvprequest** コマンドを使用します。集約または拒否されている予約のため、受信される予約は要求とは異なる場合があります。必要に応じ、単一のトンネルまたはトンネルのサブセットに関してのみ情報を表示することができます。

表示の制限

何百または何千ものトンネルが存在するものの、関心があるのはそのうちわずかのみである場合は、単一のトンネルまたはトンネルのサブセットに関してのみ出力を表示することができます。表示を制限するよう要求するには、**showiprsvprequest** コマンドで、次の適切なキーワード（出力フィルタと呼ばれます）を使用します。**destination**、**dst-port**、**source**、および**src-port**。出力フィルタは、そのいずれかまたはすべてを入力することができるほか、**detail** キーワードを指定していてもそうでなくても入力できます。

showiprsvprequestvrf *vrf-name* コマンドを使用すると、出力を特定の VRF のみに制限することもできます。

例

RSVP 集約の例 1

次に、RSVP 集約が設定されているときに **showiprsvprequest** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp request
To            From          Pro DPort Sport Next Hop      I/F      Fi Serv BPS
192.168.5.1   192.168.2.1   TCP 222   222   192.168.40.1  Se1/0    FF RATE 80K
192.168.50.1  192.168.40.1  0   46    0     10.10.10.4    Se1/0    FF LOAD 300K
```

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 *149 : show ip rsvp request* フィールドの説明

フィールド	説明
To	エンドツーエンド（E2E）受信者またはデアグリゲータの IP アドレス。
From	E2E 送信者またはアグリゲータの IP アドレス。

フィールド	説明
Pro	プロトコル コード。 • 「TCP」は、Transmission Control Protocol を示します。 • コード 0 は、集約予約を示します。
DPort	宛先ポート番号。 • 集約予約の DSCP。
Sport	送信元ポート番号です。 • 集約予約の場合、0 です。
Next Hop	ネクスト ホップの IP アドレス。 • 集約にマッピングされた E2E 予約のアグリゲータ。 • インターフェイスに対する集約または E2E 予約のネクスト ホップ RSVP ノード。
I/F	ネクスト ホップのインターフェイス。
Fi	フィルタ（Wildcard Filter、Shared Explicit、または Fixed Filter）。
Serv	サービス（可能な値は「**rate**」または「**load**」です）。
BPS	予約に対する RSVP 予約要求のレート（1 秒あたりのビット数単位）。 （注） 例では、上の行は 80 bps で伝送される E2E 予約であり、下の行は 300 bps で伝送される対応する集約要求です。

RSVP 集約の例 2

次に、RSVP 集約が設定されているときに **showiprsvprequestdetail** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp request detail

RSVP Reservation. Destination is 192.168.5.1, Source is 192.168.2.1,
  Protocol is TCP, Destination port is 222, Source port is 222
  Prev Hop: 192.168.40.1 on Serial1/0
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Average Bitrate is 80K bits/sec, Maximum Burst is 5K bytes
  Request ID handle: 0100040E.
  Policy: Forwarding. Policy source(s): Default
    Priorities - preempt: 0, defend: 0
  PSB Handle List [1 elements]: [0x19000407]
```

```
  RSB Handle List [1 elements]: [0x17000409]
  3175 Aggregation: RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46)
RSVP Reservation. Destination is 192.168.50.1, Source is 192.168.40.1,
  Protocol is 0  , Destination port is 46, Source port is 0
  Prev Hop: 10.10.10.4 on Serial1/0
  Reservation Style is Fixed-Filter, QoS Service is Controlled-Load
  Average Bitrate is 300K bits/sec, Maximum Burst is 300K bytes
  Request ID handle: 0100040B.
  Policy: Forwarding. Policy source(s): Default
    Priorities - preempt: 0, defend: 0
  PSB Handle List [1 elements]: [0x9000408]
  RSB Handle List [1 elements]: [0x100040A]
```

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 *150 : show ip rsvp request detail* : *RSVP* 集約フィールドの説明

フィールド	説明
RSVP Reservation	Destination：E2E RESV メッセージの受信者の IP アドレス。 Source：E2E RESV メッセージの送信者の IP アドレス。
Protocol	Protocol：使用されている IP プロトコル。TCP：Transmission Control Protocol。 • 集約予約の場合、0 です。
Destination port	受信者のポート番号。 • 集約予約の DSCP。
Source port	送信者のポート番号。 • 集約予約の場合、0 です。
Previous Hop	指定されたインターフェイス上の前のホップの IP アドレス。 （注） デアグリゲータから見た集約にマッピングされている E2E 予約の場合、アグリゲータの IP アドレスです。
Reservation Style	複数予約の帯域幅の共有。値は「Fixed-Filter」、「Shared-Explicit」、「および Wildcard-Filter」です。
QoS Service	設定されているサービス品質（QoS）のタイプ。値は「Guaranteed-Rate」および「Controlled -Load」です。
Average Bitrate	データのために要求される平均レート（1 秒あたりのビット数単位）。
Maximum Burst	許容される最大データ量（キロバイト単位）。
Request ID handle	記録を目的として RSVP によって要求に割り当てられた内部データベース ID。

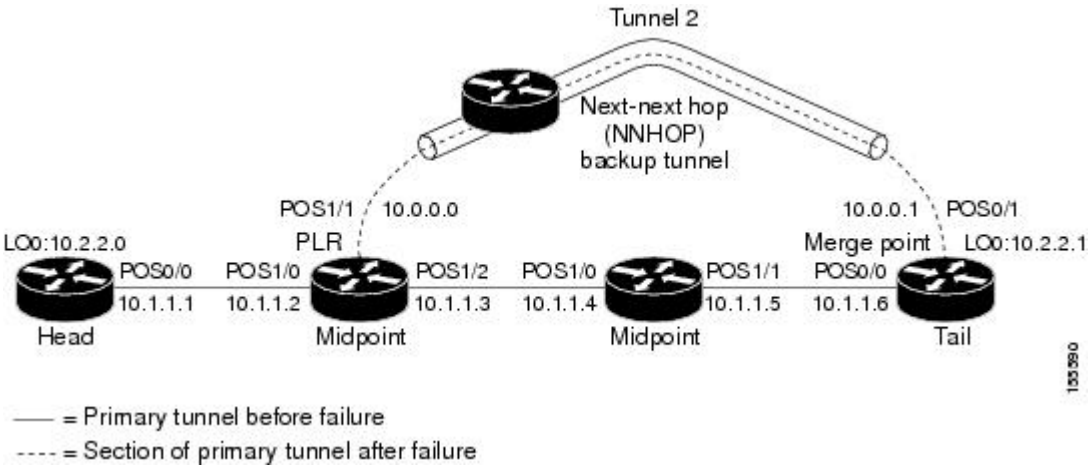
フィールド	説明
Policy	Policy status: Forwarding：RSVP RESV メッセージが受け入れられ、転送されています。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Priorities	予約の RSVP プリエンプション優先度および保持優先度。デフォルトは 0 です。
PSB Handle List	記録を目的として RSVP によって割り当てられたパス ステート ブロック（PSB）内部データベース識別子。
RSB Handle List	記録を目的として RSVP によって割り当てられた予約ステート ブロック（RSB）内部データベース識別子。
3175 Aggregation	RFC 3175「*Aggregation of RSVP for IPv4 and IPv6 Reservations*」で定義されている RSVP 集約。 （注） この E2E 予約は、アグリゲータ（送信元）IP アドレスが 192.168.40.1、宛先（デアグリゲータ）IP アドレスが 192.168.50.1、DSCP 値が「Expedited Forwarding（EF）」である RSVP 予約にマッピングされています。

マージ ポイントの例

次に、障害の前後にマージ ポイントに対して **showiprsvprequestdetail** コマンドを入力した場合の出力例を示します。

次の図は、RSVP 設定例のネットワーク トポロジを示します。

図 *57 : RSVP* 設定例のネットワーク トポロジ



例 1：障害発生前にマージ ポイントに対してコマンドを入力した場合。

```
Router# show ip rsvp request detail

RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.1.1.5 on POS0/1
   Label is 0
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
    Empty
```

例 2：障害発生後にマージ ポイントに対してコマンドを入力した場合。

```
Router# show ip rsvp request detail

RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.1.1.5 on POS0/1
   Label is 0
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
     Empty
   FRR is in progress (we are Merge Point)
 RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.0.0.0 on POS0/1
   Label is 0
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
     Empty
   FRR is in progress (we are Merge Point)
```

障害発生後には、再ルーティングされる LSP に対して 2 つのエントリがあることに注意してください。

1 つ目のエントリは、障害発生前の情報（RESV メッセージは POS0/1 上の 10.1.1.5 に送信される）を引き続き表示しています。この状態は、障害発生前は、RESV は障害発生前に送信されたパス メッセージへの応答としてアップストリームへと送信されていたことを意味します。この状態はすぐにタイムアウトするか、アップストリームのノードが障害を認識していない場合などは数分間継続してリフレッシュされます。

2 つ目のエントリは、障害発生後の情報（RESV メッセージは POS0/1 上の 10.0.0.0 に送信される）を表示しています。この状態は、障害の後は、RESV メッセージはアップストリームへと（ローカル修復ポイント（PLR）へと）送信されていることを示すもので、LSP が再ルーティングされている限り継続し、リフレッシュされます。

例 2 では、マージ ポイントは LSP のテールであります。ダウンストリームのノードがないため、レコード ルート オブジェクト（RRO）の情報はありません。

MPLS トラフィック エンジニアリング ポイントツーマルチポイントの例

次に、MPLS TE P2MP 情報を表示する **showiprsvprequestdetail** コマンドの出力例を示します。

```
Router# show ip rsvp request detail
Request:
  P2MP ID: 22  Tun ID: 22  Ext Tun ID: 10.1.1.201
  Tun Sender: 10.1.1.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
  SubGroup ID: 1
  S2L Destination : 10.1.1.203
  Prev Hop:10.1.1.205 on Ethernet1/1
  Label: 17 (incoming)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Average Bitrate is 500K bits/sec, Maximum Burst is 1K bytes
  Request ID handle: 0100042C.
  Policy: Forwarding. Policy source(s): MPLS/TE
  PSB Handle List [1 elements]: [0x1000427]
  RSB Handle List [1 elements]: [0x100042B]
```

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 *151 : show ip rsvp request* : *MPLS TE P2MP* フィールドの説明

フィールド	説明
P2MP ID	P2MP トンネルの宛先セットを指定する 32 ビットの番号。
Tun ID	トンネル ID 番号。
Ext Tun ID	拡張トンネル ID 番号。
Tun Sender	送信元の IP アドレス。
LSP ID	ラベル スイッチド パス ID 番号。
SubGroup Orig	LSP ヘッドエンド ルータ ID アドレス。
SubGroup ID	ヘッドエンド ルータからのシグナルを受ける各サブ LSP に割り当てられる増分番号。
S2L Destination	LSP テールエンド ルータ ID アドレス。

次に、ポイントツーマルチポイント トラフィックでの RSVP RESV 要求が表示されている **showiprsvprequestfiltersession-type13** コマンドの出力例を示します。

```
Router# show ip rsvp request filter session-type 13

Destination   Tun Sender    TunID LSPID P2MP-ID SubID Next Hop      I/F     BPS
192.168.5.1   10.1.1.201    22    1     22      1     192.168.40.1  Se1/0   80K
```

関連コマンド

コマンド	説明
showiprsvpreservation	現在データベースに格納されている RSVP PATH 関連の受信側情報を表示します。
showiprsvpsender	現在データベースに格納されている RSVP RESV 関連の受信側情報を表示します。

show ip rsvp reservation

現在データベースに格納されているリソース予約プロトコル（RSVP）関連の受信者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 **showiprsvpreservation** コマンドを使用します。

Cisco IOS リリース T、12.2S、12.2SB、12.2(33)SRD、Cisco IOS XE リリース 2.6、およびこれら以前のリリースでの構文

show ip rsvp reservation [detail] [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]] [**vrf** {*|*vrf-nam* **e**}]

フィルタリング セッション タイプが「all」の場合の Cisco IOS リリース 12.2(33)SRE での構文

show ip rsvp reservation [detail] [**filter** [**session-type all**]]

フィルタリング セッション タイプが「1」の場合の Cisco IOS リリース 12.2(33)SRE での構文

show ip rsvp reservation [detail] [**filter** [**session-type** *session-type-number*]] [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]

フィルタリング セッション タイプが「7」または「13」の場合の Cisco IOS リリース 12.2(33)SRE での構文

show ip rsvp reservation [detail] [**filter** [**session-type** *session-type-number*]] [**destination** *address*] [**lsp-id** *lsp-id*] [**sender** *address*] [**tunnel-id** *tunnel-id*]

構文の説明

detail	（任意）追加の受信者情報を指定します。
filter	（任意）表示する受信者のサブネットを指定します。
destination *address*	（オプション）受信者の宛先ホスト名またはIPアドレスを指定します。
dst-port *port-number*	（任意）宛先ポート番号を指定します。宛先ポート番号の範囲は 0 ～ 65535 です。
source *address*	（オプション）受信者の送信元ホスト名またはIPアドレスを指定します。
src-port *port-number*	（任意）送信元ポートの番号を指定します。送信元ポート番号の範囲は 0 ～ 65535 です。
vrf *	（任意）設定された Virtual Routing and Forwarding（VRF）インスタンスをすべて表示します。
vrf-name	（オプション）指定された VRF の名前。

session-type *session-type-number*	（任意）表示する RSVP セッションのタイプを指定します。有効な値は次のとおりです。 • **1**（IPv4 セッションの場合） • **7**（IPv4 ポイントツーポイント（P2P）トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）トンネル セッションの場合） • **13**（IPv4 ポイントツーマルチポイント（P2MP）TE LSP トンネル セッションの場合）
all	（任意）RSVP セッションのすべてのタイプを指定します。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
12.2	このコマンドが Cisco IOS Release 12.2 に統合されました。追加の予約情報を表示するため、**detail** キーワードが追加されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
12.4(4)T	このコマンドは Cisco IOS Release 12.4（4）T に統合されました。出力が、アプリケーション ID 情報を表示するように変更されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SRC	このコマンドが変更されました。コマンドの出力が、トンネル ベース アドミッション コントロール（TBAC）情報および RSVP 集約情報を表示するように変更されました。
15.0(1)M	このコマンドが変更されました。キーワード **vrf** および ***** と、引数 *vrf-name* が追加されました。
12.2(33)SRE	このコマンドが変更されました。**session-type** キーワードが追加され、指定したタイプのトンネルが表示されるようになりました。出力が変更され、MPLS TE P2MP の情報が表示されるようになりました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

（注） コマンドの構文は、プラットフォームとリリースによって異なります。キーワード **vrf** および ***** と引数 *vrf-name* は、ASR 1000 シリーズ アグリゲーション サービス ルータではサポートされていません。

指定したインターフェイスまたはすべてのインターフェイスについてデータベースに格納されている現在の受信者（RESV）情報を表示するには、**showiprsvpreservation** コマンドを使用します。この情報には、集約され、他の RSVP ルータから転送される予約が含まれます。

表示の制限

何百または何千ものトンネルが存在するものの、関心があるのはそのうちわずかのみである場合は、単一のトンネルまたはトンネルのサブセットに関してのみ出力を表示することができます。表示を制限するよう要求するには、**showiprsvpreservation** コマンドで、次の適切なキーワード（出力フィルタと呼ばれます）を使用します。**destination**、**dst-port**、**source**、および **src-port**。出力フィルタは、そのいずれかまたはすべてを入力することができるほか、**detail** キーワードを指定していてもそうでなくても入力できます。

showiprsvpreservationvrf *vrf-name* コマンドを使用すると、出力を特定の VRF のみに制限することもできます。

例

show ip rsvp reservation の例

次は、**showiprsvpreservation** コマンドの出力例です。

```
Router# show ip rsvp reservation
To              From            Pro DPort Sport Next Hop      I/F   Fi Serv
172.16.1.49     172.16.4.53     1   0     0     172.16.1.49     Se1   FF LOAD
```

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 *152 : show ip rsvp reservation* フィールドの説明

フィールド	説明
To	受信者の IP アドレス。
From	送信元の IP アドレス。
Pro	プロトコル コード。
DPort	宛先ポート番号。
Sport	送信元ポート番号です。
Next Hop	ネクスト ホップの IP アドレス。

フィールド	説明
I/F	ネクスト ホップのインターフェイス。
Fi	フィルタです（Wildcard Filter、Shared-Explicit、または Fixed-Filter）。
Serv	サービス（値は「RATE」または「LOAD」です）。

アプリケーション ID の例

次に、アプリケーション ID 情報が表示されている **showiprsvpreservationdetail** コマンドの出力例を示します。

```
Router# show ip rsvp reservation detail

RSVP Reservation. Destination is 192.168.104.3, Source is 192.168.104.1,
  Protocol is UDP, Destination port is 4444, Source port is 4444
  Next Hop is 192.168.106.2, Interface is ATM1/0.1
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Resv ID handle: 0A00040B.
  Created: 12:18:32 UTC Sat Dec 4 2004
  Average Bitrate is 5K bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Status:
  Policy: Forwarding. Policy source(s): Default
    Priorities - preempt: 5, defend: 2
    Application ID: 'GUID=www.cisco.com, VER=10.1.1.2, APP=voice, SAPP=h323'
                    '/usr/local/bin/CallManager'
```

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 *153 : show ip rsvp reservation detail*：アプリケーション *ID* フィールドの説明

フィールド	説明
RSVP Reservation	• Destination：RESV メッセージの受信者の IP アドレス。 • Source：RESV メッセージの送信者の IP アドレス。
Protocol	Protocol：使用されている IP プロトコル。UDP：User Datagram Protocol。
Destination port	受信者のポート番号。
Source port	送信者のポート番号。
Next Hop	ネクスト ホップの IP アドレス。
Interface	ネクスト ホップのインターフェイス タイプ。
Reservation Style	複数予約の帯域幅の共有。値は「Fixed-Filter」、「Shared-Explicit」、「および Wildcard-Filter」です。

フィールド	説明
QoS Service	設定されているサービス品質（QoS）のタイプ。値は「Guaranteed-Rate」および「Controlled Load」です。
Resv ID handle	記録を目的として RSVP によって RESV メッセージに割り当てられた内部データベース ID。
Created	予約が作成された日時。
Average Bitrate	データのための平均レート（1 秒あたりのビット数単位）。
Maximum Burst	許容される最大データ量（キロバイト単位）。
Min Policed Unit	アプリケーション データおよび IP レベル以上のすべてのプロトコル ヘッダーを含む、アプリケーションによって生成される最小パケットのサイズ（バイト単位）。
Max Pkt Size	許容される最大パケット（バイト単位）。
Status	ローカル ポリシーの状態。値は「Proxied」および「Proxy-terminated」です。 （注） Status フィールドが空白の場合、コマンドはその予約のミッドポイントに対して発行されていることを意味します。
Policy	Policy status: Forwarding：RSVP RESV メッセージが受け入れられ、転送されています。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Priorities	実行中のプリエンプション優先度。 • preempt：開始時の優先度。トラフィック エンジニアリング（TE）予約の場合、値は 0 から 7 までで、0 が最高です。非 TE 予約の場合、値は 0 から 65535 までで、0 が最低です。 • defend：保持優先度。値は、「preempt」と同じです。
Application ID	送信者アプリケーションを識別し、ローカル ポリシーとの照合に使用できる引用可能な文字列。この文字列には、送信者アプリケーションの X.500 識別名形式のポリシー ロケータおよびアプリケーションまたはファイル名が含まれています。

TBAC の例

次に、**showiprsvpreservationdetail** コマンドの出力例を示します。**whenTBACisconfigured:**

```
Router# show ip rsvp reservation detail

RSVP Reservation. Destination is 10.4.0.1, Source is 10.1.0.1,
  Protocol is UDP, Destination port is 100, Source port is 100
  Next Hop: 10.4.0.1 on Tunnel1, out of band
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Resv ID handle: 0100040D.
  Created: 11:59:53 IST Tue Mar 20 2007
  Average Bitrate is 10K bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Status:
  Policy: Forwarding. Policy source(s): Default
```

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 *154 : show ip rsvp reservation detail* : *TBAC* フィールドの説明

フィールド	説明
RSVP Reservation	• Destination：RESV メッセージの受信者の IP アドレス。 • Source：RESV メッセージの送信者の IP アドレス。
Protocol	Protocol：使用されている IP プロトコル。UDP：User Datagram Protocol。
Destination port	受信者のポート番号。
ソース ポート	送信者のポート番号。
Next Hop	アウトオブバンド シグナリングのトンネル インターフェイス上のネクストホップの IP アドレス。
Reservation Style	複数予約の帯域幅の共有。値は「Fixed-Filter」、「Shared-Explicit」、「および Wildcard-Filter」です。
QoS Service	設定されている QoS のタイプ。値は「Guaranteed-Rate」および「Controlled Load」です。
Resv ID handle	記録を目的として RSVP によって RESV メッセージに割り当てられた内部データベース ID。
Created	予約が作成された日時。
Average Bitrate	データのための平均レート（1 秒あたりのビット数単位）。
Maximum Burst	許容される最大データ量（キロバイト単位）。
Min Policed Unit	アプリケーション データおよび IP レベル以上のすべてのプロトコル ヘッダーを含む、アプリケーションによって生成される最小パケットのサイズ（バイト単位）。
Max Pkt Size	許容される最大パケット（バイト単位）。

フィールド	説明
Status	ローカル ポリシーの状態。値は「Proxied」および「Proxy-terminated」です。 （注） Status フィールドが空白の場合、コマンドはその予約のミッドポイントに対して発行されていることを意味します。
Policy	Policy status: Forwarding：RSVP RESV メッセージが受け入れられ、転送されています。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。

RSVP 集約の例

次に、**showiprsvpreservationdetail** コマンドの出力例を示します。**whenRSVPaggregationisconfigured:**

```
Router# show ip rsvp reservation detail

RSVP Reservation. Destination is 192.168.5.1, Source is 192.168.2.1,
  Protocol is TCP, Destination port is 222, Source port is 222
  Next Hop: 192.168.50.1 on Serial1/0
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Resv ID handle: 0600040A.
  Created: 20:27:58 EST Thu Nov 29 2007
  Average Bitrate is 80K bits/sec, Maximum Burst is 5K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  DiffServ Integration:  DSCPs: 46
  Status:
  Policy: Forwarding. Policy source(s): Default
  3175 Aggregation: RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46)
RSVP Reservation. Destination is 192.168.50.1, Source is 192.168.40.1,
  Protocol is 0  , Destination port is 46, Source port is 0
  Next Hop: 10.30.1.1 on Serial1/0
  Reservation Style is Fixed-Filter, QoS Service is Controlled-Load
  Resv ID handle: 03000408.
  Created: 20:27:50 EST Thu Nov 29 2007
  Average Bitrate is 300K bits/sec, Maximum Burst is 300K bytes
  Min Policed Unit: 20 bytes, Max Pkt Size: 0 bytes
  Status:
  Policy: Forwarding. Policy source(s): Default
```

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 *155 : show ip rsvp reservation detail* : *RSVP* 集約フィールドの説明

フィールド	説明
RSVP Reservation	• Destination：RESV メッセージの受信者の IP アドレス。 • 集約予約のデアグリゲータ。 • Source：RESV メッセージの送信者の IP アドレス。 • 集約予約のアグリゲータ。
Protocol	Protocol：使用されている IP プロトコル。TCP：Transmission Control Protocol。 • 集約予約の場合、0 です。
Destination port	受信者のポート番号。 • 集約予約の DiffServ コード ポイント（DSCP）。
Source port	送信者のポート番号。 • 集約予約の場合、0 です。
Next Hop	指定されたインターフェイス上のネクスト ホップの IP アドレス。 • アグリゲータから見た集約にマッピングされている E2E 予約の場合、デアグリゲータの IP アドレス。 • デアグリゲータから見た集約予約の場合、「None」。
Reservation Style	複数予約の帯域幅の共有。値は「Fixed-Filter」、「Shared-Explicit」、「および Wildcard-Filter」です。
QoS Service	設定されている QoS サービスのタイプ。値は「Guaranteed-Rate」および「Controlled Load」です。
Resv ID handle	記録を目的として RSVP によって RESV メッセージに割り当てられた内部データベース ID。
Created	予約が作成された日時。
Average Bitrate	データのために要求される平均レート（1 秒あたりのビット数単位）。
Maximum Burst	許容される最大データ量（キロバイト単位）。
Min Policed Unit	アプリケーション データおよび IP レベル以上のすべてのプロトコル ヘッダーを含む、アプリケーションによって生成される最小パケットのサイズ（バイト単位）。 • RSVP 集約用に設定されたノード上では、常に 0 または 20 です。

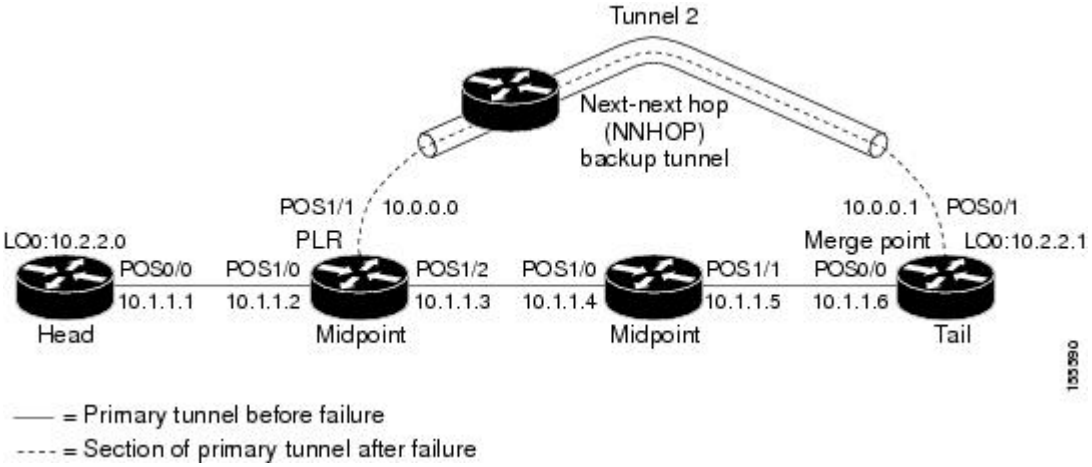
フィールド	説明
Max Pkt Size	許容される最大パケット（バイト単位）。 • RSVP 集約用に設定されたノード上では、常に 0 です。
Status	ローカルポリシーの状態。ポリシーの送信元およびプリエンプションの値。 （注） Status フィールドが空白の場合、コマンドはその予約のミッドポイントに対して発行されていることを意味します。 （注） プリエンプションの値は、ルータで RSVP プリエンプションが有効になっている場合のみ表示されます。
ポリシー	Policy status: Forwarding：RSVP RESV メッセージが受け入れられ、転送されています。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「default」、「local」、および「Multiprotocol Label Switching (MPLS)/traffic engineering (TE)」です。
3175 Aggregation	当該の E2E 予約が送信元（アグリゲータ）および宛先（デアグリゲータ）エンドポイント、IP アドレス、および集約予約 DSCP にマッピングされている集約予約。

ローカル修復ポイント（PLR）の例

次に、障害の前後に PLR に対して **showiprsvpreservationdetail** コマンドを入力した場合の出力例を示します。

次の図は、RSVP 設定例のネットワーク トポロジを示します。

図 *62 : RSVP* 設定例のネットワーク トポロジ



例 1：障害発生前に PLR に対してコマンドを入力した場合

```
Router# show ip rsvp reservation detail
RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.1.1.4 on POS1/2
   Label is 18
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
     10.1.1.5/32, Flags:0x0 (No Local Protection)
       Label record: Flags 0x1, ctype 1, incoming label 18
     10.1.1.6/32, Flags:0x0 (No Local Protection)
       Label record: Flags 0x1, ctype 1, incoming label 0
```

例 2：障害発生後に PLR に対してコマンドを入力した場合

```
Router# show ip rsvp reservation detail
RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   FRR is in progress: (we are PLR)
    Bkup Next Hop is  10.0.0.1 on POS1/1
        Label     is  0
    Orig Next Hop was 10.1.1.4 on POS1/2
        Label     was 18
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
  RRO:
    10.2.2.1/32, Flags:0x0 (No Local Protection)
      Label record: Flags 0x1, ctype 1, incoming label 0
```

例 1 および 例 2 では、次の点（斜体のテキストを参照）に注意してください。

- PLR では、LSP が再ルーティングされたとき（つまり、バックアップ トンネルをアクティブに使用しているとき）に、「Fast Reroute (FRR) is in progress (we are PLR)」と表示されています。
- 障害発生後は、RESV メッセージは、別のインターフェイスに、別のネクストホップから到着しています。障害発生前の表示には、元の NHOP および到着インターフェイスが表示されています。障害発生後の表示には、元および新規（Bkup）の NHOP および到着インターフェイスが両方とも表示されています。ラベルも表示されています。
- RESV メッセージが障害を回避する（つまり、別のリンクまたはホップを通過する）ため、障害発生後は、到着 RESV メッセージ内のレコード ルート オブジェクト（RRO）が変わっています。

MPLS トラフィック エンジニアリング ポイントツーマルチポイントの例

次に、ポイントツーマルチポイント情報が表示されている **showiprsvpreservationdetail** コマンドの出力例を示します。

```
Router# show ip rsvp reservation detail

Reservation:
  P2MP ID: 22  Tun ID: 22  Ext Tun ID: 10.1.1.201
  Tun Sender: 10.1.1.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
  SubGroup ID: 1
  S2L Destination : 10.1.1.203
  Next Hop: 10.0.0.205 on Ethernet0/0
  Label: 20 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Resv ID handle: 0100042A.
  Created: 09:13:16 EST Tue Jun 30 2009
  Average Bitrate is 500K bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 1500 bytes
  RRO:
    10.1.1.205/32, Flags:0x20 (No Local Protection, Node-id)
      Label subobject: Flags 0x1, C-Type 1, Label 20
    10.1.1.202/32, Flags:0x20 (No Local Protection, Node-id)
      Label subobject: Flags 0x1, C-Type 1, Label 17
    10.1.1.203/32, Flags:0x20 (No Local Protection, Node-id)
      Label subobject: Flags 0x1, C-Type 1, Label 16
  Status:
  Policy: Accepted. Policy source(s): MPLS/TE
```

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 *156 : show ip rsvp reservation detail* : *MPLS TE P2MP* フィールドの説明

フィールド	説明
P2MP ID	P2MP トンネルの宛先セットを指定する 32 ビットの番号。
Tun ID	トンネル ID 番号。
Ext Tun ID	拡張トンネル ID 番号。
Tun Sender	送信元の IP アドレス。
LSP ID	ラベル スイッチド パス ID 番号。
SubGroup Orig	LSP ヘッドエンド ルータ ID アドレス。
SubGroup ID	ヘッドエンド ルータからのシグナルを受ける各サブ LSP に割り当てられる増分番号。
S2L Destination	LSP テールエンド ルータ ID アドレス。

次に、ポイントツーマルチポイント トラフィックの RSVP RESV メッセージが表示されている **showiprsvpreserverationfiltersession-type13** コマンドの出力例を示します。

```
Router# show ip rsvp reservation filter session-type 13

Destination   Tun Sender    TunID LSPID P2MP-ID SubID Next Hop      I/F     BPS
10.1.1.203     10.1.1.201     22    1     22      1     10.0.0.205    Et0/0   500K
10.1.1.206     10.1.1.201     22    1     22      2     10.0.0.205    Et0/0   500K
10.1.1.213     10.1.1.201     22    1     22      3     10.0.0.205    Et0/0   500K
```

```
10.1.1.214      10.1.1.201      22    1     22      4     10.0.1.202    Et0/1   500K
10.1.1.216      10.1.1.201      22    1     22      5     10.0.1.202    Et0/1   500K
10.1.1.217      10.1.1.201      22    1     22      6     10.0.1.202    Et0/1   500K
```

関連コマンド

コマンド	説明
clearipsvphelloinstancecounters	Hello インスタンス カウンタの値をクリア（リフレッシュ）します。
iprsvpreservation	ルータで送信者からのRSVP RESV メッセージの受信をシミュレートできるようにします。
showiprsvpsender	現在データベースに格納されている RSVP RESV 関連の受信側情報を表示します。

show ip rsvp sbm

ルータ上にある特定のリソース予約プロトコル（RSVP）対応のインターフェイスまたはすべての RSVP 対応のインターフェイス用に設定された Subnetwork Bandwidth Manager（SBM）に関する情報を表示するには、EXEC モードで **showiprsvpsbm** コマンドを使用します。

show ip rsvp sbm [detail] [*interface-type interface-number*]

構文の説明

detail	（任意）NonResvSendLimit オブジェクトの値など詳細な SBM 設定情報。
interface-type interface-number	（任意）SBM 設定情報を表示するインターフェイス名およびインターフェイス タイプ。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.1(1)T	**detail** キーワードが追加されました。
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

RSVP を使用するように設定された特定のインターフェイスに関する SBM 設定情報を取得するには、**showiprsvpsbm** コマンドでインターフェイス名を指定します。ルータ上の RSVP に対応したすべてのインターフェイスに関する情報を取得するには、インターフェイス名を指定せずに **showiprsvpsbm** コマンドを使用します。

NonResvSendLimit オブジェクトの値を表示するには、**detail** キーワードを使用します。

例

次の例では、ルータ 1 上にある RSVP 対応のイーサネット インターフェイス 1 および 2 の情報を表示しています。

```
Router# show ip rsvp sbm
Interface DSBM Addr      DSBM Priority    DSBM Candidate   My Priority
Et1       10.0.0.0       70               yes              70
Et2       10.2.2.150     100              yes              100
```

次の例では、ルータ 1 上にある RSVP 対応のイーサネット インターフェイス e2 の情報を表示しています。

```
Router# show ip rsvp sbm e2
Interface DSBM Addr       DSBM Priority    DSBM candidate   My Priority
e2        10.2.2.150      100              yes              100
```

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 *157 : show ip rsvp sbm* フィールドの説明

フィールド	説明
Interface	ルータ上の Designated Subnetwork Bandwidth Manager（DSBM）候補インターフェイスの名前。
DSBM Addr	DSBM の IP アドレス。
DSBM Priority	DSBM の優先度。
DSBM Candidate	Yes になるのは、この SBM を DSBM 候補として設定するために **iprsvpdsbmcandidate** コマンドを発行した場合です。No になるのは、そのように設定しなかった場合です。
My Priority	このインターフェイス用に設定された優先度。

次の例では、ルータ 1 上にある RSVP 対応のイーサネット インターフェイス 2 の情報を表示しています。左側のカラムには、ローカル SBM の設定が表示され、右側のカラムには、現在の DSBM の対応する情報が表示されます。この例では、DSBM が選定されたので、情報は同じです。

```
Router# show ip rsvp sbm detailInterface:Ethernet2
Local Configuration             Current DSBM
  IP Address:10.2.2.150         IP Address:10.2.2.150
  DSBM candidate:yes             I Am DSBM:yes
  Priority:100                   Priority:100
  Non Resv Send Limit             Non Resv Send Limit
    Rate:500 Kbytes/sec             Rate:500 Kbytes/sec
    Burst:1000 Kbytes               Burst:1000 Kbytes
    Peak:500 Kbytes/sec             Peak:500 Kbytes/sec
    Min Unit:unlimited              Min Unit:unlimited
    Max Unit:unlimited              Max Unit:unlimited
```

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 *158 : show ip rsvp sbm detail* フィールドの説明

フィールド	説明
Local Configuration	ローカル DSBM 候補コンフィギュレーション。
Current DSBM	現在の DSBM コンフィギュレーション。
Interface	ルータ上の DSBM 候補インターフェイスの名前。

フィールド	説明
IP Address	ローカルの DSBM 候補または現在の DSBM の IP アドレス。
DSBM candidate	Yes になるのは、この SBM を DSBM 候補として設定するために **iprsvpdsbmcandidate** コマンドを発行した場合です。No になるのは、そのように設定しなかった場合です。
I am DSBM	ローカルの候補が DSBM の場合は Yes になります。ローカルの候補が DSBM でない場合は No になります。
Priority	ローカルの DSBM 候補または現在の SBM 用に設定された優先度。
利率	DSBM 候補の平均レート（kbps 単位）。
Burst	DSBM 候補の最大バースト サイズ（KB 単位）。
Peak	DSBM 候補のピーク レート（kbps 単位）。
Min Unit	DSBM 候補の最小ポリシング済みユニット（バイト単位）。
Max Unit	DSBM 候補の最大パケット サイズ（バイト単位）。

関連コマンド

Command	Description
debugiprsvp	SBM メッセージ処理、DSBM 選択プロセス、および標準 RSVP 対応メッセージ処理情報に関する情報を表示します。
debugiprsvpdetail	RSVP と SBM に関する詳細情報を表示します。
debugiprsvpdetailsbm	SBM メッセージのみに関する詳細情報と、SBM と DSBM の状態遷移を表示します。
iprsvpdsbmcandidate	インターフェイスを DSBM 候補として設定します。
iprsvpdsbmnon-resv-send-limit	NonResvSendLimit オブジェクト パラメータを設定します。

show ip rsvp sender

現在データベースに格納されているリソース予約プロトコル（RSVP）PATH 関連の送信者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 **showiprsvpsender** コマンドを使用します。

Cisco IOS リリース T、12.2S、12.2SB、12.2（33）SRD、Cisco IOS XE リリース 2.6、およびそれ以前のリリースの構文

show ip rsvp sender [detail] [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]] [**vrf** {******vrf-name*}]

フィルタリング セッション タイプが「all」の場合の Cisco IOS リリース 12.2(33)SRE での構文

show ip rsvp sender [detail] [**filter** [**session-type all**]]

フィルタリング セッション タイプが「1」の場合の Cisco IOS リリース 12.2(33)SRE での構文

show ip rsvp sender [detail] [**filter** [**session-type** *session-type-number*]] [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]

フィルタリング セッション タイプが「7」または「13」の場合の Cisco IOS リリース 12.2(33)SRE での構文

show ip rsvp sender [detail] [**filter** [**session-type** *session-type-number*]] [**destination** *address*] [**lsp-id** *lsp-id*] [**sender** *address*] [**tunnel-id** *tunnel-id*]

構文の説明

detail	（任意）追加の送信者情報を指定します。
filter	（任意）表示する送信者のサブセットを指定します。
destination *address*	（任意）送信者の宛先となる IP アドレスのホスト名を指定します。
dst-port *port-number*	（任意）宛先ポート番号を指定します。指定できる範囲は 0 ～ 65535 です。
source *address*	（任意）送信者の送信元となる IP アドレスのホスト名を指定します。
src-port *port-number*	（任意）送信元ポートの番号を指定します。指定できる範囲は 0 ～ 65535 です。
vrf *	（任意）設定された Virtual Routing and Forwarding（VRF）インスタンスをすべて表示します。
vrf-name	（オプション）指定された VRF の名前。

session-type *session-type-number*	（任意）表示する RSVP セッションのタイプを指定します。有効な値は次のとおりです。 • **1** IPv4 セッションの場合。 • **7**（IPv4 ポイントツーポイント（P2P）トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）トンネル セッションの場合）。 • **13**（IPv4 ポイントツーマルチポイント（P2MP）TE LSP トンネル セッションの場合）
all	（任意）RSVP セッションのすべてのタイプを指定します。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
12.0(22)S	コマンド出力が Fast Reroute 情報を表示するように変更され、Cisco 10000 シリーズ エッジ サービス ルータ（ESR）のサポートが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
12.4(4)T	コマンド出力がアプリケーション ID 情報を表示するように変更されました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SRB	コマンド出力が高速ローカル修復（FLR）情報を表示するように変更されました。
12.2(33)SRC	コマンドの出力が、トンネル ベース アドミッション コントロール（TBAC）情報および RSVP 集約情報を表示するように変更されました。
15.0(1)M	このコマンドが変更されました。キーワード **vrf** および ***** と、引数 *vrf-name* が追加されました。
12.2(33)SRE	このコマンドが変更されました。**session-type** キーワードが追加され、指定したタイプのトンネルが表示されるようになりました。出力が変更され、MPLS TE P2MP の情報が表示されるようになりました。

リリース	変更箇所
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

（注） コマンドの構文は、プラットフォームとリリースによって異なります。**vrf** キーワードと ***** キーワード、および *vrf-name* 引数は、ASR 1000 シリーズ アグリゲーション サービス ルータではサポートされていません。

指定のインターフェイスまたはすべてのインターフェイスに関して現在データベースに格納されている RSVP 送信元（PATH）情報を表示するには、**showiprsvpsender** コマンドを使用します。

showiprsvpsender コマンドは、ラベル スイッチド パス（LSP）が高速に再ルーティングされた前後で RSVP シグナリングの状態を判別するのに便利です。**showiprsvpsender** コマンドは、ローカル修復ポイント（PLR）またはマージ ポイント（MP）で使用すると特に便利です。

表示の制限

何百または何千ものトンネルが存在するものの、関心があるのはそのうちわずかのみである場合は、単一のトンネルまたはトンネルのサブセットに関してのみ出力を表示することができます。表示を制限するよう要求するには、**showiprsvpsender** コマンドで、次の適切なキーワード（出力フィルタと呼ばれます）を使用します。**destination**、**dst-port**、**source**、および **src-port**。出力フィルタは、そのいずれかまたはすべてを入力することができるほか、**detail** キーワードを指定していてもそうでなくても入力できます。

FLR 統計

FLR 手順の最中やその前後に FLR 統計を表示するには、**showiprsvpsenderdetail** コマンドを使用します。このコマンドは、パス ステート ブロック（PSB）がいつ修復されたかを表示し、FLR 手順が終了した後いつクリーンアップが始まったかを判別するのに使用できます。ただし、このコマンドは古い PLR セグメントや MP セグメントを表示しません。

例

show ip rsvp sender の例

次は、**showiprsvpsender** コマンドの出力例です。

```
Router# show ip rsvp sender
To              From            Pro  DPort  Sport  Prev Hop      I/F    BPS
172.16.1.49     172.16.4.53     1    0      0      172.16.3.53   Et1    80K
172.16.2.51     172.16.5.54     1    0      0      172.16.3.54   Et1    80K
192.168.50.1    192.168.40.1    0    46     0      none          none   17179868160
```

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 *159 : show ip rsvp sender* フィールドの説明

フィールド	説明
To	受信者の IP アドレス。
From	送信元の IP アドレス。
Pro	プロトコル コード。 • コード 1 は、TCP や User Datagram Protocol（UDP）などの IP プロトコルを示します。 • コード 0 は、集約予約を示します。
DPort	宛先ポート番号。 • 集約予約の Differentiated Services Code Point（DSCP; DiffServ コード ポイント）。
Sport	送信元ポート番号です。 • 集約予約の場合は 0 です。
Prev Hop	前のホップの IP アドレス。 • ノードがこの予約のアグリゲータである場合は None です。
I/F	前のホップのインターフェイス。 • ノードがこの予約のアグリゲータである場合は None です。
BPS	送信者データ フローの sender_tspec 特性の指定に従います。ビット レートが 1 秒あたりのビット数で指定されます。 • 集約予約の場合は常に 17179868160 です。

アプリケーション ID の例

次に、アプリケーション ID を設定した **showiprsvpsenderdetail** コマンドの出力例を示します。

```
Router# show ip rsvp sender detail
PATH Session address: 192.168.104.3, port: 4444. Protocol: UDP
  Sender address: 192.168.104.1, port: 4444
     Inbound from: 192.168.104.1 on interface:
  Traffic params - Rate: 5K bits/sec, Max. burst: 1K bytes
                   Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Path ID handle: 09000408.
```

```
Incoming policy: Accepted. Policy source(s): Default
  Priorities - preempt: 5, defend: 2
  Application ID: 'GUID=www.cisco.com, VER=10.1.1.2, APP=voice, SAPP=h323'
                  '/usr/local/bin/CallManager'
Status: Proxied
Output on ATM1/0.1. Policy status: Forwarding. Handle: 04000409
  Policy source(s): Default
```

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 *160 : show ip rsvp sender detail* フィールドの説明

フィールド	説明
PATH Session address	PATH メッセージの宛先 IP アドレス。 • [ポート（port）] : 宛先ポートの番号。 • [プロトコル（Protocol）] : 使用された IP プロトコル。
Sender address	PATH メッセージの送信元 IP アドレス。 • [ポート（port）] : 送信元ポートの番号。
Inbound from	送信者の IP アドレスおよびインターフェイス名。 （注） 空白のインターフェイス フィールドは、PATH メッセージの発生元が、**show** コマンドを実行しているルータ（ヘッドエンド ルータ）であることを意味します。指定したインターフェイスとは、PATH メッセージの発生元が上流に位置するルータであることを意味します。
Traffic params	有効なトラフィック パラメータ： • [レート（Rate）] : 速度（キロビット/秒）。 • [最大バースト（Max. burst）] : 許可されたデータの最大量（キロバイト）。 • [最小ポリシング済みユニット（Min Policed Unit）] : IP レベル以上のアプリケーション データやすべてのプロトコル ヘッダーなど、アプリケーションによって生成された最も小さなパケットのサイズ（バイト）。 • [最大パケット サイズ（Max Pkt Size）] : 許可されている最大パケット（バイト）。
PATH ID handle	記録を目的として RSVP によって PATH メッセージに割り当てられた内部データベース ID。

フィールド	説明
Incoming policy	受信ポリシーの状態： • [承認済み（Accepted）]：RSVP PATH メッセージは承認中ですが、転送されていません。 • [未承認（Not Accepted）]：RSVP PATH メッセージは拒否されています。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Priorities	有効なプリエンプション優先度： • [プリエンプション処理する（preempt）]：起動優先度。トラフィックエンジニアリング（TE）予約の場合、値は 0 から 7 までで、0 が最も高くなります。TE 以外の予約の場合、値は 0 から 65535 までで、0 が最も低くなります。 • [防衛（defend）]：保持優先度。値は、[プリエンプション処理する（preempt）] の場合と同じです。
Application ID	送信者アプリケーションを識別し、ローカル ポリシーとの照合に使用できる引用可能な文字列。この文字列には、送信者アプリケーションの X.500 識別名形式のポリシー ロケータおよびアプリケーションまたはファイル名が含まれています。
Status	ローカル ポリシーのステータス： • [プロキシ済み（Proxied）]：ヘッド。 • [プロキシ終了（Proxy-terminated）]：テール。 • [遮断済み（Blockaded）]：テールまたはミッドポイントで、RESVERROR メッセージを最近受信したところです。このため、PSB は遮断済み状態になります。
Output on ATM1/0/1	ポリシー ステータス（発信インターフェイス上）： • [転送（Forwarding）]：着信 PATH メッセージを転送しています。 • [非転送（Not Forwarding）]：発信 PATH メッセージを拒否しています。 • [ハンドル（Handle）]：記録目的で RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。

FLR の前の例

次に、FLR 発生前の **showiprsvpsenderdetail** コマンドの出力例を示します。

```
Router# show ip rsvp sender detail

PATH:
   Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
   Sender address: 10.10.10.10, port: 1
   Path refreshes:
     arriving: from PHOP 172.16.31.34 on Et0/0 every 30000 msecs
   Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
     Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
   Path ID handle: 01000401.
   Incoming policy: Accepted. Policy source(s): Default
   Status:
   Output on Ethernet1/0. Policy status: Forwarding. Handle: 02000400
     Policy source(s): Default
   Path FLR: Never repaired
```

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 *161 : show ip rsvp sender detail* フィールドの説明：*FLR* 前

フィールド	説明
PATH	PATH メッセージ情報： • 宛先の IP アドレス。 • プロトコルの ID 番号。 • ポリシング。 • 宛先ポート番号。
Sender address	PATH メッセージの送信元 IP アドレス。 • [ポート（port）]：送信元ポートの番号。
Path refreshes	更新情報： • 送信元の IP アドレス（前のホップ [PHOP]）。 • インターフェイス名および番号 • 頻度（ミリ秒（ms））。

フィールド	説明
Traffic params	有効なトラフィック パラメータ： • [レート（Rate）]：速度（キロビット/秒）。 • [最大バースト（Max. burst）]：許可されたデータの最大量（キロバイト）。 • [最小ポリシング済みユニット（Min Policed Unit）]：IP レベル以上のアプリケーション データやすべてのプロトコル ヘッダーなど、アプリケーションによって生成された最も小さなパケットのサイズ（バイト）。 • [最大パケット サイズ（Max Pkt Size）]：許可されている最大パケット（バイト）。
PATH ID handle	記録を目的として RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Incoming policy	受信ポリシーの状態： • [承認済み（Accepted）]：RSVP PATH メッセージは承認中ですが、転送されていません。 • [未承認（Not Accepted）]：RSVP PATH メッセージは拒否されています。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Status	ローカル ポリシーのステータス： • [プロキシ済み（Proxied）]：ヘッド。 • [プロキシ終了（Proxy-terminated）]：テール。 • [遮断済み（Blockaded）]：テールまたはミッドポイントで、RESVERROR メッセージを最近受信したところです。このため、パス ステート ブロック（PSB）は遮断済み状態になります。 （注）　空白のフィールドは上記のいずれでもないことを意味します。
Output on *interface*	ポリシー ステータス（発信インターフェイス上）： • [転送（Forwarding）]：着信 PATH メッセージを転送しています。 • [非転送（Not Forwarding）]：発信 PATH メッセージを拒否しています。 • [ハンドル（Handle）]：記録目的で RSVP によって PATH メッセージに割り当てられた内部データベース ID。

フィールド	説明
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Path FLR	[修復なし（Never repaired）]：ノードがローカル修復ポイント（PLR）になることはなく、このため、PSB を修復しなかったことを示します。

FLR 中の PLR での例

（注） FLR 手順を開始するノードは、ローカル修復ポイント（PLR）です。

次に、FLR 手順中の PLR での **showiprsvpsenderdetail** コマンドの出力例を示します。

```
Router# show ip rsvp sender detail

PATH:
   Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
   Sender address: 10.10.10.10, port: 1
   Path refreshes:
     arriving: from PHOP 172.16.31.34 on Et0/0 every 30000 msecs
   Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
     Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
   Path ID handle: 01000401.
   Incoming policy: Accepted. Policy source(s): Default
   Status:
   Path FLR: PSB is currently being repaired...try later
   PLR - Old Segments: 1
    Output on Ethernet1/0, nhop 172.16.36.34
    Time before expiry: 2 refreshes
    Policy status: Forwarding. Handle: 02000400
       Policy source(s): Default
```

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 *162 : show ip rsvp sender detail* フィールドの説明：*FLR* 中の *PLR*

フィールド	説明
PATH	PATH メッセージ情報には、次のものがあります。 • 宛先の IP アドレス。 • プロトコルの ID 番号。 • ポリシング。 • 宛先ポート番号。

フィールド	説明
Sender address	PATH メッセージの送信元 IP アドレス。 • [ポート（port）]：送信元ポートの番号。
Path refreshes	更新情報： • 送信元の IP アドレス（前のホップ [PHOP]）。 • インターフェイス名および番号 • 頻度（ミリ秒（ms））。
Traffic params	有効なトラフィック パラメータ： • [レート（Rate）]：速度（キロビット/秒）。 • [最大バースト（Max. burst）]：許可されたデータの最大量（キロバイト）。 • [最小ポリシング済みユニット（Min Policed Unit）]：IP レベル以上のアプリケーションデータやすべてのプロトコルヘッダーなど、アプリケーションによって生成された最も小さなパケットのサイズ（バイト）。 • [最大パケット サイズ（Max Pkt Size）]：許可されている最大パケット（バイト）。
PATH ID handle	記録を目的として RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Incoming policy	受信ポリシーの状態： • [承認済み（Accepted）]：RSVP PATH メッセージは承認中ですが、転送されていません。 • [未承認（Not Accepted）]：RSVP PATH メッセージは拒否されています。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。

フィールド	説明
Status	ローカル ポリシーのステータス： • [プロキシ済み（Proxied）]：ヘッド。 • [プロキシ終了（Proxy-terminated）]：テール。 • [遮断済み（Blockaded）]：テールまたはミッドポイントで、RESVERROR メッセージを最近受信したところです。このため、PSB は遮断済み状態になります。 （注）　空白のフィールドは上記のいずれでもないことを意味します。
Path FLR	PSB は現在修復中です。FLR が進行中です。

PLR - Old Segments	PLR が FLR 手順を開始した後の古いセグメントまたはインターフェイスの数。古いセグメントごとに、次の情報が表示されます。
	• [インターフェイスで出力（Output on interface）]：FLR 後の発信インターフェイスおよびネクストホップ IP アドレス。
	• [期限切れまでの時間（Time before expiry）]：古いルート（セグメント）が期限切れになるまでに、新規セグメント上で送信される PATH メッセージの数。
	• ポリシー ステータス（発信インターフェイス上）：
	  • [転送（Forwarding）]：着信 PATH メッセージを転送しています。
	  • [非転送（Not Forwarding）]：発信 PATH メッセージを拒否しています。
	  • [ハンドル（Handle）]：記録目的で RSVP によって PATH メッセージに割り当てられた内部データベース ID。
	• [ポリシーソース（Policy source(s)）]：有効なローカル ポリシーのタイプ。値は [デフォルト（Default）]、[ローカル（Local）]、[MPLS/TE] のいずれかです。

FLR 中の MP での例

（注）　新旧のパス（セグメントまたはインターフェイスとも呼ばれます）が接触するノードがマージ ポイント（MP）です。

次に、FLR 手順中の MP での **showiprsvpsenderdetail** コマンドの出力例を示します。

```
Router# show ip rsvp sender detail
```

```
PATH:
   Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
   Sender address: 10.10.10.10, port: 1
   Path refreshes:
     arriving: from PHOP 172.16.37.35 on Et1/0 every 30000 msecs
Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
     Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
   Path ID handle: 09000406.
   Incoming policy: Accepted. Policy source(s): Default
   Status: Proxy-terminated
   Path FLR: Never repaired
   MP - Old Segments: 1
    Input on Serial2/0, phop 172.16.36.35
    Time before expiry: 9 refreshes
```

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 *163 : show ip rsvp sender detail* フィールドの説明：*FLR* 中の *MP*

フィールド	説明
PATH	PATH メッセージ情報： • 宛先の IP アドレス。 • プロトコルの ID 番号。 • ポリシング。 • 宛先ポート番号。
Sender address	PATH メッセージの送信元 IP アドレス。 • [ポート（port）]：送信元ポートの番号。
Path refreshes	更新情報： • 送信元の IP アドレス（前のホップ [PHOP]）。 • インターフェイス名および番号 • 頻度（ミリ秒（ms））。

フィールド	説明
Traffic params	有効なトラフィック パラメータ： • [レート（Rate）]：速度（キロビット/秒）。 • [最大バースト（Max. burst）]：許可されたデータの最大量（キロバイト）。 • [最小ポリシング済みユニット（Min Policed Unit）]：IP レベル以上のアプリケーション データやすべてのプロトコル ヘッダーなど、アプリケーションによって生成された最も小さなパケットのサイズ（バイト）。 • [最大パケット サイズ（Max Pkt Size）]：許可されている最大パケット（バイト）。
PATH ID handle	記録を目的として RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Incoming policy	受信ポリシーの状態： • [承認済み（Accepted）]：RSVP PATH メッセージは承認中ですが、転送されていません。 • [未承認（Not Accepted）]：RSVP PATH メッセージは拒否されています。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Status	ローカル ポリシーのステータス： • [プロキシ済み（Proxied）]：ヘッド。 • [プロキシ終了（Proxy-terminated）]：テール。 • [遮断済み（Blockaded）]：テールまたはミッドポイントで、RESVERROR メッセージを最近受信したところです。このため、PSB は遮断済み状態になります。 （注）　空白のフィールドは上記のいずれでもないことを意味します。
Path FLR	[修復なし（Never repaired）]：ノードが PLR になることはなく、このため、PSB を修復しなかったことを示します。

フィールド	説明
PLR - Old Segments	PLR が FLR 手順を開始する前の MP 上にあった古いセグメントまたはインターフェイスの数。古いセグメントごとに、次の情報が表示されます。 • インターフェイスで入力（Input on *interface*）：受信インターフェイスおよび前のホップ IP アドレス。 • [期限切れまでの時間（Time before expiry）]：このセグメントが期限切れになるまでに、他のセグメントで受信する PATH メッセージの数。

FLR 後の PLR での例

次に、FLR 手順後の PLR での **showiprsvpsenderdetail** コマンドの出力例を示します。

```
Router# show ip rsvp sender detail

PATH:
   Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
   Sender address: 10.10.10.10, port: 1
   Path refreshes:
     arriving: from PHOP 172.16.31.34 on Et0/0 every 30000 msecs
   Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
     Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
   Path ID handle: 05000401.
   Incoming policy: Accepted. Policy source(s): Default
   Status:
   Output on Serial3/0. Policy status: Forwarding. Handle: 3B000406
     Policy source(s): Default
   Path FLR: Started 12:56:16 EST Thu Nov 16 2006, PSB repaired 532(ms) after.
           Resv/Perr: Received 992(ms) after.
```

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 *164 : show ip rsvp sender detail* フィールドの説明：*FLR* 後の *PLR*

フィールド	説明
PATH	PATH メッセージ情報には、次のものがあります。 • 宛先の IP アドレス。 • プロトコルの ID 番号。 • ポリシング。 • 宛先ポート番号。
Sender address	PATH メッセージの送信元 IP アドレス。 • [ポート（port）]：送信元ポートの番号。

フィールド	説明
Path refreshes	更新情報には次のものがあります。 • 送信元の IP アドレス（前のホップ [PHOP]）。 • インターフェイス名および番号 • 頻度（ミリ秒（ms））。
Traffic params	有効なトラフィック パラメータ： • [レート（Rate）]：速度（キロビット/秒）。 • [最大バースト（Max. burst）]：許可されたデータの最大量（キロバイト）。 • [最小ポリシング済みユニット（Min Policed Unit）]：IP レベル以上のアプリケーション データやすべてのプロトコル ヘッダーなど、アプリケーションによって生成された最も小さなパケットのサイズ（バイト）。 • [最大パケット サイズ（Max Pkt Size）]：許可されている最大パケット（バイト）。
Path ID handle	記録を目的として RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Incoming policy	受信ポリシーの状態： • [承認済み（Accepted）]：RSVP PATH メッセージは承認中ですが、転送されていません。 • [未承認（Not Accepted）]：RSVP PATH メッセージは拒否されています。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Status	ローカル ポリシーのステータス： • [プロキシ済み（Proxied）]：ヘッド。 • [プロキシ終了（Proxy-terminated）]：テール。 • [遮断済み（Blockaded）]：テールまたはミッドポイントで、RESVERROR メッセージを最近受信したところです。このため、PSB は遮断済み状態になります。 （注）　空白のフィールドは上記のいずれでもないことを意味します。

フィールド	説明
Output on Serial3/0	ポリシー ステータス（発信インターフェイス上）： • [転送（Forwarding）]：着信 PATH メッセージを転送しています。 • [非転送（Not Forwarding）]：発信 PATH メッセージを拒否しています。 • [ハンドル（Handle）]：記録目的で RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Path FLR	RSVP がいつ RIB から通知を受信し、PATH メッセージが送信されてからどのくらい経過したかを示す FLR 統計。この遅延が発生するのは、PATH メッセージが送信されたインターフェイスに待機時間が設定されていた場合や、これよりも先に他の PSB が処理された場合、あるいはその両方が発生した場合です。統計には、関連する RESV メッセージや PATHERROR メッセージをいつ受信したかも表示されます。 （注） この遅延により、指定したフローで Quality of Service（QoS）が確保されなかった時間がわかります。

TBAC の例

次に、TBAC が設定されている場合の **showiprsvpsenderdetail** コマンドの出力例を示します。

```
Router# show ip rsvp sender detail

PATH:
  Destination 10.0.0.3, Protocol_Id 17, Don't Police , DstPort 2
  Sender address: 10.0.0.1, port: 2
  Path refreshes:
    arriving: from PHOP 10.1.1.1 on Et0/0 every 30000 msecs. Timeout in 189 sec
  Traffic params - Rate: 10K bits/sec, Max. burst: 10K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 02000412.
  Incoming policy: Accepted. Policy source(s): Default
  Status:
  Output on Tunnel1, out of band. Policy status: Forwarding. Handle: 0800040E
    Policy source(s): Default
  Path FLR: Never repaired
```

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 *165 : show ip rsvp sender detail* フィールドの説明：*TBAC* あり

フィールド	説明
PATH	PATH メッセージ情報： • 宛先の IP アドレス。 • プロトコルの ID 番号。 • ポリシング。 • 宛先ポート番号。
Sender address	PATH メッセージの送信元 IP アドレス。 • [ポート（port）]：送信元ポートの番号。
Path refreshes	更新情報： • 送信元の IP アドレス（前のホップ [PHOP]）。 • インターフェイス名および番号 • 頻度（ミリ秒（ms））。 （注）　空白のフィールドは、更新が発生しなかったことを意味します。
Traffic params	有効なトラフィック パラメータ： • [レート（Rate）]：速度（キロビット/秒）。 • [最大バースト（Max. burst）]：許可されたデータの最大量（キロバイト）。 • [最小ポリシング済みユニット（Min Policed Unit）]：IP レベル以上のアプリケーションデータやすべてのプロトコルヘッダーなど、アプリケーションによって生成された最も小さなパケットのサイズ（バイト）。 • [最大パケット サイズ（Max Pkt Size）]：許可されている最大パケット（バイト）。
PATH ID handle	記録を目的として RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Incoming policy	受信ポリシーの状態： • [承認済み（Accepted）]：RSVP PATH メッセージは承認中ですが、転送されていません。 • [未承認（Not Accepted）]：RSVP PATH メッセージは拒否されています。

フィールド	説明
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Status	ローカル ポリシーのステータス： • [プロキシ済み（Proxied）]：ヘッド。 • [プロキシ終了（Proxy-terminated）]：テール。 • [遮断済み（Blockaded）]：テールまたはミッドポイントで、RESVERROR メッセージを最近受信したところです。このため、PSB は遮断済み状態になります。 （注）　空白のフィールドは上記のいずれでもないことを意味します。
Output on Tunnel1	ポリシー ステータス（アウトオブバンド シグナリングがあるアウトバウンド トンネル上）： • [転送（Forwarding）]：着信 PATH メッセージを転送しています。 • [非転送（Not Forwarding）]：発信 PATH メッセージを拒否しています。 • [ハンドル（Handle）]：記録目的で RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Path FLR	[修復なし（Never repaired）]：ノードがローカル修復ポイント（PLR）になることはなく、このため、PSB を修復しなかったことを示します。

RSVP 集約の例

次に、RSVP 集約が設定されているときに **showiprsvpsenderdetail** コマンドを実行した場合の出力例を示します。

```
Router# show ip rsvp sender detail

PATH:
  Destination 10.10.10.21, Protocol_Id 17, Don't Police , DstPort 1
  Sender address: 10.10.10.11, port: 1
  Path refreshes:
    arriving: from PHOP 10.10.10.34 on Et1/0 every 30000 msecs
  Traffic params - Rate: 10K bits/sec, Max. burst: 10K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 0F000406.
  Incoming policy: Accepted. Policy source(s): Default
  Status:
  3175 Aggregation: agg_info : AggResv 10.10.10.34->10.10.10.2_46
```

```
  Output on Serial2/0. Policy status: Forwarding. Handle: 09000405
    Policy source(s): Default
  Path FLR: Never repaired
PATH:
  Deaggregator 10.10.10.2, DSCP 46, Don't Police
  Aggregator address: 10.10.10.34
  Path refreshes:
    arriving: from PHOP 192.168.34.36 on Et1/0 every 30000 msecs
  Traffic params - Rate: 17179868160 bits/sec, Max. burst: 536870784 bytes
    Min Policed Unit: 1 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 1500040A.
  Incoming policy: Accepted. Policy source(s): Default
  Status: Proxy-terminated
  Path FLR: Never repaired
```

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 *166 : show ip rsvp sender detail* フィールドの説明：*RSVP* 集約あり

フィールド	説明
PATH	E2E 予約の PATH メッセージ情報： • 宛先の IP アドレス。 • プロトコルの ID 番号。 • ポリシング。 • 常に [ポリシングしない（Don't Police）] です。 • 宛先ポート番号。
Sender address	PATH メッセージの送信元 IP アドレス。 • [ポート（port）]：送信元ポートの番号。
Path refreshes	更新情報： • 送信元の IP アドレス（前のホップ [PHOP]）。 • インターフェイス名および番号 • 頻度（ミリ秒（ms））。 （注）　空白のフィールドは、更新が発生しなかったことを意味します。

フィールド	説明
Traffic params	有効なトラフィック パラメータ： • [レート（Rate）]：速度（キロビット/秒）。 • 集約予約の場合、常に [最大レート（MAX rate）] になる可能性があります。 • [最大バースト（Max. burst）]：許可されたデータの最大量（キロバイト）。 • 集約予約の場合、常に [最大バースト（MAX burst）] になる可能性があります。 • [最小ポリシング済みユニット（Min Policed Unit）]：IP レベル以上のアプリケーション データやすべてのプロトコル ヘッダーなど、アプリケーションによって生成された最も小さなパケットのサイズ（バイト）。 • [最大パケット サイズ（Max Pkt Size）]：許可されている最大パケット（バイト）。
PATH ID handle	記録を目的として RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Incoming policy	受信ポリシーの状態： • [承認済み（Accepted）]：RSVP PATH メッセージは承認中ですが、転送されていません。 • [未承認（Not Accepted）]：RSVP PATH メッセージは拒否されています。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Status	ローカル ポリシーのステータス： • [プロキシ済み（Proxied）]：ヘッド。 • [プロキシ終了（Proxy-terminated）]：テール。 • [遮断済み（Blockaded）]：テールまたはミッドポイントで、RESVERROR メッセージを最近受信したところです。このため、PSB は遮断済み状態になります。 （注） 空白のフィールドは上記のいずれでもないことを意味します。

フィールド	説明
3175 Aggregation: agg_info	指定した送信元（アグリゲータ）エンドポイント、宛先（デアグリゲータ）エンドポイント、および DSCP とともに、この E2E 予約がマップされる集約予約の IP アドレス。
Output on Serial2/0	ポリシー ステータス（発信インターフェイス上）： • [転送（Forwarding）]：着信 PATH メッセージを転送しています。 • [非転送（Not Forwarding）]：発信 PATH メッセージを拒否しています。 • [ハンドル（Handle）]：記録目的で RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Path FLR	[修復なし（Never repaired）]：ノードがローカル修復ポイント（PLR）になることはなく、このため、PSB を修復しなかったことを示します。
PATH	集約予約の PATH メッセージ情報： • デアグリゲータ IP アドレス。 • DiffServ コード ポイント（DSCP）値。 • ポリシング。 • 常に [ポリシングしない（Don't Police）] です。 • アグリゲータ IP アドレス。 （注） 残りのパラメータは、前のフィールドに定義されます。

PLR と MP の例

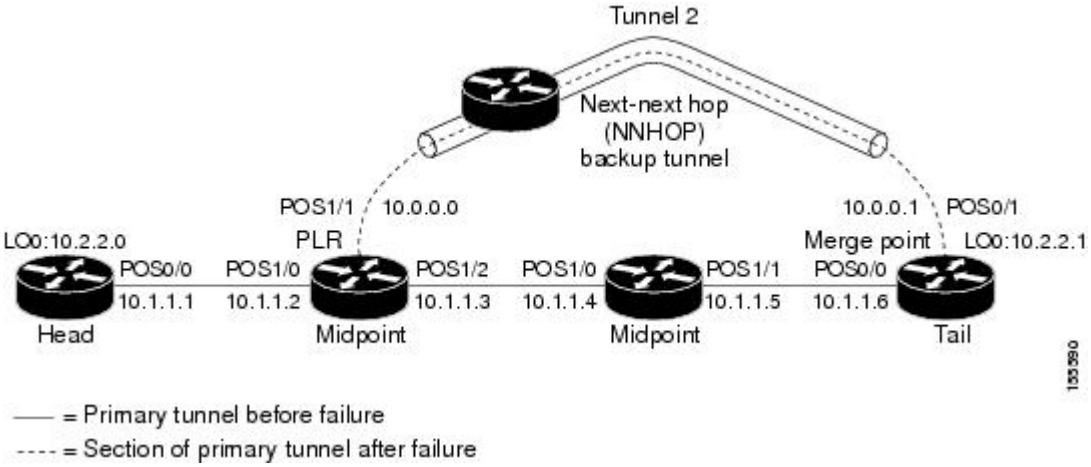
次に、次のような状況下における **showiprsvpsenderdetail** コマンドの出力例を示します。

- コマンドを障害発生前に PLR で入力します（例 1）。
- コマンドを障害発生後に PLR で入力します（例 2）。
- コマンドを障害発生前に MP で入力します（例 3）。
- コマンドを障害発生後に MP で入力します（例 4）。
- コマンド出力には、すべての送信者が表示されます（例 5）。

- コマンド出力には、特定の宛先を持つ送信者のみが表示されます（例 6）。
- コマンド出力には、特定の宛先を持つ送信者に関する詳細が表示されます（例 7）。

次の図は、RSVP 設定例のネットワーク トポロジを示します。

図 *67 : RSVP* 設定例のネットワーク トポロジ



例 1：コマンドを障害発生前に PLR で入力する

次に、障害発生前に PLR で入力したときの **showiprsvpsenderdetail** コマンドの出力例を示します。

```
Router# show ip rsvp sender detail
PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS1/0 from PHOP 10.1.1.1
   Path refreshes being sent to NHOP 10.1.1.4 on POS1/1
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   ERO:
     10.1.1.4 (Strict IPv4 Prefix, 8 bytes, /32)
     10.1.1.5 (Strict IPv4 Prefix, 8 bytes, /32)
     10.1.1.6 (Strict IPv4 Prefix, 8 bytes, /32)
     10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Not active
     Outbound FRR: Ready -- backup tunnel selected
       Backup Tunnel: Tu2        (label 0)
       Bkup Sender Template:
         Tun Sender: 10.0.0.0, LSP ID: 126
       Bkup FilerSpec:
         Tun Sender: 10.0.0.0, LSP ID 126
```

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。

（注） Fast Reroute には [フラグ（Flags）] フィールドが重要です。設定する必要があるフラグについては、表の [フラグ（Flags）] フィールドの説明を参照してください。

表 *167 : show ip rsvp sender detail* フィールドの説明：障害発生前の *PLR* 上

フィールド
ThefirstfivefieldsprovideinformationthatuniquelyidentifiestheLSP. **ThefirstthreefieldsidentifytheLSP'ssession(thatis,thecontentsoftheSESSIONobjectinarrivingPATHmessages).**
Tun Dest
Tun ID
Ext Tun ID
ThenexttwofieldsidentifytheLSP'ssender(SENDER_TEMPLATEobjectofarrivingPATHmessages).
Tun Sender
LSP ID
TheremainingfieldsindentedunderPATHprovideadditionalinformationaboutthisLSP.
SessionAttr：セッション属性。到着した PATH メッセージの SESSION_ATTRIBUTE オブジェクトに含まれている情報のことで、設定優先度、保持優先度、フラグ、セッション名などがあります。
Setup Prio
Holding Prio

フィールド
フラグ（Flags）
ERO：PATH メッセージの EXPLICIT_ROUTE オブジェクト（ERO）を参照します。このフィールドには、このノードにおける ERO の内容が表示されます。PATH メッセージが送信者（ヘッドエンド）から受信者（テールエンド）に移動すると、各ノードは ERO から自身の IP アドレスを削除します。表示された値は、このノードとテール間にあるホップの残りを反映しています。
Fast-RerouteBackupinfo：この LSP の Fast Reroute に関連する情報。
Inbound FRR

フィールド	
Outbound FRR	
Backup Tunnel	

フィールド
Bkup Sender Template

フィールド	
Bkup FilerSpec	

例 2：コマンドを障害発生後に PLR で入力する

LSP がバックアップ トンネルをアクティブに使用して始まり、コマンドを障害発生後に PLR で入力すると、表示が次の出力に示すように変わります。

```
Router# show ip rsvp sender detail
PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS1/0 from PHOP 10.1.1.1
   Path refreshes being sent to NHOP 10.2.2.1 on Tunnel2
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   ERO:
     10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
     10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Not active
```

```
  Outbound FRR: Active -- using backup tunnel
    Backup Tunnel: Tu2        (label 0)
    Bkup Sender Template:
      Tun Sender: 10.0.0.0, LSP ID: 126
    Bkup FilerSpec:
      Tun Sender: 10.0.0.0, LSP ID 126
    Orig Output I/F: Et2
    Orig Output ERO:
      10.1.1.4 (Strict IPv4 Prefix, 8 bytes, /32)
      10.1.1.5 (Strict IPv4 Prefix, 8 bytes, /32)
      10.1.1.6 (Strict IPv4 Prefix, 8 bytes, /32)
      10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
```

LSP がバックアップ トンネルをアクティブに使用すると、次の変更が行われます。

- PATH の更新が元のインターフェイスから元の NHOP に送信されなくなります。それらは、バックアップ トンネルを介して、バックアップ トンネルのテールであるノード（NHOP または NNHOP）に送信されます。
- ERO は、NHOP または NNHOP で到着時に受け入れられるように変更されます。
- 元の ERO と現在使用中の新しい ERO の両方が表示されます。
- 元の出力インターフェイス（つまり、障害発生前にこの LSP の PATH メッセージを送信したインターフェイス）が表示されます。

例 3：コマンドを障害発生前に MP で入力する

同じ **showiprsvpsender** コマンドをマージ ポイント（バックアップ トンネル テール）で入力すると、表示が障害発生の前から後に変わります。次に、障害発生前の出力例を示します。

```
Router# show ip rsvp sender detail
PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS0/0 from PHOP 10.1.1.5
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Not active
     Outbound FRR: No backup tunnel selected
```

例 4：コマンドを障害発生後に MP で入力する

障害発生後、次の変更が行われます。

- PATH メッセージの受信元のインターフェイスおよび前のホップ（PHOP）が変わります。
- 着信 FRR がアクティブになります。

- 元の PHOP と元の入力インターフェイスが次の出力に示すように表示されます。

次に、障害発生後の出力例を示します。

```
Router# show ip rsvp sender detail
PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS0/1 from PHOP 10.0.0.0 on Loopback0
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Active
       Orig Input I/F: POS0/0
       Orig PHOP: 10.1.1.5
       Now using Bkup Filterspec w/ sender: 10.0.0.0 LSP ID: 126
     Outbound FRR: No backup tunnel selected
```

次の変更に留意してください。

- 障害発生後、PATH の更新は別のインターフェイスに別の PHOP から到着します。
- 元の PHOP および入力インターフェイスは、Fast-Reroute Backup 情報の下に表示されます。また、FILTERSPEC オブジェクトも一緒に表示され、これはメッセージ（RESV や RESVTEAR など）を送信するときに使用されるようになります。

例 5：コマンド出力にすべての送信者が表示される

次の例では、すべての送信者に関する情報を表示しています。

```
Router# show ip rsvp sender
To              From            Pro DPort Sport Prev Hop        I/F  BPS  Bytes
10.2.2.1        10.2.2.0        1   1     59    10.1.1.1        Et1   0G     1K
10.2.2.1        172.31.255.255  1   2     9                           0G     1K
10.2.2.1        10.2.2.0        1   3     12    10.1.1.1        Et1   0G     1K
10.2.2.1        172.31.255.255  1   3     20                          0G     1K
172.16.0.0      172.31.255.255  1   0     23                          0G     1K
172.16.0.0      172.31.255.255  1   1     22                          0G     1K
172.16.0.0      172.31.255.255  1   1000  22                          0G     1K
```

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 *168 : show ip rsvp sender* フィールドの説明

フィールド	説明
To	受信者の IP アドレス。
From	送信元の IP アドレス。

フィールド	説明
Pro	プロトコル コード。コード 1 は、Internet Control Message Protocol（ICMP）を示します。
DPort	宛先ポート番号。
Sport	送信元ポート番号です。
Prev Hop	前のホップの IP アドレス。
I/F	前のホップのインターフェイス。
BPS	アドバタイズするアプリケーションが達成する可能性がある予約レート（1 秒あたりのビット数）。
Bytes	アドバタイズするアプリケーションが達成する可能性があるバースト サイズのバイト。

例 6：コマンド出力に特定の宛先を持つ送信者のみを表示する

特定の宛先を持つ送信者に関する情報のみを表示するには、次の出力に示すように宛先フィルタを指定します。この例では、宛先は 172.16.0.0 です。

```
Router# show ip rsvp sender filter destination 172.16.0.0
To          From         Pro DPort Sport Prev Hop    I/F  BPS  Bytes
172.16.0.0  172.31.255   1   0     23                     0G     1K
172.16.0.0  172.31.255   1   1     22                     0G     1K
172.16.0.0  172.31.255   1   1000  22                     0G     1K
```

例 7：特定の宛先を持つ送信者に関する詳細を表示する

宛先ポートが 1000 の送信者（例 6 を参照）に関する詳細を表示するには、宛先ポート フィルタとともにコマンドを指定します。

```
Router# show ip rsvp sender filter detail dst-port 1000
PATH:
  Tun Dest 172.16.0.0 Tun ID 1000 Ext Tun ID 172.31.255.255
  Tun Sender: 172.31.255.255, LSP ID: 22
  Path refreshes being sent to NHOP 10.1.1.4 on Ethernet2
  Session Attr::
    Setup Prio: 7, Holding Prio: 7
    Flags: SE Style
    Session Name:tagsw4500-25_t1000
  ERO:
    10.1.1.4 (Strict IPv4 Prefix, 8 bytes, /32)
    172.16.0.0 (Strict IPv4 Prefix, 8 bytes, /32)
  Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
  Fast-Reroute Backup info:
```

```
    Inbound  FRR: Not active
    Outbound FRR: No backup tunnel selected
```

VRF の例

次に、myvrf という名前の VRF に関連付けられたすべての送信者を表示する **showiprsvpsendervrfmyvrfdetail** コマンドの出力例を示します。

```
Router# show ip rsvp sender detail vrf myvrf
PATH:
  Destination 10.10.10.21, Protocol_Id 17, Don't Police , DstPort 1
  Sender address: 10.10.10.11, port: 1
  Path refreshes:
Traffic params - Rate: 10K bits/sec, Max. burst: 10K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 0F000406.
  Incoming policy: Accepted. Policy source(s): Default
  Status: Proxied
Output on Serial2/0. Policy status: Forwarding. Handle: 09000405
    Policy source(s): Default
  Path FLR: Never repaired
  VRF: myvrf
```

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 *169 : show ip rsvp sender detail* フィールドの説明：*VRF* あり

フィールド	説明
PATH	E2E 予約の PATH メッセージ情報： • 宛先の IP アドレス。 • プロトコルの ID 番号。 • ポリシング。 • 常に [ポリシングしない（Don't Police）] です。 • 宛先ポート番号。
Sender address	PATH メッセージの送信元 IP アドレス。 • [ポート（port）]：送信元ポートの番号。
Path refreshes	更新情報： • 送信元の IP アドレス（前のホップ [PHOP]）。 • インターフェイス名および番号 • 頻度（ミリ秒（ms））。 （注）　空白のフィールドは、更新が発生しなかったことを意味します。

フィールド	説明
Traffic params	有効なトラフィック パラメータ： • [レート（Rate）]：速度（キロビット/秒）。 • 集約予約の場合、常に [最大レート（MAX rate）] になる可能性があります。 • [最大バースト（Max. burst）]：許可されたデータの最大量（キロバイト）。 • 集約予約の場合、常に [最大バースト（MAX burst）] になる可能性があります。 • [最小ポリシング済みユニット（Min Policed Unit）]：IP レベル以上のアプリケーション データやすべてのプロトコル ヘッダーなど、アプリケーションによって生成された最も小さなパケットのサイズ（バイト）。 • [最大パケット サイズ（Max Pkt Size）]：許可されている最大パケット（バイト）。
PATH ID handle	記録を目的として RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Incoming policy	受信ポリシーの状態： • [承認済み（Accepted）]：RSVP PATH メッセージは承認中ですが、転送されていません。 • [未承認（Not Accepted）]：RSVP PATH メッセージは拒否されています。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Status	ローカル ポリシーのステータス： • [プロキシ済み（Proxied）]：ヘッド。 • [プロキシ終了（Proxy-terminated）]：テール。 • [遮断済み（Blockaded）]：テールまたはミッドポイントで、RESVERROR メッセージを最近受信したところです。このため、PSB は遮断済み状態になります。 （注）　空白のフィールドは上記のいずれでもないことを意味します。

フィールド	説明
Output on Serial2/0	ポリシー ステータス（発信インターフェイス上）： • [転送（Forwarding）]：着信 PATH メッセージを転送しています。 • [非転送（Not Forwarding）]：発信 PATH メッセージを拒否しています。 • [ハンドル（Handle）]：記録目的で RSVP によって PATH メッセージに割り当てられた内部データベース ID。
Policy source(s)	実行中のローカル ポリシーのタイプ。値は「Default」、「Local」、および「MPLS/TE」です。
Path FLR	[修復なし（Never repaired）]：ノードがローカル修復ポイント（PLR）になることはなく、このため、PSB を修復しなかったことを示します。
VRF	送信者が表示される VRF の名前。

MPLS トラフィック エンジニアリング ポイントツーマルチポイントの例

次に、ポイントツーマルチポイント情報が表示されている **showiprsvpsenderdetail** コマンドの出力例を示します。

```
Router# show ip rsvp sender detail

P2MP ID: 22  Tun ID: 22  Ext Tun ID: 10.1.1.201
  Tun Sender: 10.1.1.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
  SubGroup ID: 1
  S2L Destination : 10.1.1.203
  Path refreshes:
    sent:     to   NHOP 10.0.0.205 on Ethernet0/0
  Session Attr:
    Setup Prio: 7, Holding Prio: 7
    Flags: (0xF) Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
    Session Name: R201_t22
  ERO: (incoming)
    10.1.1.201 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.201 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.205 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.202 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.0.202 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.0.203 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.203 (Strict IPv4 Prefix, 8 bytes, /32)
  ERO: (outgoing)
    10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.205 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.202 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.0.202 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.0.203 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.203 (Strict IPv4 Prefix, 8 bytes, /32)
  Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
    Min Policed Unit: 1 bytes, Max Pkt Size 2147483647 bytes
  Fast-Reroute Backup info:
```

```
   Inbound  FRR: Not active
   Outbound FRR: Ready -- backup tunnel selected
     Backup Tunnel: Tu666      (label 20)
     Bkup Sender Template:
       Tun Sender: 10.0.2.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
       SubGroup ID: 1
     Bkup FilerSpec:
       Tun Sender: 10.0.2.201, LSP ID: 1, SubGroup Orig: 10.1.1.201
       SubGroup ID: 1
 Path ID handle: 01000414.
 Incoming policy: Accepted. Policy source(s): MPLS/TE
 Status: Proxied
 Output on Ethernet0/0. Policy status: Forwarding. Handle: 02000413
   Policy source(s): MPLS/TE
```

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 *170 : show ip rsvp sender--MPLS TE P2MP* フィールドの説明

フィールド	説明
P2MP ID	P2MP トンネルの宛先セットを指定する 32 ビットの番号。
Tun ID	トンネル ID 番号。
Ext Tun ID	拡張トンネル ID 番号。
Tun Sender	送信元の IP アドレス。
LSP ID	ラベル スイッチド パス ID 番号。
SubGroup Orig	LSP ヘッドエンド ルータ ID アドレス。
SubGroup ID	ヘッドエンド ルータからのシグナルを受ける各サブ LSP に割り当てられる増分番号。
S2L Destination	LSP テールエンド ルータ ID アドレス。

次に、ポイントツーマルチポイント トラフィックでの RSVP RESV 要求が表示されている **showiprsvpsenderfiltersession-type13** コマンドの出力例を示します。

```
Router# show ip rsvp sender filter session-type 13

Session Type 13 (te-p2mp-lsp)
Destination     Tun Sender      TunID LSPID P2MP-ID    SubID I/F      BPS
10.1.1.203       10.1.1.201       22    1     22         1     none     500K
10.1.1.206       10.1.1.201       22    1     22         2     none     500K
10.1.1.213       10.1.1.201       22    1     22         3     none     500K
10.1.1.214       10.1.1.201       22    1     22         4     none     500K
10.1.1.216       10.1.1.201       22    1     22         5     none     500K
10.1.1.217       10.1.1.201       22    1     22         6     none     500K
```

関連コマンド

コマンド	説明
iprsvpsender	ルータで送信者からの RSVP PATH メッセージの受信をシミュレートできるようにします。
showiprsvpreservation	現在データベースに格納されている RSVP PATH 関連の受信側情報を表示します。

show ip rsvp signalling

オプションでリソース予約プロトコル（RSVP）メッセージのレート制限パラメータおよび更新削減パラメータが含まれている RSVP シグナリング情報を表示するには、EXEC モードで **showiprsvpsignalling** コマンドを使用します。

show ip rsvp signalling [{**rate-limit**|**refresh reduction**}]

構文の説明

rate-limit	（任意）シグナリングメッセージのレート制限パラメータ。
refreshreduction	（任意）更新削減パラメータおよび設定。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.2(13)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

showiprsvpsignalling コマンドは、レート制限パラメータまたは更新削減パラメータを表示するためにそれぞれ **rate-limit** キーワードまたは **refreshreduction** を指定して使用します。

例

次のコマンドは、レート制限パラメータを表示します。

```
Router# show ip rsvp signalling rate-limit
Rate Limiting:enabled
  Max msgs per interval:4
  Interval length (msec):20
  Max queue size:500
  Max msgs per second:200
  Max msgs allowed to be sent:37
```

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。

表 *171 : show ip rsvp signalling rate-limit* コマンド フィールドの説明

フィールド	説明
Rate Limiting: enabled (active) or disabled (not active)	有効な RSVP レート制限パラメータ。次のものがあります。 • [間隔あたりの最大メッセージ（Max msgs per interval）]：送信が許可された 1 つの間隔（タイムフレーム）あたりのメッセージ数。 • [間隔の長さ（ミリ秒）（Interval length (msecs)）]：間隔（タイムフレーム）の長さ（ミリ秒）。 • [最大キューサイズ（Max queue size）]：メッセージ キューの最大サイズ（バイト）。 • [1 秒あたりの最大メッセージ（Max msgs per second）]：送信が許可された 1 秒あたりのメッセージの最大数。

次のコマンドは、更新削減パラメータを表示します。

```
Router# show ip rsvp signalling refresh reduction
Refresh Reduction:enabled
  ACK delay (msec):250
  Initial retransmit delay (msec):1000
  Local epoch:0x74D040
  Message IDs:in use 600, total allocated 3732, total freed 3132
```

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。

表 *172 : show ip rsvp signalling refresh reduction* コマンド フィールドの説明

フィールド	説明
Refresh Reduction: enabled (active) or disabled (not active)	有効な RSVP 更新削減パラメータ。次のものがあります。 • [ACK 遅延（ミリ秒）（ACK delay (msec)）]：受信側ルータが確認応答（ACK）を送信するまでの期間（ミリ秒）。 • [初期再送信遅延（ミリ秒）（Initial retransmit delay (msec)）]：送信側ルータがメッセージを再送信するまでの期間（ミリ秒）。 • [ローカル エポック（Local epoch）]：更新削減および信頼性の高いメッセージングのためのローカル ルータを定義する RSVP プロセス識別子。ノードが再起動するか、または RSVP プロセスが再実行されるたびにランダムに生成されます。 • [メッセージ ID（Message IDs）]：使用中のメッセージ識別子（ID）の数、割り当て済みの合計数、および使用可能な（解放された）合計数。

関連コマンド

コマンド	説明
clearipsvpsignallingrate-limit	削除したメッセージを記録するカウンタをクリアします。
clearipsvpsignallingrefreshreduction	再送信および順序が間違っていたメッセージを記録するカウンタをクリアします。
debugipsvprate-limit	RSVP レート制限イベントのデバッグ メッセージを表示します。
ipsvpsignallingrate-limit	指定の期間中に隣接ルータに送信される RSVP メッセージの伝送レートを制御します。
ipsvpsignallingrefreshreduction	リフレッシュ削減をイネーブルにします。

show ip rsvp signalling blockade

現在遮断されているリソース予約プロトコル（RSVP）セッションを表示するには、EXECモードで **showiprsvpsignallingblockade** コマンドを使用します。

show ip rsvp signalling blockade [detail] [{*nameaddress*}]

構文の説明

detail	（任意）追加の遮断情報。
name	（任意）遮断されているルータの名前。
address	（任意）予約の宛先の IP アドレス。

コマンド デフォルト

キーワードや引数なしで **showiprsvpsignallingblockade** コマンドを入力した場合は、ルータ上で遮断されたすべてのセッションが表示されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.2(13)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

show ip rsvp signalling blockade コマンドは、現在遮断されている RSVP セッションを表示する場合に使用します。

RSVP 送信者は、対応する受信者が Resv メッセージを送信して、RSVP が設定されているルータでアドミッション コントロールを失うと遮断されます。Resv メッセージへの返答としてアドミッション コントロール エラーのある ResvError メッセージが送信されると、この障害のダウンストリームに位置するすべてのルータは関連する送信者を遮断済みとしてマークします。その結果、遮断状態がタイムアウトするまで、それらのルータにはそのセッションにおける後続の Resv 更新へのコントリビューションが含まれません。

遮断は、共有予約に対するサービス妨害問題を解決します。この問題の場合、その予約を共有するすべての受信者にアドミッション コントロール障害を引き起こす目的で 1 人の受信者が大量の帯域幅をリクエストします。他の受信者が制限内にあるリクエストを行っているにもかかわらずです。

例

次の例は、現在遮断されているすべてのセッションを示しています。

```
Router# show ip rsvp signalling blockade
To              From            Pro DPort Sport Time Left Rate
192.168.101.2   192.168.101.1   UDP 1000  1000  27        5K
192.168.101.2   192.168.101.1   UDP 1001  1001  79        5K
192.168.101.2   192.168.101.1   UDP 1002  1002  17        5K
225.1.1.1       192.168.104.1   UDP 2222  2222  48        5K
```

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。

表 *173 : show ip rsvp signalling blockade* コマンド フィールドの説明

フィールド	説明
To	受信者の IP アドレス。
From	送信元の IP アドレス。
Pro	使用されるプロトコル。
DPort	宛先ポート番号。
Sport	送信元ポート番号です。
Time Left	遮断が期限切れになるまでの時間（秒）。
Rate	データの平均レート（1秒あたりのビット数）。

次の例は、現在遮断されているセッションに関する詳細を示しています。

```
Router# show ip rsvp signalling blockade detail
Session address: 192.168.101.2, port: 1000. Protocol: UDP
Sender address:  192.168.101.1, port: 1000
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:      5K bits/second
    Maximum burst:        5K bytes
    Peak bitrate:         5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:    5K bits/second
    Slack:                0 milliseconds
  Blockade ends in:       99 seconds
Session address: 192.168.101.2, port: 1001. Protocol: UDP
Sender address:  192.168.101.1, port: 1001
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:      5K bits/second
    Maximum burst:        5K bytes
    Peak bitrate:         5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:    5K bits/second
    Slack:                0 milliseconds
  Blockade ends in:       16 seconds
Session address: 192.168.101.2, port: 1002. Protocol: UDP
Sender address:  192.168.101.1, port: 1002
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:      5K bits/second
    Maximum burst:        5K bytes
    Peak bitrate:         5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:    5K bits/second
```

```
    Slack:                0 milliseconds
  Blockade ends in:       47 seconds
Session address: 225.1.1.1, port: 2222. Protocol: UDP
Sender address:  192.168.104.1, port: 2222
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:      5K bits/second
    Maximum burst:        5K bytes
    Peak bitrate:         5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:    5K bits/second
    Slack:                0 milliseconds
  Blockade ends in:       124 seconds
```

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。

表 *174 : show ip rsvp signalling blockade detail* コマンド フィールドの説明

フィールド	説明
Session address	遮断の影響を受ける予約の宛先 IP アドレス。
ポート	遮断の影響を受ける予約の宛先ポート番号。
Protocol	遮断の影響を受ける予約によって使用されるプロトコル。User Datagram Protocol（UDP）や TCP などがあります。
Sender address	遮断の影響を受ける予約の送信元 IP アドレス。
port	遮断の影響を受ける予約の送信元ポート番号。
Admission control error location	アドミッション コントロール エラーが発生したルータの IP アドレス。
Flowspec that caused blockade	遮断を引き起こした flowspec のパラメータ。
Average bitrate	flowspec の平均レート（1 秒あたりのビット数）。
Maximum burst	flowspec の最大バース サイズ（バイト単位）。
Peak bitrate	flowspec のピーク レート（bps）。
Minimum policed unit	flowspec の最小ポリシング済みユニット（バイト単位）。
Maximum packet size	flowspec の最大パケット サイズ（バイト単位）。
Requested bitrate	flowspec の要求レート（1 秒あたりのビット数）。
Slack	パケット配信をスケジュールするためにルータに割り当てられる時間（ミリ秒）。
Blockade ends in	遮断が期限切れになるまでの時間（秒）。

show ip rsvp signalling fast-local-repair

リソース予約プロトコル（RSVP）によって維持される fast-local-repair（FLR）固有の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 **showiprsvpsignallingfast-local-repair** コマンドを使用します。

show ip rsvp signalling fast-local-repair [**statistics** [**detail**]]

構文の説明

statistics	（任意）FLR 手順に関する情報を表示します。
detail	（任意）FLR 手順に関する追加情報を表示します。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。
15.0(1)M	このコマンドが変更されました。ローカル修復ポイント（PLR）で FLR がトリガーされた Virtual Routing and Forwarding（VRF）名を表示するように出力が変更されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

showiprsvpsignallingfast-local-repair コマンドは、設定されている FLR および RSVP メッセージ ペーシング レートを表示する場合に使用します。

showiprsvpsignallingfast-local-repairstatistics コマンドは、FLR 手順および次のような関連情報を表示する場合に使用します。

- プロセス番号
- 状態
- 開始時刻
- 修復したパス ステート ブロック（PSB）の数
- 修復レート
- ルーティング情報ベース（RIB）通知処理時間
- 最後の PSB の修復時間

showiprsvpsignallingfast-local-repairstatisticsdetail コマンドは、次のような FLR 手順に関する詳細な情報を表示する場合に使用します。

- ルーティング通知の時間
- キュー内のすべての通知を処理するための経過時間
- 使用したレートおよびペーシング単位（ミリ秒単位の更新間隔）
- 修復した PSB の数
- RSVP が中断した回数

実行ごとに次の情報が表示されます。

- プロシージャの先頭を基準にした実行の開始時間
- RSVP が再度中断した時間
- この実行で処理した通知の数

ネイバーごとに次の情報が表示されます。

- このネイバーに送信された最初の PATH メッセージの遅延
- このネイバーに送信された最後の PATH メッセージの遅延

例

show ip rsvp signalling fast-local-repair の例

次の例では、FLR レートに関する情報を表示しています。

```
Router# show ip rsvp signalling fast-local-repair
Fast Local Repair: enabled
   Max repair rate (paths/sec): 400
   Max processed   (paths/run): 1000
```

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 *175 : show ip rsvp signalling fast-local-repair* フィールドの説明

フィールド	説明
Fast Local Repair	FLR 状態。値は次のとおりです。 • [有効（enabled）] : FLR は設定されます。 • [無効（disabled）] : FLR は設定されません。
Max repair rate (paths/sec)	最大修復レート（1 秒あたりのパスの数）。
Max processed (paths/run)	処理する最大通知要素（1回の実行あたりのパス数）。

show ip rsvp signalling fast-local-repair statistics の例

次の例では、FLR 手順に関する情報を表示します。

```
Router# show ip rsvp signalling fast-local-repair statistics
Fast Local Repair: enabled
   Max repair rate (paths/sec): 1000
   Max processed   (paths/run): 1000
FLR Statistics:
  FLR   State    Start                          #PSB   Repair RIB Proc Last
  Proc.          Time                           Repair Rate   Time      PSB
  1     DONE     15:16:32 MET Wed Oct 25 2006   2496   1000   91(ms)    3111(ms)
```

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 *176 : show ip rsvp signalling fast-local-repair statistics* フィールドの説明

フィールド	説明
Fast Local Repair	FLR 状態。値は次のとおりです。 • [有効（enabled）] : FLR は設定されます。 • [無効（disabled）] : FLR は設定されません。
Max repair rate (paths/sec)	最大修復レート（1 秒あたりのパスの数）。
Max processed (paths/run)	処理する最大通知要素（1 回の実行あたりのパス数）。
FLR Statistics	FLR 関連情報。
FLR Proc.	FLR 手順番号。最後の 32 個のプロシージャが最新のものから順にリストされ、1 ～ 32 まで番号付けされます。
State	FLR 手順の現在の状態。値は次のとおりです。 • [完了（DONE）] : FLR 手順は完了しました。 • [処理中（IN PROGRESS）] : FLR 手順は完了していません。
Start Time	RSVP がルーティング通知を受信した時刻。
#PSB Repair	修復した PSB の数
Repair Rate	使用した修復レート（1 秒あたりのパスの数）。

フィールド	説明
RIB Proc Time	RSVP がすべての RIB 通知を処理し、パス更新をスケジュールするのに費やした時間（マイクロ秒（us）、ミリ秒（msec または ms）、または秒（sec））。 （注） この値は、列幅に合うように変換されます。ただし、秒はほとんど使用されません。RSVP RIB 通知処理が非常に高速であるためです。
Last PSB	FLR 手順が開始してから RSVP が最後の PATH メッセージを送信するまでの経過時間（マイクロ秒（us）、ミリ秒（msec または ms）、または秒（sec））。 （注） この値は、列幅に合うように変換されます。ただし、秒はほとんど使用されません。RSVP RIB 通知処理が非常に高速であるためです。

show ip rsvp signalling fast-local-repair statistics detail の例

次の例では、FLR 手順に関する詳細情報を表示します。

```
Router# show ip rsvp signalling fast-local-repair statistics detail
Fast Local Repair: enabled
   Max repair rate (paths/sec): 1000
   Max processed   (paths/run): 1000
FLR Statistics:
   FLR 1: DONE
     Start Time: 15:16:32 MET Wed Oct 25 2006
     Number of PSBs repaired:          2496
     Used Repair Rate (msgs/sec):      1000
     RIB notification processing time: 91(ms)
     Time of last PSB refresh:         3111(ms)
     Time of last Resv received:       4355(ms)
     Time of last Perr received:       0(us)
     Suspend count: 2
       Run  Number   Started              Duration
       ID   of ntf.  (time from Start)
       2    498      81(ms)               10(ms)
       1    998      49(ms)               21(ms)
       0    1000     0(us)                22(ms)
     FLR Pacing Unit: 1 msec
     Affected neighbors:
       Nbr Address     Interface    Relative Delay Values (msec) VRF
       10.1.2.12       Et0/3        [500  ,..., 5000  ]          vrf1
       10.1.2.12       Et1/3        [500  ,..., 5000  ]          vrf2
```

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 *177 : show ip rsvp signalling fast-local-repair statistics detail* フィールドの説明

フィールド	説明
Fast Local Repair	FLR 状態。値は次のとおりです。 • [有効（enabled）]：FLR は設定されます。 • [無効（disabled）]：FLR は設定されません。
Max repair rate (paths/sec)	最大修復レート（1 秒あたりのパスの数）。
Max processed (paths/run)	処理する最大通知要素（1 回の実行あたりのパス数）。
FLR Statistics	FLR 関連情報。
FLR 1	FLR 手順番号と現在の状態。最後の 32 個のプロシージャが最新のものから順にリストされ、1 ～ 32 まで番号付けされます。状態の値は次のとおりです。 • [完了（DONE）]：FLR 手順は完了しました。 • [処理中（IN PROGRESS）]：FLR 手順は完了していません。
Start Time	RSVP がルーティング通知を受信した時刻。
Number of PSBs repaired	修復した PSB の合計数。
Used Repair Rate (msgs/sec)	使用した修復レート（1 秒あたりのメッセージ数）。
RIB notification processing time	RSVP がすべての RIB 通知を処理するのに費やした時間（ミリ秒（ms））。
Time of last PSB refresh	FLR 手順が開始してから RSVP が最後の PATH 更新メッセージを送信するまでの経過時間（ミリ秒（ms））。
Time of last Resv received	FLR 手順が開始してから RSVP が最後の RESV メッセージを受信するまでの経過時間（ミリ秒（ms））。
Time of last Perr received	FLR 手順が開始してから RSVP が最後の PATHERROR メッセージを受信するまでの経過時間（マイクロ秒（us））。
Suspend count	特定のプロシージャ中に RSVP が中断した回数。 （注） この値がゼロ以外の場合、実行ごとに詳細が表示されます。
Run ID	RSVP による各実行の識別子（番号）。
Number of ntf.	実行で処理された通知の数（PSB）。

フィールド	説明
Started (time from Start)	FLR手順の先頭を基準にした実行の開始時間（ミリ秒（ms））。
Duration	実行の時間の長さ（ミリ秒（ms））。
FLR ペーシング単位（FLR Pacing Unit）	RSVP メッセージ ペーシングの頻度（ミリ秒（msec））。つまり、PATH メッセージが送信される頻度です。値は切り捨てられます。
Affected neighbors	FLR 手順に関与するネイバー。
Nbr Address	プロシージャに関与する各ネイバーの IP アドレス。
Interface	ネイバーのインターフェイス。
Relative Delay Values	PSB 更新が送信された時間（ミリ秒（msec））。 （注） サンプルの表示では、1 ミリ秒のペーシング単位があります。このため、10.1.2.12 に対する PSB は 500、501、502、503、... 2995 から 1 ミリ秒の遅延で送信されました。5 ミリ秒のペーシング単位が使用された場合、遅延は 500、505、510、... 2990、2995 になります。
VRF	PLR で FLR をトリガーした VRF 名。

関連コマンド

コマンド	説明
iprsvpsignallingfast-local-repairnotifications	RSVP が一時停止する前に処理される通知の数を設定します。
iprsvpsignallingfast-local-repairrate	FLR 手順のために RSVP で使用される修復を設定します。
iprsvpsignallingfast-local-repairwait	FLR プロシージャの開始に使用される遅延を設定します。
iprsvpsignallingrate-limit	指定の期間中に隣接ルータに送信されるRSVPメッセージの伝送レートを制御します。

show ip rsvp signalling rate-limit

リソース予約プロトコル（RSVP）レート制限パラメ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 **showiprsvpsignallingrate-limit** コマンドを使用します。

show ip rsvp signalling rate-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 モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。
12.0(24)S	このコマンドが、Cisco IOS Release 12.0(24)S に統合されました。
12.0(29)S	コマンド出力は、改訂されたレート制限パラメータを表示するように変更されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(18)SXF5	このコマンドが、Cisco IOS Release 12.2(18)SXF5 に統合されました。
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。
Cisco IOS XE リリース 2.3	このコマンドが、Cisco IOS XE Release 2.3 に統合されました。

例

次のコマンドは、レート制限パラメータを表示します。

```
Router# show ip rsvp signalling rate-limit
Rate Limiting:
  Burst: 1
  Limit: 20
  Maxsize: 500
  Period <msec>: 5
  Max rate <msgs/sec>: 2
```

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。

表 *178 : show ip rsvp signalling rate-limit* フィールドの説明

フィールド	説明
Rate Limiting	RSVP レート制限パラメータを有効または無効にします。使用できるキーワードには次のものがあります。 • [バースト（Burst）]：各期間にキューから送信されたメッセージの数。 • [制限（Limit）]：各期間にキューから送信されたメッセージの最大数。 • [最大サイズ（Maxsize）]：メッセージ キューの最大サイズ（バイト）。 • [期間（ミリ秒）（Period (msec)）]：ミリ秒単位の間隔（時間内） • [最大レート（メッセージ/秒）（Max rate (msgs/sec)）]：送信が許可された 1 秒あたりのメッセージの最大数。

関連コマンド

コマンド	説明
clearipsvpsignallingrate-limit	最大キューのためにドロップされたメッセージの数をクリア（ゼロに設定）します。
debugiprsvprate-limit	RSVP レート制限イベントのデバッグ メッセージを表示します。
iprsvpsignallingrate-limit	指定の期間中に隣接ルータに送信される RSVP メッセージの伝送レートを制御します。

show ip rsvp signalling refresh

リソース予約プロトコル（RSVP）メッセージの RSVP シグナリング更新動作パラメ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 **showiprsvpsignallingrefresh** コマンドを使用します。

show ip rsvp signalling refresh {**interval**|**misses**|**reduction**}

構文の説明

interval	定常の更新メッセージ間の時間間隔を指定します。
misses	トリガー状態のタイムアウト時に受信しない更新の数を指定します。
reduction	RSVP 更新削減パラメータおよび設定を指定します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。
12.2(24)T	**interval** キーワードおよび **misses** キーワードが追加されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。

使用上のガイドライン

showiprsvpsignallingrefresh コマンドは、更新動作パラメータを表示する場合に使用します。

例

次の例は、更新間隔パラメータを示しています。

```
Router# show ip rsvp signalling refresh interval

Refresh interval (msec): 30000
```

次の例は、更新ミス パラメータを示しています。

```
Router# show ip rsvp signalling refresh misses
Refresh misses: 4
```

次の例は、更新削減パラメータを示しています。

```
Router# show ip rsvp signalling refresh reduction
Refresh Reduction: disabled
  ACK delay (msec): 250
  Initial retransmit delay (msec): 1000
```

```
Local epoch: 0x6975F6
Message IDs: in use 0, total allocated 0, total freed 0
```

関連コマンド

コマンド	説明
clearipsvpsignallingrate-limit	削除したメッセージを記録するカウンタをクリアします。
debugipsvprate-limit	RSVP レート制限イベントのデバッグ メッセージを表示します。
ipsvpsignallingrate-limit	指定の期間中に隣接ルータに送信される RSVP メッセージの伝送レートを制御します。

show ip rsvp snooping

リソース予約プロトコル（RSVP）スヌーピングが有効になっている VLAN のリストを表示するには、特権 EXEC モードで **show ip rsvp snooping** コマンドを使用します。

show ip rsvp snooping

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(44)SE	このコマンドが導入されました。

使用上のガイドライン

ip rsvp snooping コマンドを使用すると、必要な VLAN で RSVP スヌーピングを有効にできます。**show ip rsvp snooping** コマンドでは、いくつの VLAN で RSVP スヌーピングが有効になっているかを表示できます。VLAN詳細はオプションで、VLANごとのスヌーピングをサポートするプラットフォームでのみ表示できます。VLAN 詳細を **ip rsvp snooping** コマンドに指定しないと、スヌーピングはすべての VLAN で有効になり、**show ip rsvp snooping** コマンドは同じことを示します。

例

次の出力例には、RSVP スヌーピングが有効になっている VLAN のリストが表示されています。

```
Device# show ip rsvp snooping

*May 29 09:06:27.597: %SYS-5-CONFIG_I: Configured from console by consoleoping

RSVP Snooping is enabled on this Vlans
----------------------------------------
VLan 70         VLan 71         VLan 72
VLan 73         VLan 74
----------------------------------------
```

次の出力例は、RSVP スヌーピングがすべての VLAN で有効になっていることを示しています。

```
Device# show ip rsvp snooping

RSVP snooping is enabled globally.
```

関連コマンド

コマンド	説明
ip rsvp snooping	VLANの特定のセットでRSVPスヌーピングを有効にします。

show ip rsvp tos

リソース予約プロトコル（RSVP）インターフェイスに関する IP タイプ オブ サービス（ToS）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 **showiprsvptos** コマンドを使用します。

show ip rsvp tos [**type number**]

構文の説明

type	（任意）インターフェイスのタイプです。
number	（オプション）インターフェイスの番号。

コマンド モード

ユーザ EXEC モード（>）
特権 EXEC モード（#）

コマンド履歴

リリース	変更箇所
15.0(1)M	このコマンドが導入されました。

使用上のガイドライン

RSVP を使用するように設定された特定のインターフェイスに関する IP ToS 情報を取得するには、show ip rsvp tos コマンドでインターフェイス名を指定します。ルータ上の RSVP に対応したすべてのインターフェイスに関する IP ToS 情報を取得するには、インターフェイス名を指定せずに ip rsvp tos コマンドを使用します。

例

次の例は、RSVP が有効になっているインターフェイスの IP ToS 情報を示しています。

```
Router# show ip rsvp tos ethernet 0/1
Interface name   Precedence  Precedence   TOS          TOS
                   conform    exceed     conform     exceed
Ethernet0/0          -          -          -           -
Ethernet0/1          -          -          -           -
Ethernet1/1          -          -          4           -
Ethernet1/2          3          -          -           -
```

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。

表 *179 : show ip rsvp tos* フィールドの説明

フィールド	説明
Interface name	インターフェイスの詳細を表示します。

フィールド	説明
Precedence conform	インターフェイスでのIPプレシデンスの準拠に関する情報を表示します。 （注） 「Precedence conform」の値は、RSVP Flowspec に準拠するトラフィックに対し、0から7までの範囲のIPプレシデンス値を指定します。
Precedence exceed	インターフェイスでのIPプレシデンスの超過に関する情報を表示します。 （注） 「Precedence exceed」の値は、RSVP Flowspec を超過するトラフィックに対し、0から7までの範囲のIPプレシデンス値を指定します。
TOS conform	インターフェイスでの IP タイプ オブ サービス（ToS）の準拠に関する情報を表示します。 （注） 「TOS conform」の値は、RSVP Flowspec に準拠するトラフィックに対し、0 から 31 までの範囲の ToS 値を指定します。
TOS exceed	インターフェイスでの IP タイプ オブ サービス（ToS）の超過に関する情報を表示します。 （注） 「TOS exceed」の値は、RSVP Flowspec を超過するトラフィックに対し、0 から 31 までの範囲の ToS 値を指定します。

関連コマンド

コマンド	説明
show ip rsvp	RSVP 関連情報を表示します。
showiprsvpinterface	RSVP 関連のインターフェイス情報を表示します。
showiprsvpprecedence	RSVP対応インターフェイスのIPプレシデンス情報を表示します。

show ip rsvp transport

リソース予約プロトコル（RSVP）トランスポートプロトコル（TP）セッション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 **showiprsvptransport** コマンドを使用します。

show ip rsvp transport {**clients**|**statistics**}

構文の説明

clients	TPセッションを開始したRSVPクライアントに関する情報を表示します。
statistics	RSVP TP セッションの統計を表示します。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.1(3)T	このコマンドが導入されました。
15.1(1)S	このコマンドが、Cisco IOS Release 15.1(1)S に統合されました。

例

次は、**showiprsvptransportstatistics** コマンドの出力例です。

```
Router# show ip rsvp transport statistics
RSVP Transport Statistics:
 Transport Statistics: 2
  Start Time: 05:57:42 IST Thu Nov 5 2009
  Destination: 10.1.1.2, Protocol_Id: 6, DstPort: 22
  Client_id: 1, Initiator_Id: 10.1.1.1
  Source: 10.1.1.1, SrcPort: 11, Instance_Id: 9999
 Outgoing interface: Ethernet1/0
  Event type: RSVP_TP_EVENT_SESSION_DOWN
 Transport Statistics: 1
  Start Time: 05:57:16 IST Thu Nov 5 2009
  Destination: 10.1.1.2, Protocol_Id: 6, DstPort: 22
  Client_id: 1, Initiator_Id: 10.1.1.1
  Source: 10.1.1.1, SrcPort: 11, Instance_Id: 9999
  Incoming interface: Ethernet0/0
  TP data: example1
  Event type: RSVP_TP_EVENT_MSG_RCVD
  Received message type: Path
```

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 *180 : show ip rsvp transport statistics* フィールドの説明

フィールド	説明
Transport Statistics	RSVP TP 統計に関する情報を保存するために使用するバッファ サイズ（メガバイト（MB））を表示します。
Start Time	ルータが RSVP 統計の記録を開始したときからの時間を表示します。
Destination	PATH メッセージが送信される宛先アドレスです。
Protocol_Id	RSVP をトランスポート プロトコルとして設定するために使用される識別子。
DstPort	PATH メッセージが送信される宛先ポートです。
Client_id	トランスポートプロトコルとしてRSVPを開始したクライアントの識別番号。
Initiator_Id	トランスポート サービス要求を開始するノードを識別するホスト名または IP アドレスです。
Source	PATH メッセージの送信元となる発信元アドレスです。
SrcPort	PATH メッセージの送信元となる送信元ポートです。
Instance_Id	特定のクライアントアプリケーションと特定のイニシエータからのトランスポート サービス要求を識別するインスタンス ID です。
Incoming interface	PATH メッセージの送信元であるインターフェイスのタイプと番号。
TP data	トランスポート プロトコル データ。
Event type	発生したイベントのタイプ。
Received message type	送信されるメッセージのタイプ。

次の例は、RSVP クライアント ID およびクライアント タイプ情報を表示する方法を示しています。

```
Router# show ip rsvp transport clients
Client-ID  Type
1           CLI
```

関連コマンド

コマンド	説明
showiprsvptransportsender-host	RSVP PATH 状態情報を表示します。

show ip rsvp transport sender

リソース予約プロトコル（RSVP）PATH 状態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 **showiprsvptransportsender** コマンドを使用します。

show ip rsvp transport sender [**vrf** {******vrf-name*}] **[detail]** [**filter** [{**destination** *dest-address*|**dst-port** *dst-port*|**source** *source-addr*|**src-port** *src-port*}]]

構文の説明

vrf	（任意）VPN ルーティングおよび転送（VRF）詳細を指定します。
*****	（任意）すべての VRF およびグローバル ルーティング ドメインの RSVP PATH 状態情報を表示します。
vrf-name	（任意）VRF 名です。
detail	（任意）PATH 状態情報の詳しい説明を表示します。
filter	（任意）表示をフィルタして、出力を制限します。
destination	（任意）表示をフィルタして、宛先に関連する情報を表示します。
dest-address	（任意）宛先を指定する IP アドレス。
dst-port	（任意）表示をフィルタして、宛先ポートに関連する情報を表示します。
dst-port	宛先ポートまたはトンネル ID。指定できる範囲は 0 ～ 65535 です。
source	（任意）表示をフィルタして、送信元に関連する情報を表示します。
source-addr	（任意）送信元を指定する IP アドレス。
src-port	（任意）表示をフィルタして、送信元ポートに関連する情報を表示します。
src-port	（任意）宛先ポートまたはリンクステート パケット（LSP）ID。指定できる範囲は 0 ～ 65535 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	変更箇所
15.1(3)T	このコマンドが導入されました。
15.1(1)S	このコマンドが、Cisco IOS Release 15.1(1)S に統合されました。

使用上のガイドライン

showiprsvptransport コマンドを使用すると、トランスポート プロトコルとして設定された RSVP に関連する情報を表示できます。

例

次の例は、送信者から受信者に送信される PATH メッセージに関する情報を表示する方法を示しています。

```
Router# show ip rsvp transport sender
To              From            Pro DPort Sport Prev Hop        I/F
10.1.1.1        10.2.2.2        TCP 101   101   none            none
```

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 *181 : show ip rsvp transport sender* フィールドの説明

フィールド	説明
To	受信者の IP アドレス。
From	送信者またはクライアントの IP アドレス。
Pro	RSVP をトランスポート プロトコルとして設定するために使用される識別子。
DPort	PATH メッセージが送信される宛先ポートです。
Sport	PATH メッセージの送信元となる送信元ポートです。
Prev Hop	送信者から受信者に PATH メッセージを転送するために使用されるホップ アドレス。

次の例は、RSVP メッセージに関する詳細情報を表示する方法を示しています。

```
Router# show ip rsvp transport sender detail
Transport PATH:
  Destination 10.1.1.1, Protocol_Id 6,  DstPort 101
  Sender address: 10.2.2.2, port: 101
  Path refreshes:
     Path ID handle: 01000402.
  Client_id: 251
   Initiator_id: 10.2.2.2
   Instance_id: 3421
```

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 *182 : show ip rsvp transport sender detail* フィールドの説明

フィールド	説明
Transport PATH:	PATH メッセージを送信するために取得されたトランスポート パスに関連する情報を表示します。
Destination	PATH メッセージが送信される宛先アドレスです。
Protocol_Id	RSVP をトランスポートプロトコルとして設定するために使用される識別子。
DstPort	PATH メッセージが送信される宛先ポートです。

フィールド	説明
Sender address	PATH メッセージの送信元となる発信元アドレスです。
port	PATH メッセージの送信元となる送信元ポートです。
Path refreshes	PATH メッセージおよび Resv メッセージの定期更新に関する情報を表示します。
Path ID handle	PATH メッセージおよび Resv メッセージが更新された回数を表示します。
Client ID	トランスポート プロトコルとして RSVP を開始したクライアントの識別番号。
Initiator_id	トランスポートサービス要求を開始するノードを識別するホスト名またはIPアドレスです。
Instance_id	特定のクライアントアプリケーションと特定のイニシエータからのトランスポート サービス要求を識別するインスタンス ID です。

関連コマンド

コマンド	説明
iprsvptransport	RSVPをトランスポートプロトコルとして設定します。
iprsvptransportsender-host	静的な RSVP ホスト パスを設定します。
showiprsvptransport	RSVP TP セッションに関する情報を表示します。

show ip rtp header-compression

Real-Time Transport Protocol（RTP）統計を表示するには、特権 EXEC モードで **showiprtpheader-compression** コマンドを使用します。

show ip rtp header-compression [*interface-type interface-number*] **[detail]**

構文の説明

interface-type interface-number	（任意）インターフェイス タイプおよび番号
detail	（任意）各接続の詳細を表示します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
11.3	このコマンドが導入されました。
12.1(5)T	Distributed Compressed Real-Time Transport Protocol（dCRTP）機能に関する情報が含まれるように、このコマンドが変更されました。
12.3(11)T	Enhanced Compressed Real-Time Transport Protocol（ECRTP）機能に関する情報が含まれるように、このコマンド出力が変更されました。
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

Route Switch Processor（RSP）上では、**showiprtpheader-compression** コマンドに **detail** キーワードを使用できません。ただし、Versatile Interface Processor（VIP）上では、show ip rtp header-compression コマンドに **detail** キーワードを使用できます。VIP 上で show ip rtp header-compression interface-type interface-number detail コマンドを入力すると、特定インターフェイスの RTP ヘッダー圧縮に関する詳細情報が得られます。

例

次の例では、インターフェイス上の ECRTP からの統計を表示しています。

```
Router# show ip rtp header-compression

RTP/UDP/IP header compression statistics:
  Interface Serial2/0 (compression on, IETF, ECRTP)
    Rcvd:    1473 total, 1452 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
```

```
Sent:     1234 total, 1216 compressed, 0 status msgs, 379 not predicted
          41995 bytes saved, 24755 bytes sent
          2.69 efficiency improvement factor
Connect: 16 rx slots, 16 tx slots,
          6 misses, 0 collisions, 0 negative cache hits, 13 free contexts
          99% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

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 *183 : show ip rtp header-compression* 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タイプと番号。
Rcvd	後続のフィールドに記載されている、受信統計情報
total	インターフェイスの受信パケット数。
compressed	圧縮されたヘッダーを持つ受信パケット数。
errors	エラー数。
status msgs	ピアから受信した再同期メッセージの数
dropped	ドロップされたパケットの数
buffer copies	コピーされたバッファの数。
buffer failures	バッファの割り当てに失敗した回数。
Sent	後続のフィールドに記載されている、送信統計情報
total	インターフェイスの送信パケット数。
compressed	圧縮されたヘッダーを持つ送信パケット数
status msgs	ピアから送信された再同期メッセージの数
not predicted	コンプレッサへ最適な経路を使用しなかったパケット数
bytes saved	圧縮によって得られた合計削減数（バイト）
bytes sent	圧縮後に送信された合計バイト数
efficiency improvement factor	圧縮効率。
Connect	後続のフィールドに記載されている接続統計情報。
rx slots	受信されたスロットの合計数。
tx slots	送信されたスロットの合計数。

フィールド	説明
misses	ミスの合計数。
collisions	衝突数
negative cache hits	ネガティブ キャッシュの合計ヒット数
free contexts	使用可能なコンテキスト リソースの数。
hit ratio	コンテキストが関連付けられている受信パケットの割合。
five minute miss rate	1秒あたりに検出された新規フローの数（過去5分間の平均）。
max	報告された新規フローの最大平均レート。

関連コマンド

コマンド	説明
iprtpcompression-connections	インターフェイス上でサポートされる RTP ヘッダー圧縮接続の総数を指定します。
iprtpheader-compression	RTP ヘッダー圧縮をイネーブルにします。

show ip tcp header-compression

TCP/IP ヘッダー圧縮統計を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showiptcpheader-compression** コマンドを使用します。

show ip tcp header-compression [*interface-type interface-number*] **[detail]**

構文の説明

interface-type interface-number	（任意）インターフェイス タイプおよび番号
detail	（任意）各接続の詳細を表示します。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。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
12.4	このコマンドが Cisco Release 12.4 に統合され、その他の圧縮統計情報がコマンド出力に含まれるように変更されました。
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。
12.4(15)T12	このコマンドが変更されました。特別な Van Jacobson（VJ）フォーマットの TCP ヘッダー圧縮のサポートが追加されました。

例

次は、**showiptcpheader-compression** コマンドの出力例です。

```
Router# show ip tcp header-compression

TCP/IP header compression statistics:
  Interface Serial2/0 (compression on, IETF)
    Rcvd:    53797 total, 53796 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    53797 total, 53796 compressed, 0 status msgs, 0 not predicted
             1721848 bytes saved, 430032 bytes sent
             5.00 efficiency improvement factor
    Connect: 16 rx slots, 16 tx slots,
             1 misses, 0 collisions, 0 negative cache hits, 15 free contexts
             99% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

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 *184 : show ip tcp header-compression* のフィールドの説明

フィールド	説明
Interface Serial2/0 (compression on, IETF)	圧縮がイネーブルであるインターフェイスのタイプおよび番号
Rcvd:	後続のフィールドに記載されている、受信統計情報
total	インターフェイスで受信された TCP パケットの合計数
compressed	圧縮された TCP パケットの合計数
errors	エラー状態で受信されたパケットの数
status msgs	ピアから受信した再同期メッセージの数
dropped	無効な圧縮のためにドロップされたパケット数
buffer copies	圧縮解除のために、より大きいバッファにコピーする必要があるパケットの数
buffer failures	バッファの不足のためにドロップされたパケット数
Sent:	後続のフィールドに記載されている、送信統計情報
total	インターフェイスで送信された TCP パケットの合計数
compressed	圧縮された TCP パケットの合計数
status msgs	ピアから送信された再同期メッセージの数
not predicted	コンプレッサへ最適な経路を使用しなかったパケット数
bytes saved	圧縮によって得られた合計削減数（バイト）
bytes sent	圧縮後に送信された合計バイト数
efficiency improvement factor	TCP ヘッダー圧縮による回線効率の改善。圧縮パケット バイト数に対する総パケット バイト数の比率で表されます。この比率は、1.00 を超えている必要があります。
Connect:	後続のフィールドに記載されている、接続統計情報
rx slots	受信されたスロットの合計数。
tx slots	送信されたスロットの合計数。
misses	一致しなかった回数を示します。出力の喪失比率が大きい場合は、認められる同時圧縮接続の数は、非常に小さくなります。
collisions	衝突数

フィールド	説明
negative cache hits	ネガティブ キャッシュの合計ヒット数 （注） このフィールドは、TCP ヘッダー圧縮とは関係ありません。Real-Time Transport Protocol（RTP）ヘッダー圧縮に使用されます。
free contexts	フリー コンテキストの合計数 （注） フリーコンテキスト（接続とも呼ばれる）は、TCPヘッダー圧縮に現在使用されておらず、使用可能なリソースの数を示します。
hit ratio	ソフトウェアが一致を発見し、ヘッダーを圧縮できた回数の割合。
Five minute miss rate 0 misses/sec	長期的な喪失比率の傾向を（より正確に）観察するために、最近 5 分間の喪失比率を計算します。
max	前のフィールドの最大値

Cisco IOS リリース 12.4（15）T12 の次の例は、TCP の特別な VJ フォーマットが有効になっていることを示しています。

```
Router# show ip tcp header-compression serial 5/0 detail

TCP/IP header compression statistics:
 DLCI 100        Link/Destination info: ip 10.72.72.2
Configured:
 Max Header 60 Bytes, Max Time 50 Secs, Max Period 32786 Packets, Feedback On, Spl-VJ
On
Negotiated:
 Max Header 60 Bytes, Max Time 50 Secs, Max Period 32786 Packets, Feedback On, Spl-VJ
On
TX contexts:
```

関連コマンド

Command	Description
ipheader-compressionspecial-vj	特別な VJ フォーマットの TCP ヘッダー圧縮を有効にします。
iptcpcompression-connections	インターフェイス上に存在できる TCP ヘッダー圧縮接続数の合計数を指定します。
special-vj	コンテキスト ID が圧縮パケットに含まれるように、特別な VJ フォーマットの TCP ヘッダー圧縮を有効にします。

show ip vrf

定義済みのバーチャル 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）インスタンスおよび関連するインターフェイスのセットを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipvrf** コマンドを使用します。

show ip vrf [{**brief**|**detail**|**interfaces**|**id**}] [*vrf-name*]

構文の説明

brief	（任意）VRF および関連するインターフェイスの簡潔な情報を表示します。
detail	（任意）VRF および関連するインターフェイスの詳細な情報を表示します。
interfaces	（任意）特定の VRF または任意の VRF にバインドされたすべてのインターフェイスに関する詳細な情報を表示します。
id	（任意）さまざまな VPN の PE ルータに設定されている VPN ID を表示します。
vrf-name	（任意）VRF に割り当てられた名前。

コマンド デフォルト

キーワードや引数を指定しないと、このコマンドは設定されたすべての VRF に関する簡潔な情報を表示します。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(17)ST	このコマンドが変更されました。id キーワードが追加されました。VPN ID 情報が show ip vrf detail コマンドの出力に追加されました。
12.2(4)B	このコマンドが Cisco IOS Release 12.2(4)B に組み込まれました。
12.2(8)T	このコマンドが Cisco IOS Release 12.2(8)T に統合されました。
12.3(6)	このコマンドが Cisco IOS Release 12.3(6) に統合されました。このコマンドは、関連する仮想アクセス インターフェイス（VAI）ごとにダウンストリーム VRF を表示します。
12.2(27)SBC	このコマンドが、Cisco IOS Release 12.2(27)SBC に統合されました。
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。

使用上のガイドライン

VRF 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。2 つの詳細レベルを使用できます。

- **brief** キーワード（またはキーワードなし）は、簡潔な情報を表示します。
- **detail** キーワードは、すべての情報を表示します。

特定の VRF または任意の VRF にバインドされたすべてのインターフェイスに関する情報を表示するには、interfaces キーワードを使用します。PE ルータに割り当てられた VPN ID に関する情報を表示するには、id キーワードを使用します。

showipvrf コマンドを使用すると、その出力ではインターフェイス名およびサブインターフェイス名が切り捨てられます。たとえば、GigabitEthernet3/1/0.100 は Gi3/1/0.100 として表示されます。

例

Cisco IOS T Train、Cisco IOS SB Train、Cisco IOS B Train、および Cisco IOS SX Train

次の例では、関連する VAI ごとにダウンストリーム VRF など、ルータに設定されたすべての VRF に関する情報を表示しています。ハイライトされている行（ドキュメントで参照する目的のみ）は、ダウンストリーム VRF を示します。

```
Router# show ip vrf
  Name                              Default RD          Interfaces
  v1                                20:20               Gi0/2.4294967291
                                                        Gi0/2.4294967293
                                                        Gi0/2.4294967294
                                                        Gi0/2.4294967295
  vpn152-1                          152:1               Lo1
```

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 *185 : show ip vrf* フィールドの説明

フィールド	説明
Name	VRF 名を指定します。
Default RD	デフォルトのルート識別子を指定します。
Interfaces	ネットワーク インターフェイスを指定します。

次の例では、各 VRF に関連付けられたすべての VAI など、ルータに設定されたすべての VRF に関する詳細な情報を表示しています。

```
Router# show ip vrf detail vpn152-1
VRF vpn152-1; default RD 152:1; default VPNID <not set>
VRF Table ID = 2
  Interfaces:
    Lo1
  Connected addresses are not in global routing table
  Export VPN route-target communities
```

```
  RT:152:1
Import VPN route-target communities
  RT:152:1
No import route-map
No export route-map
VRF label distribution protocol: not configured
```

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 *186 : show ip vrf detail* フィールドの説明

フィールド	説明
default VPNID	ネットワーク内のすべての VPN を一意に識別する VPN ID を指定します。
VRF Table ID	VRF ルーティング テーブルを一意に識別します。
Interfaces	ネットワーク インターフェイスを指定します。
Export VPN route-target communities	VPN ルート ターゲット エクスポート コミュニティを指定します。
Import VPN route-target communities	VPN ルートターゲットインポートコミュニティを指定します。
VRF Label Distribution Protocol	VRF コンテキストでの MPLS Label Distribution Protocol。これは、VRF が Carrier Supporting Carrier（CSC）用に設定されている場合に必要です。これは、LDP（VRF インターフェイスに対する **mplsip** コマンドで有効にします）または BGP（ルータ bgp VRF アドレス ファミリ コンフィギュレーション モードの **send-label** コマンドで有効にします）にすることができます。

次の例は、特定の VRF にバインドされたインターフェイスを示しています。

```
Router# show ip vrf interfaces
Interface              IP-Address      VRF                              Protocol
Gi0/2.4294967291       unassigned      v1                               down
Gi0/2.4294967293       unassigned      v1                               down
Gi0/2.4294967294       unassigned      v1                               down
Gi0/2.4294967295       unassigned      v1                               down
Lo1                    10.1.1.1        vpn152-1                         up
```

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 *187 : show ip vrf interfaces* のフィールドの説明

フィールド	説明
Interface	VRF のネットワーク インターフェイスを指定します。
IP-Address	VRF インターフェイスの IP アドレスを指定します。

フィールド	説明
VRF	VRF 名を指定します。
Protocol	VRF インターフェイスごとにプロトコルの状態（稼働または停止）を表示します。

Cisco IOS SR Train

次の例では、**detail** キーワードを指定した **showipvrf** コマンドからの出力を表示しています。表示される情報は vpn1 という名前の VRF のものです。

```
Router# show ip vrf detail vpn1
VRF vpn1 (VRF Id = 1); default RD 1:1; default VPNID <not set>
 Interfaces:
 Lo1                       Lo99                      Et0/0
VRF Table ID = 1
 Export VPN route-target communities
 RT:1:1
 Import VPN route-target communities
  RT:1:1                    RT:2:1
No import route-map
No export route-map
 VRF label distribution protocol: not configured
 VRF label allocation mode: per-prefix
```

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 *188 : show ip vrf detail* フィールドの説明

フィールド	説明
VRF ID	ルータ内の VRF を一意に識別します。
VRF ラベル割り当てモード（VRF label allocation mode）	ルート タイプに基づいて使用されるラベル モードのタイプを示します。

関連コマンド

Command	Description
importmap	VRF のインポート ルート マップを作成します。
ipvrf	VRF ルーティング テーブルを設定します。
ipvrfforwarding(interfaceconfiguration)	VRF をインターフェイスまたはサブインターフェイスと関連付けます。
rd	VRF のルーティング テーブルと転送テーブルを作成します。
route-target	VRF 用にルート ターゲット拡張コミュニティを作成します。

Command	Description
vpnid	VRF に VPN ID を割り当てます。

show lane qos database

（注） Cisco IOS リリース 15.1M から、Cisco IOS ソフトウェアでは **showlaneqosdatabase** コマンドは使用できません。

特定の LAN エミュレーション（LANE）Quality of Service（QoS）データベースの内容を表示するには、特権 EXEC モードで **showlaneqosdatabase** コマンドを使用します。

show lane qos database *name*

構文の説明

name	表示する QoS over LANE データベースを指定します。

コマンド デフォルト

デフォルトではこのコマンド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	変更箇所
12.1(2)E	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
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。
15.1M	このコマンドは削除されました。

例

この例では、Catalyst 5000 ファミリ ATM Module の QoS over LANE データベースの内容を表示する方法を示します。

```
ATM# show lane qos database user1
QOS: user1
    configured cos values: 5-7, usage: 1
    dst nsap: 47.009181000000061705B0C01.00E0B0951A40.0A
    pcr: 500000, mcr: 100000
```

この例では、Cisco 4500、7200、または 7500 シリーズ ルータの QoS over LANE データベースの内容を表示する方法を示します。

```
Router# show lane qos database user2
QOS: user2
```

```
configured cos values: 5-7, usage: 1
dst nsap: 47.009181000000061705B0C01.00E0B0951A40.0A
pcr: 500000, mcr: 100000
```

関連コマンド

コマンド	説明
atm-address	特定の ATM アドレスに関連付けられた QoS パラメータを指定します。
laneclientqos	QoS over LANE データベースをインターフェイスに適用します。
laneqosdatabase	QoS over LANE データベースを構築する処理を開始します。
ubr+cos	CoS 値を UBR+ VCC にマップします。

show mls qos から wrr-queue threshold

- show metadata application table （1580 ページ）
- show metadata flow （1582 ページ）
- show mls qos （1589 ページ）
- show mls qos aggregate policer （1594 ページ）
- show mls qos free-agram （1596 ページ）
- show mls qos interface （1597 ページ）
- show mls qos maps （1599 ページ）
- show mls qos mpls （1603 ページ）
- show mls qos protocol （1605 ページ）
- show mls qos queuing interface （1606 ページ）
- show mls qos statistics-export info （1610 ページ）
- show platform hardware acl entry global-qos （1612 ページ）
- show platform hardware pp active infrastructure pi npd rx policer （1614 ページ）
- show platform hardware qfp active feature qos config global （1616 ページ）
- show platform lowq （1618 ページ）
- show platform qos policy-map （1619 ページ）
- show platform software infrastructure punt statistics （1622 ページ）
- show policy-manager events （1624 ページ）
- show policy-manager policy （1626 ページ）
- show policy-map （1628 ページ）
- show policy-map class （1645 ページ）
- show policy-map control-plane （1647 ページ）
- show policy-map interface （1651 ページ）
- show policy-map interface brief （1704 ページ）
- show policy-map interface port-channel （1716 ページ）
- show policy-map interface service group （1718 ページ）
- show policy-map interface service instance （1721 ページ）
- show policy-map mgre （1726 ページ）
- show policy-map multipoint （1729 ページ）

- show policy-map session （1731 ページ）
- show policy-map target service-group （1739 ページ）
- show policy-map type access-control （1741 ページ）
- show policy-map type nat （1744 ページ）
- show policy-map type port-filter （1746 ページ）
- show protocol phdf （1748 ページ）
- show qbm client （1751 ページ）
- show qbm pool （1753 ページ）
- show qdm status （1756 ページ）
- show queue （1758 ページ）
- show queueing （1764 ページ）
- show queueing interface （1772 ページ）
- show random-detect-group （1777 ページ）
- show running-config service-group （1780 ページ）
- show sdm prefer current （1782 ページ）
- show service-group （1783 ページ）
- show service-group interface （1786 ページ）
- show service-group state （1788 ページ）
- show service-group stats （1789 ページ）
- show service-group traffic-stats （1792 ページ）
- show subscriber policy ppm-shim-db （1794 ページ）
- show table-map （1795 ページ）
- show tech-support nbar platform （1797 ページ）
- show tech-support rsvp （1813 ページ）
- show traffic-shape （1814 ページ）
- show traffic-shape queue （1817 ページ）
- show traffic-shape statistics （1822 ページ）
- show vrf （1825 ページ）
- show wrr-queue （1829 ページ）
- subscriber accounting accuracy （1830 ページ）
- svc-bundle （1831 ページ）
- table-map（値マッピング） （1832 ページ）
- tcp （1835 ページ）
- tcp contexts （1836 ページ）
- traffic-shape adaptive （1838 ページ）
- traffic-shape fecn-adapt （1840 ページ）
- traffic-shape group （1842 ページ）
- traffic-shape rate （1845 ページ）
- trust （1848 ページ）
- tx-ring-limit （1850 ページ）
- vbr-nrt （1852 ページ）

- vc-hold-queue （1857 ページ）
- wrr-queue bandwidth （1858 ページ）
- wrr-queue cos-map （1860 ページ）
- awrr-queue dscp-map （1862 ページ）
- wrr-queue queue-limit （1864 ページ）
- wrr-queue random-detect （1866 ページ）
- wrr-queue threshold （1868 ページ）

show metadata application table

デバイスに定義されているメタデータアプリケーションのリストを表示するには、特権EXECモードで **show metadata application table** コマンドを使用します。

show metadata application table

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.2(1)T	このコマンドが導入されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

例

次に、**show metadata application table** コマンドの出力例を示します。

```
Device# show metadata application table

ID     Name                  Vendor                Vendor id
-------------------------------------------------------------------------------
113    telepresence-media    -                     -
114    telepresence-contr$   -                     -
478    telepresence-data     -                     -
414    webex-meeting         -                     -
56     citrix                -                     -
81     cisco-phone           -                     -
472    vmware-view           -                     -
473    wyze-zero-client      -                     -
61     rtp                   -                     -
64     h323                  -                     -
5060   sip                   -                     -
554    rtsp                  -                     -
496    jabber                -                     -
5222   xmpp-client           -                     -
```

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 *189 : show metadata application table* のフィールドの説明

フィールド	説明
ID	アプリケーションID。内部的にアプリケーション名にマッピングされます。
Name	アプリケーションの名前。

関連コマンド

コマンド	説明
metadata application-params	メタデータ アプリケーション エントリ コンフィギュレーション モードにして、新しいメタデータ アプリケーション パラメータを作成します。

show metadata flow

メタデータ フロー情報を表示するには、特権 EXEC モードで **show metadata flow** コマンドを使用します。

show metadata flow {**classification table** |**local-flow-id** *flow-id* [**source** {**msp** |**nbar** |**rsvp**}] |**statistics** |**table** [{[**application name** *app-name*[{**ip** |**ipv6**}]] |**filter** [{**destination** {*ip-address ipv6-address*}}] [{**source** {*ip-address ipv6-address*}}] |**ip** |**ipv6**}]}

構文の説明

classification	メタデータ コントロール プレーン分類情報を表示します。
table	すべてのフロー エントリのメタデータ フロー情報を表示します。
local-flow-id *flow-id*	指定されたローカル フロー ID の情報を表示します。この ID は、ローカルに作成された特定の 5 タプルのメタデータ フロー エントリに固有の ID です。 • ローカル フロー ID は、フロー エントリが作成されるときに自動的に生成されます。
source	（任意）指定されたソースのメタデータ フロー情報を表示します。
msp	（任意）Media-Proxy Services のメタデータ フロー情報を表示します。
nbar	（任意）Network-Based Application Recognition（NBAR）のメタデータ フロー情報を表示します。
rsvp	（任意）リソース予約プロトコル（RSVP）のメタデータ フロー情報を表示します。
statistics	メタデータ フロー統計情報を表示します。
application	（任意）指定されたアプリケーションのメタデータ フロー情報を表示します。
name *app-name*	（任意）指定されたアプリケーションのすべてのフローを指定します。
ip	（任意）指定された IPv4 アドレスのメタデータ フロー情報を表示します。
ipv6	（任意）指定された IPv6 アドレスのメタデータ フロー情報を表示します。
filter	（任意）フィルタ基準に基づいてメタデータ フロー情報を表示します。
destination }	（任意）指定された宛先アドレスのメタデータ フロー情報を表示します。
source	（任意）指定された送信元アドレスのメタデータ フロ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	変更箇所
15.2(1)T	このコマンドが導入されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。
15.3(1)T	このコマンドが変更されました。**source**、**msp**、**nbar**、および **rsvp** キーワードが追加されました。IPv6 アドレス情報がコマンド出力に追加されました。

例

次に、**show metadata flow classification table** コマンドの出力例を示します。

```
Device# show metadata flow classification table

Policy Type Codes:
QOS     : QOS                              PM      : Performance Monitor
PMD     : Performance Monitor Dynamic      MACE    : MACE
-------------------------------------------------------------------------------
Target          Flow ID    Dir   Policy     Filter(s)
                                 Type
---------------+----------+-----+----------+-----------------------------------

Se2/0           1          OUT
Se2/0           2          OUT
Se2/0           3          OUT
Se2/0           4          OUT   QOS        application telepresence-media
Se2/0           5          OUT   QOS        application telepresence-media
Se2/0           6          OUT
Se2/0           7          OUT
Se2/0           8          OUT   QOS        application telepresence-media
Se2/0           9          OUT
```

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 *190 : show metadata classification table* フィールドの説明

フィールド	説明
Target	ポリシー マップが添付されているインターフェイス名。
Flow ID	フロー エントリ識別子。
Dir	フローエントリの方向。INは、フローがネットワーク要素に入っていることを示します。OUT は、フローがネットワーク要素から出て行っていることを示します。CL は、フローが正常に分類されたことを示します。

次に、 コマンドの出力例を示します。

```
Device# show metadata flow local-flow-id 22

To                                      From

Protocol SPort   DPort   Ingress I/F             Egress I/F
2012:33:1:2::2                          2012:33:1:2::1
UDP      49002   49003   n/a                     Serial2/0

Metadata Attributes :

Global Session Id           :   74657374-2D54-502D-3100-000000000000-00000000-00000000
Clock Frequency             :   123456
End Point Model             :   Test-TP-Model
Application Signaling Type  :   sip
Application Transport Type  :   rtp
Application Traffic Type    :   realtime
Application Device Class    :   room-conferencing
Application Category        :   voice-and-video
Application Group           :   telepresence-group
Application Media Type      :   video
Application Tag             :   218103921 (telepresence-media)
Application Name            :   telepresence-media

Matched filters :

 Direction: IN:
 Direction: OUT:
```

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 *191 : show metadata flow local-flow-id* フィールドの説明

フィールド	説明
To	フロー エントリの宛先アドレス。
From	フロー エントリの送信元アドレス。
Protocol	フローに使用されるトランスポート プロトコル（TCP または UDP）。
SPort	フロー エントリの送信元ポート。有効な範囲は 1 ～ 65535 です。
DPort	フロー エントリの宛先ポート。有効な範囲は 1 ～ 65535 です。
Ingress I/F	入力インターフェイス特定のネットワーク要素の着信インターフェイス。
Egress I/F	出力インターフェイス。特定のネットワーク要素の発信インターフェイス。
Global Session ID	アプリケーションのグローバル セッション ID。
Clock Frequency	アプリケーション クロックの周波数。
End Point Model	アプリケーションのモデル。

フィールド	説明
Application Signaling Type	アプリケーション ベンダーの名前。
Application Transport Type	メタデータ アプリケーションの転送タイプ。
Application Traffic Type	メタデータ アプリケーションのトラフィック タイプ。
Application Device Class	メタデータ アプリケーションの分類。
Application Category	メタデータ アプリケーションのカテゴリ。
Application Group	メタデータ アプリケーションのグループ。
Application Media Type	メタデータ アプリケーションのメディアのタイプ。
Application Tag	アプリケーション識別子。 • すべてのメタデータ アプリケーション名は、一意のアプリケーション タグにマップされます。
Application Name	メタデータ アプリケーションの名前。
Direction	アプリケーションの方向。

次に、**show metadata flow statistics** コマンドの出力例を示します。

```
Device# show metadata flow statistics

Interface specific report :

Serial2/0: Classified flows : Ingress 0, Egress 0

Chunk statistics :

Type               Allocated       Returned        Failed

IP Flow             9                 0               0
Flow Key            29                20              0
Source List         4                 0               0
Flow Info           29                29              0
Attribute Data      29                29              0
Feature Object      2                 0               0

Event Statistics:

Add Flow                : 9         Delete Flow             : 0
Received                : 30        Rejected                : 0
Transient               : 0         Posted                  : 29
Ingress Change          : 0         Egress Change           : 11
Unknown                  : 0         Source Limit Exceeded    : 0
```

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 *192 : show metadata flow statistics* フィールドの説明

フィールド	説明
Interface specific report	インターフェイスごとに出力フローまたは入力フローの数を指定するレポート。
Ingress	インターフェイスに入ったフローの数。
Egress	インターフェイスから出たフローの数。
Chunk statistics	チャンク メモリに固有の情報。
Type	どのような種類の情報やデータ構造の用途に対してメモリ消費量を記録するかを示します。
Allocated	指定された情報の種類に対して割り当てられたメモリ。
Returned	指定された情報の種類のためにシステムに返されたメモリ。
Failed	メモリ割り当て失敗の記録。
Event Statistics	デバイスで発生した各フロー イベントに固有の情報。
Add Flow	ネットワーク要素に追加されたフローの数。
Delete Flow	ネットワーク要素から削除されたフローの数。
Received	ネットワーク要素が受信したフローの数。
Rejected	ネットワーク要素が拒否したフローの数。
Transient	一時的な状態にあるフローの数。
Posted	リソース予約プロトコル（RSVP）が受信した変更通知の数。
Ingress Change	入力インターフェイスが変更された回数。
Egress Change	出力インターフェイスが変更された回数。
Unknown	不明イベントを受信した回数。
Source Limit Exceeded	デバイスに対して定義されているフロー制限が超過した回数。

次に、**show metadata flow table** コマンドの出力例を示します。

```
Device# show metadata flow table

Total number of IPV4 metadata flows 6

Flow  To              From            Proto DPort SPort Ingress      Egress

4     10.0.0.1        10.0.0.2        UDP   49008 49007             Se2/0
6     10.0.0.3        10.0.0.4        UDP   49004 49003             Se2/0
```

```
5     10.2.0.3        10.2.0.6        UDP   49010 49009             Se2/0
2     10.2.1.6        10.2.2.6        UDP   49004 49003             Se2/0
1     10.2.2.6        10.2.3.6        UDP   49002 49001             Se2/0
3     10.2.3.6        10.2.3.7        UDP   49006 49005             Se2/0


Total number of IPV6 metadata flows 3

To                                      From
Flow  Proto DPort SPort Ingress      Egress

2001:DB8:1::1                           2001:DB8:1::2
9     UDP   49001 49000              Se2/0
2001:DB8:1::3                           2001:DB8:1::4
7     UDP   49001 49000              Se2/0
2001:DB8:1::12                          2001:DB8:1::13
8     UDP   49003 49002              Se2/0
```

（注） IPv6 メタデータ フロー テーブルの出力が 2 行に表示されていますが、これは IPv6 アドレスが長くなることがあるからです。

次に、**show metadata flow table application name sip ip** コマンドの出力例を示します。

```
Device#  show metadata flow table application name sip ip

Flow  To              From           Protocol  DPort  SPort  Ingress   Egress  SSRC

2     209.165.201.14  209.165.201.18  UDP      70    80       Eth1/1   Eth1/2  3000
```

次に、**show metadata flow table application name sip ipv6** コマンドの出力例を示します。

```
Device# show metadata flow table application name sip ipv6

To                                      From
Flow  Proto DPort SPort Ingress      Egress

2001:DB8:1::3                           2001:DB8:1::4
9     UDP   49001 49000              Se2/0
2001:DB8:1::5                           2001:DB8:1::6
7     UDP   49001 49000              Se2/0
2001:DB8:1::12                          2001:DB8:1::14
8     UDP   49003 49002              Se2/0
```

次は、**show metadata flow table filter destination** コマンドの出力例です。フィルタ基準として送信元または宛先 IPv4 アドレスを指定できます。

```
Device# show metadata flow table filter destination 209.165.201.1

Entries To: 209.165.201.1

Flow ID    From            Protocol DPort   SPort   Ingress I/F    Egress I/F
1          209.165.201.3    UDP      1000    1000    Et0/0          Et0/1
2          209.165.201.3    UDP      1001    1001    Et0/0          Et0/1
Total Flows: 2
```

次に、**show metadata flow table ipv6** コマンドの出力例を示します。

```
Device# show metadata flow table ipv6

To                                      From
Flow  Proto DPort SPort Ingress      Egress

2001:DB8:1::1                          2001:DB8:1::2
9     UDP   49001 49000              Se2/0
2001:DB8:1::3                          2001:DB8:1::4
7     UDP   49001 49000              Se2/0
2001:DB8:1::12                         2001:DB8:1::13
8     UDP   49003 49002              Se2/0
```

関連コマンド

コマンド	説明
debug metadata	メタデータ フローのデバッグを有効にします。
metadata application-params	メタデータ アプリケーションエントリ コンフィギュレーション モードにして、新しいメタデータ アプリケーション パラメータを作成します。
show metadata application table	デバイスに定義されているメタデータ アプリケーションのリストを表示します。
metadata flow	デバイスでメタデータを有効にします。

show mls qos

マルチレイヤ スイッチング（MLS）Quality of Service（QoS）情報を表示するには、特権 EXEC モードで **showmlsqos** コマンドを使用します。

show mls qos [{**arp**|**ipv6**|**ip**|**ipx**|**last**|**mac**|**module** [*module-number*]} [{*interface interface-number*|**slot** *slot*|**null 0**|**port-channel** *number*|**vlan** *vlan-id*}]] **[detailed]**

構文の説明

arp	（オプション）アドレス解決プロトコル（ARP）情報を表示します。
ipv6	（任意）IPv6 情報を表示します。
ip	（任意）MLS IP ステータスに関する情報を表示します。
ipx	（任意）MLS Internetwork Packet exchange（IPX）ステータスに関する情報を表示します。
last	（任意）最終パケットのポリシングに関する情報を表示します。
mac	（任意）MAC アドレスベースの QoS ステータスに関する情報を表示します。
module *module-number*	（任意）モジュール（スロット）番号を指定します。グローバルおよびインターフェイス単位の QoS イネーブルおよびディセーブル設定、およびグローバル QoS カウンタを表示します。
interface	（任意）インターフェイス タイプ。有効な値は、**ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**、**ge-wan**、**pos**、および **atm** です。
interface-number	（任意）モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
slot *slot*	（任意）スロット番号を指定します。グローバルおよびインターフェイス単位の QoS イネーブルおよびディセーブル設定、およびグローバル QoS カウンタを表示します。
null0	（任意）ヌル インターフェイスを指定します。有効値は **0** だけです。
port-channel *number*	（任意）チャネル インターフェイスを指定します。1 ～ 282 の範囲の最大 64 個の値があります。
vlan *vlan-id*	（任意）VLAN ID を指定します。有効値の範囲は 1 ～ 4094 です。
detailed	（任意）その他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	変更箇所
12.2(14)SX	このコマンドが Supervisor Engine 720 に導入されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
12.2(18)SXE	**arp** キーワードおよび **ipv6** キーワードが Supervisor Engine 720 にのみ追加されました。
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。

12.2(33)SXI	• Catalyst 6500 シリーズ スイッチで次の情報がコマンド出力に追加されました。
	  • 過去 30 秒のカウンタの表示。
	  • 過去 5 分にわたるピーク 30 秒のカウンタの表示。
	  • 5 分平均およびピークのパケット/秒（pps）レートの表示。
	• ピーク レートは、10 秒の解像度でモニタされます。Cisco IOS リリース 12.2(33)SXI より前のリリースは、30 秒の解像度でモニタされていました。

使用上のガイドライン

Supervisor Engine 720 で設定されているシステムでは、ge-wan、pos、atm の各インターフェイスはサポートされていません。

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

257 ～ 282 の **port-channel***number* 値は、コンテント スイッチング モジュール（CSM）およびファイアウォール サービス モジュール（FWSM）でのみサポートされています。

Catalyst 6500 シリーズ スイッチ

Cisco IOS リリース 12.2(33)SXI 以降のリリースでは、**showmlsqos** コマンドの出力に次の情報が含まれています。

- 過去 30 秒のカウンタの表示。
- 過去 5 分にわたるピーク 30 秒のカウンタの表示。
- 5 分平均およびピークの bps レートの表示。

ピーク レートは、10 秒の解像度でモニタされます。Cisco IOS リリース 12.2(33)SXI より前のリリースは、30 秒の解像度でモニタされます。

例

最後にログに記録されたパケットの例

次に、最後に記録されたパケットに関する情報を表示する例を示します。

```
Router# show mls qos last
QoS engine last packet information:
    Packet was transmitted
    Output TOS/DSCP: 0xC0/48[unchanged]   Output COS: 0[unchanged]
    Aggregate policer index: 0(none)
    Microflow policer index: 0(none)
```

IPv6 の例

次に、IPv6 情報を表示する例を示します。

```
Router# show mls qos ipv6
QoS Summary [IPv6]:      (* - shared aggregates, Mod - switch module)
     Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                 Id         Id
-------------------------------------------------------------------------------
      All  7   -    Default    0    0*    No  0      189115356              0
```

例

次に、QoS 情報を表示する場合の例を示します。

```
Router# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS ip packet dscp rewrite enabled globally
QoS is disabled on the following interfaces:
Fa6/3 Fa6/4
QoS DSCP-mutation map is enabled on the following interfaces:
Fa6/5
Vlan or Portchannel(Multi-Earl) policies supported: Yes
Egress policies supported: Yes
----- Module [5] -----
QoS global counters:
Total packets: 164
IP shortcut packets: 0
Packets dropped by policing: 0
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0
MPLS packets with EXP changed by policing: 0
```

例

次の例では、キーワードを入力しない場合の出力を示します。

```
Router# show mls qos
  QoS is enabled globally
```

```
  Microflow QoS is enabled globally
QoS global counters:
    Total packets: 217500
    IP shortcut packets: 344
    Packets dropped by policing: 344
    IP packets with TOS changed by policing 18323
    IP packets with COS changed by policing 1602
    Non-IP packets with COS changed by policing 0
```

Catalyst 6500 シリーズ スイッチの例

Cisco IOS リリース 12.2(33)SXI 以降のリリースの **showmlsqos** コマンド出力には、以前のリリースよりも多くのパケット カウンタ情報が含まれています。

この例は、**detailed** キーワードを指定した Cisco IOS リリース 12.2(33)SXI の出力を示しています。

```
Router# show mls qos detailed
  QoS is enabled globally
  Policy marking depends on port_trust
  QoS ip packet dscp rewrite enabled globally
  Input mode for GRE Tunnel is Pipe mode
  Input mode for MPLS is Pipe mode
  Vlan or Portchannel(Multi-Earl) policies supported: Yes
  Egress policies supported: Yes
 ----- Module [5] -----
Traffic:            Total pkt's   30-s pkt's    peak pkts  5-min avg pps   peak pps
-------------------------------------------------------------------------------
Total packets:           775606           46           22              2          5
IP shortcut packets:    5465402           33           16              1          1
Packets dropped by
policing:                     0            0            0              0          0
IP packets with TOS
changed by policing:         41           10            4              0          0
IP packets with COS
changed by policing:          2            0            0              0          0
Non-IP packets with COS
changed by policing:          0            0            0              0          0
MPLS packets with EXP
changed by policing:          0            0            0              0          0
```

次の表では、**detailed** キーワードを入力すると追加される重要なフィールドについて説明します。

表 *193 : show mls qos detailed* フィールドの説明

フィールド	説明
Total packets	累積的なカウンタ。
IP shortcut packets	IP ショートカット パケットの数。
Packets dropped by policing	ポリシングでドロップされたパケットの数。

フィールド	説明
Packets changed by policing	ポリシングで変更されたパケットの数。
30-s pkts	過去 5 分にわたる 30 秒パケット合計数。
30-s peak pkts	過去 5 分にわたる 30 秒パケット ピーク数。
5-min avg pps	過去5分間の平均パケット/秒（pps）レート。
5-min peak pps	過去 5 分間のピーク pps レート。

関連コマンド

コマンド	説明
mlsqos(globalconfigurationmode)	QoS 機能をグローバルにイネーブルにします。
mlsqos(interfaceconfigurationmode)	インターフェイスでの QoS 機能をイネーブルにします。
showmlsqosaggregate-policer	集約ポリサーに関する情報を表示します。
showmlsqosfree-agram	スイッチ プロセッサおよび DFC 上にある空の集約 RAM インデックスの数を表示します。
showmlsqosinterface	インターフェイス レベルで MLS QoS 情報を表示します。
showmlsqosmaps	MLS QoS マッピング情報を表示します。
showmlsqosmpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。
showmlsqosprotocol	プロトコル パススルー情報を表示します。
showmlsqosstatistics-export	MLS 統計データ エクスポート ステータスおよび設定を表示します。

show mls qos aggregate policer

マルチレイヤ スイッチング（MLS）Quality of Service（QoS）の集約ポリサーに関する情報を表示するには、EXEC モードで **showmlsqosaggregatepolicer** コマンドを使用します。

show mls qos aggregate policer [*aggregate-name*]

構文の説明

aggregate-name	（任意）集約ポリサーの名前。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

集約ポリシングは、分散型フォワーディング カード（DFC）を装備した各スイッチング モジュール上、およびポリシー フィーチャ カード 2（PFC2。DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチングモジュールからのフロー統計情報は合算されません。集約ポリシングの統計情報は、DFC を装備したスイッチング モジュール、PFC2、および PFC2 がサポートする DFC を装備していないスイッチング モジュールごとに表示できます。

例

次の例では、MLS QoS の集約ポリサーに関する情報を表示する方法を示します。

```
Router# show mls qos aggregate-policer
ag1 (undefined)
    AgId=0 [ pol1 pol2 ]
ag2 64000 64000 conform-action set-dscp-transmit 56 exceed-action drop
    AgId=0 [ pol3 ]
ag3 32000 32000 conform-action set-dscp-transmit 34 exceed-action drop
```

出力の意味は、次のとおりです。

- **AgId** パラメータは、ハードウェア ポリサー ID を表示し、割り当て済みであればゼロ以外になります。
- ポリサーを使用するポリシー マップ（ある場合）は、角カッコ（[]）内にリストされます。
- ポリサーを使用するポリシーがない場合、**AgId** 行は表示されません。

- ポリサーがポリシー マップで参照されているものの、まだ定義されていない場合は、[**undefined**] が表示されます。

関連コマンド

コマンド	説明
mlsqosaggregate-policer	ポリシーマップで使用するために、名前付き集約ポリサーを定義します。

show mls qos free-agram

スイッチプロセッサおよび分散型フォワーディングカード（DFC）上にある空の集約RAMインデックスの数を表示するには、EXEC モードで **showmlsqosfree-agram** コマンドを使用します。

show mls qos free-agram

構文の説明

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

このコマンドには、デフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.2(18)SXD	このコマンドのサポートが、Supervisor Engine 720 および Supervisor Engine 2 に導入されました。
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。

例

次に、スイッチプロセッサおよびDFC上にある空の集約RAMインデックスの数を表示する例を示します。

```
Router# show mls qos free-agram
Total Number of Available AG RAM indices : 1023
 Module [1]
 Free AGIDs : 1023
 Module [6]
 Free AGIDs : 1023
```

show mls qos interface

インターフェイス レベルの マルチレイヤ スイッチング（MLS）Quality of Service（QoS）情報を表示するには、特権 EXEC モードで **showmlsqosinterface** コマンドを使用します。

show mls qos interface [*interface-id*] **[policers]**

構文の説明

interface-id	（任意）QoS 情報を表示するインターフェイスを指定します。
policers	（任意）インターフェイスに設定されたすべてのポリサー、それらの設定、および割り当てられてないポリサー数を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに実装されました。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
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。

使用上のガイドライン

すべてのインターフェイスのパラメータを表示するには、キーワードを指定しないで **showmlsqosinterface** コマンドを使用します。

特定のインターフェイスのパラメータを表示するには、**showmlsqosinterface***interface-id* コマンドを使用します。

ほとんどのシスコ スイッチ プラットフォームでは、グローバル コマンド「(no) mls qos」は MLS QoS 状態を有効または無効に切り替えるために使用します。MLS QoS がグローバルに無効になっている場合、スイッチを通過するすべてのトラフィックの CoS/IP プレシデンス/DSCP 値は変更されません。一方、MLS QoS が有効になっている場合、デフォルトではすべてのインターフェイスが信頼しない状態になります。つまり、受信したすべての CoS/IP プレシデンス/DSCP 値が 0 に再マークされます。

Cisco_2600 と Cisco_3600 シリーズ スイッチ

(no)mlsqos グローバル コマンドは Cisco_2600 や Csico_3600 シリーズ スイッチではサポートされていないため、インターフェイスのデフォルトの信頼状態に関して固有の状況が生じます。

デフォルトでは、Cisco_2600 または Cisco_3600 シリーズ スイッチ上のインターフェイスで設定された「mls qos」関連のコマンドがない場合、すべての着信トラフィックの CoS/IP プレシデンス/DSCP 値はスイッチを通過するため再マークされません。これは、MLS QoS が他のシスコ スイッチで無効になっている場合と同じ結果をもたらします。

例

次は、**showmlsqosinterfacefastethernet0/1** コマンドの出力例です。

```
Router# show mls qos interface fastethernet0/1
FastEthernet0/1
trust state: trust cos
COS override: dis
default COS: 0
```

次の例は、インターフェイスに設定された mls QoS コマンドがなく、着信トラフィックの CoS/IP プレシデンス/DSCP 値がスイッチを通過するため再マークされないことを示しています。

```
Router# show mls qos interface f1/1
FastEthernet1/1
trust state: none  <<<
trust mode: none  <<<
COS override: dis
default COS: 0
pass-through: none
```

関連コマンド

コマンド	説明
mlsqoscos	ポートのデフォルトの MLS CoS 値を定義するか、またはポート上のすべての受信パケットにデフォルトの CoS 値を割り当てます。
mlsqosmap	MLS CoS/DSCP マップおよび DSCP/CoS マップを定義します。
mlsqostrust	MLS ポートの信頼状態を設定し、CoS または DSCP 値の検査によってトラフィックを分類します。

show mls qos maps

マルチレイヤ スイッチング（MLS）Quality of Service（QoS）マッピング情報を表示するには、特権 EXEC モードで **showmlsqosmaps** コマンドを使用します。

Cisco 2600、3660、3700、3845、7200、7400、および 7500 シリーズ ルータ
show mls qos maps [{**cos-dscp**|**dscp-cos**}]

Cisco 7600 シリーズ ルータおよび Catalyst 6500 シリーズ スイッチ
show mls qos maps
[{**cos-dscp**|**cos-mutation**|**dscp-cos**|**dscp-exp**|**dscp-mutation**|**exp-dscp**|**exp-mutation**|**ip-prec-dscp**|**policed-dscp**}]

構文の説明

cos-dscp	（任意）サービス クラス（CoS）と DiffServ コードポイント（DSCP）とのマップを表示します。
dscp-cos	（任意）DSCP/CoS マップを表示します。
cos-mutation	（任意）CoS 変換マップを表示します。
dscp-exp	（任意）DSCP/exp マップを表示します。
dscp-mutation	（任意）DSCP 変換マップを表示します。
exp-dscp	（任意）exp/DSCP マップを表示します。
exp-mutation	（任意）exp 変換マップを表示します。
ip-prec-dscp	（任意）IP precedence/DSCP マップを表示します。
policed-dscp	（任意）ポリシング済み DSCP マップを表示します。

コマンド デフォルト

すべての MLS QoS マップが表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.1(6)EA2	このコマンドが導入されました。
12.2(14)SX	このコマンドが Cisco 7600 シリーズ ルータに実装されました。
12.2(15)ZJ	このコマンドが、Cisco 2600 シリーズ ルータ、Cisco 3600 シリーズ ルータ、および Cisco 3700 シリーズ ルータのプラットフォームに実装されました。
12.2(17b)SXA	このコマンドは、**cos-mutation**、**exp-dscp**、**exp-mutation** の各キーワードをサポートするように変更されました。

リリース	変更箇所
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。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズ ルータ上の Cisco IOS Release 12.3(4)T に統合されました。
12.2(33)SXI	すべてのマップ タイプ キーワードのサポートが追加されました。

使用上のガイドライン

マップは、トラフィックのプライオリティを表す内部DSCP値を生成するために使用します。すべてのマップを表示するには、キーワードを指定しないで**showmlsqosmaps**コマンドを使用します。

例

次に、各 CoS 値のマップ先となる DSCP 値を表示する **showmlsqosmapscos-dscp** コマンドの出力例を示します。

```
Router# show mls qos maps cos-dscp
Cos-dscp map:
        cos:  0  1  2  3  4  5  6  7
     --------------------------------
       dscp:  8  8  8  8 24 32 56 56
```

次に、各 DSCP 値のマップ先となる CoS 値を表示する **showmlsqosmapsdscp-cos** コマンドの出力例を示します。

```
Router# show mls qos maps dscp-cos
Dscp-cos map:
       dscp:  0  8 10 16 18 24 26 32 34 40 46 48 56
     ---------------------------------------------
         cos:  0  1  1  1  2  2  3  3  4  4  5  6  7
```

次に、QoS マップの設定を表示する例を示します。

```
Router# show mls qos maps
   Policed-dscp map:
            0  1  2  3  4  5  6  7  8  9
   ---------------------------------
      00:  00 01 02 03 04 05 06 07 08 09
      10:  10 11 12 13 14 15 16 17 18 19
      20:  20 21 22 23 24 25 26 27 28 29
      30:  30 31 32 33 34 35 36 37 38 39
      40:  40 41 42 43 44 45 46 47 48 49
      50:  50 51 52 53 54 55 56 57 58 59
      60:  60 61 62 63
   Dscp-cos map:
            0  1  2  3  4  5  6  7  8  9
   ---------------------------------
      00:  00 00 00 00 00 00 00 00 01 01
      10:  01 01 01 01 01 01 02 02 02 02
      20:  02 02 02 02 03 03 03 03 03 03
      30:  03 03 04 04 04 04 04 04 04 04
      40:  05 05 05 05 05 05 05 05 06 06
      50:  06 06 06 06 06 06 07 07 07 07
      60:  07 07 07 07
   Cos-dscp map:
```

```
          cos:   0  1  2  3  4  5  6  7
        ---------------------------------
         dscp:   0  8 16 24 32 40 48 56
    IpPrecedence-dscp map:
        ipprec:   0  1  2  3  4  5  6  7
        ---------------------------------
         dscp:   0  8 16 24 32 40 48 56
Router#
```

ポリシング済み DSCP および DSCP-CoS マップの表示では、新規の DSCP 値または CoS 値がテーブルの本文に表示されます。元の DSCP 値の 10 進が左側の縦列に表示され、単位の桁が先頭行に表示されます。たとえば、DSCP-CoS マップは、元の DSCP 値が 32 ～ 39 の範囲にある場合、CoS が 4 に設定されることを示しています。

CoS-DSCP マップおよび IP プレシデンス DSCP マップには、各 CoS 値または IP プレシデンス値のマップ先となる DSCP 値が表示されます。たとえば、IP プレシデンス DSCP マップは、元の IP プレシデンス値が 3 の場合、DSCP が 24 に設定されることを示しています。

次に、DSCP 変換マッピング設定を確認する例を示します。

```
Router# show mls qos maps | begin DSCP mutation

DSCP mutation map mutmap1:                    (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    08 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
 <...Output Truncated...>
Router#
```

DSCP 変換マップの表示では、マーキング済み DSCP 値がテーブルの本体に表示されます。元の DSCP 値の 1 桁め（d1）は d1 のラベルが付いた左側の縦列に表示され、2 桁め（d2）は先頭行に表示されます。たとえば、DSCP 値 30 は、新しい DSCP 値 08 にマップされます。

関連コマンド

コマンド	説明
mlsqosmap	CoS/DSCP マップおよび DSCP/CoS マップを定義します。
mlsqosmapcos-dscp	信頼されたインターフェイスに入力CoS/DSCPマップを定義します。
mlsqosmapcos-mutation	パケットの CoS を新しい CoS 値にマッピングします。
mlsqosmapdscp-cos	出力 DSCP/CoS マップを定義します。
mlsqosmapdscp-mutation	指定した DSCP 変換マップを定義します。
mlsqosmapip-prec-dscp	信頼されたインターフェイスに入力 IP precedence/DSCP マップを定義します。

コマンド	説明
mlsqosmappoliced-dscp	ポリシング済み DSCP 値とマーキング済み DSCP 値のマップを設定します。

show mls qos mpls

ポリシー マップにおけるマルチプロトコル ラベル スイッチング（MPLS）Quality of Service（QoS）クラスのインターフェイスの概要を表示するには、ユーザ EXEC モードまたは、特権 EXEC モードで **showmlsqosmpls** コマンドを使用します。

show mls qos mpls [{**interface-type** *interface-number*|**module slot**}]

構文の説明

interface-type *interface-number*	（任意）インターフェイス タイプ。有効な値は次のとおりです。 • **fastethernet** • **gigabitethernet** • **tengigabitethernet**. （任意）モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
module slot	（任意）モジュールのスロット番号を指定します。

コマンド モード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(17a)SX	このコマンドが Supervisor Engine 720 に導入されました。
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。

使用上のガイドライン

このコマンドをサポートするのは、PFC3BXL または PFC3B モードだけです。

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

例

次の例は、ポリシー マップにおける MPLS QoS クラスのインターフェイスの概要を示しています。

```
Router# show mls qos mpls
QoS Summary [MPLS]: (* - shared aggregates, Mod - switch module)
Int Mod Dir Class-map DSCP Agg Trust Fl AgForward-By AgPoliced-By
Id Id
--------------------------------------------------------------------------------
```

```
Fa3/38 5 In exp2 0 1 dscp 0 378900 0
Fa3/41 5 In exp4 0 3 dscp 0 0 0
All 5 - Default 0 0* No 0 1191011240 0
```

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 *194 : show mls qos mpls* フィールドの説明

フィールド	説明
QoS Summary [MPLS]: (* - shared aggregates, Mod - switch module)	* で示される共有集約ポリサー、およびモジュールの種類があるかどうかを示します。
Int Mod Dir Class-map DSCP Agg Trust Fl AgForward-By AgPoliced-By	次の行の列ヘッダーを表示します。このようなヘッダーには、インターフェイス名と番号、モジュール番号、方向、クラスマップ名、DSCP 値などがあります。
Fa3/38 5 In exp2 0 1 dscp 0 378900 0	次の情報を提供します。 • Fa3/38：インターフェイス名と番号。 • 5：シャーシ内のモジュール番号。 • In：適用するポリシーの方向（In = 入力）。 • exp2：ポリシーに設定されているクラス マップ。 • 0：DiffServ コード ポイント（DSCP）値。 • 1：クラス マップに割り当てられたポリサー ID。 • dscp：ポートに設定された信頼性の値。この例では、値は DSCP で信頼されています。 • 0：フロー ID（フロー ポリサーが設定されている場合）。 • 378900：集約転送済みバイト、つまり、転送されたトラフィック。 • 0：集約ポリシング済みバイト、つまり、このトラフィックはポリシングの対象になりました。
All 5 - Default 0 0* No 0 1191011240 0	集約転送済みバイトや集約ポリシング済みバイトなど、先行する行の合計。

関連コマンド

コマンド	説明
mlsqosexp-mutation	出力EXP変換マップをインターフェイスに付加します。
mlsqosmapexp-dscp	内部 DSCP マップに入力 EXP 値を定義します。
mlsqosmapexp-mutation	パケットの EXP を新しい EXP 値にマッピングします。

show mls qos protocol

プロトコル パススルー情報を表示するには、EXEC モードで **showmlsqosprotocol** コマンドを使用します。

show mls qos protocol [**module** *number*]

構文の説明

module *number*	（任意）モジュール番号を指定します。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.2(17a)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(18)SXE	Supervisor Engine 2 でこのコマンドのサポートが導入されましたが、Address Resolution Protocol（ARP）、Integrated Intermediate System-to-Intermediate System（IS-IS）、または Enhanced Interior Gateway Routing Protocol（EIGRP）はサポートされていません。 Supervisor Engine 720 でのみ Neighbor Discovery Protocol パケットのサポートが追加されました。
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。

例

次に、プロトコル パススルー情報を表示する例を示します。

```
Router# show mls qos protocol
RIP : Passthru mode
OSPF : Passthru mode
ND : Policing mode Cir = 32000 Burst = 1000
----- Module [5] -----
Routing protocol RIP is using AgId 0*
Routing protocol OSPF is using AgId 0*
Routing protocol ND is using AgId 1
----- Module [6] -----
Routing protocol RIP is using AgId 0*
Routing protocol OSPF is using AgId 0*
```

関連コマンド

コマンド	説明
mlsqosprotocol	ルーティング プロトコル パケット ポリシングを定義します。

show mls qos queuing interface

インターフェイスのキューイング統計情報を表示するには、ユーザ EXEC モードで **showmlsqosqueuinginterface** コマンドを使用します。

show mls qos queuing interface {*type*|**vlan**}

構文の説明

type	インターフェイス タイプ。 Cisco 7600 シリーズ ルータの場合、有効なインターフェイス タイプは **ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**、**pos**、**atm**、および **ge-wan** です。
vlan	VLAN 識別番号を指定します。有効な値は 1 ～ 4094 です。

コマンド モード

ユーザ EXEC (>)

コマンド履歴

リリース	変更箇所
15.0(1)S	このコマンドは、Cisco 7600 シリーズ ルータ上の LAN カードに導入されました。

使用上のガイドライン

Cisco 7600 シリーズ ルータ

pos、atm、および ge-wan インターフェイスは、Supervisor Engine 2 が搭載された Cisco 7600 シリーズ ルータでのみサポートされています。

typenumber 引数を **interface** キーワードとともに使用すると、モジュール番号とポート番号を指定できます。有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、ギガビット イーサネット インターフェイスを指定し、13 スロット シャーシに設置された 48 ポート 10/100BASE-T イーサネット モジュールを使用する場合、モジュール番号の有効値の範囲は 1 ～ 13 であり、ポート番号の有効値の範囲は 1 ～ 48 です。

ハードウェアにプログラミングされた値を検証するには、**showqm-spport-data** コマンドを使用します。

例

次の例は、Endor（RSP720-10G）カードでの **showmlsqosqueuinginterfacegigabitethernet5/1** コマンドの出力例を示しています。

```
Router# show mls qos queuing interface gig5/1
Weighted Round-Robin
  Port QoS is enabled
  Port is untrusted
  Extend trust state: not trusted [COS = 0]
  Default COS is 0
    Queueing Mode In Tx direction: mode-cos
    Transmit queues [type = 1p3q8t]:
```

```
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       01         WRR                 08
       02         WRR                 08
       03         WRR                 08
       04         Priority            01
WRR bandwidth ratios:  100[queue 1] 150[queue 2] 200[queue 3]
    queue-limit ratios:     50[queue 1]  20[queue 2]  15[queue 3]  15[Pri Queue]
    queue tail-drop-thresholds
    -------------------------
    1     70[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    2     70[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    3     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    queue random-detect-min-thresholds
    ----------------------------------
      1    40[1] 70[2] 70[3] 70[4] 70[5] 70[6] 70[7] 70[8]
      2    40[1] 70[2] 70[3] 70[4] 70[5] 70[6] 70[7] 70[8]
      3    70[1] 70[2] 70[3] 70[4] 70[5] 70[6] 70[7] 70[8]
    queue random-detect-max-thresholds
    ----------------------------------
      1    70[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      2    70[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      3    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    WRED disabled queues:
    queue thresh cos-map
    ---------------------------------------
    1     1      0
    1     2      1
    1     3
    1     4
    1     5
    1     6
    1     7
    1     8
    2     1      2
    2     2      3 4
    2     3
    2     4
    2     5
    2     6
    2     7
    2     8
    3     1      6 7
    3     2
    3     3
    3     4
    3     5
    3     6
    3     7
    3     8
    4     1      5
    Queueing Mode In Rx direction: mode-cos
    Receive queues [type = 2q8t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       01         WRR                 08
       02         WRR                 08
    WRR bandwidth ratios:  100[queue 1]   0[queue 2]
    queue-limit ratios:    100[queue 1]   0[queue 2]
    queue tail-drop-thresholds
    -------------------------
    1     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    2     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    queue random-detect-min-thresholds
```

```
  ----------------------------------
    1    40[1] 40[2] 50[3] 50[4] 50[5] 50[6] 50[7] 50[8]
    2    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  queue random-detect-max-thresholds
  ----------------------------------
    1    70[1] 80[2] 90[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    2    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  queue thresh cos-map
  ---------------------------------------
  1     1      0 1 2 3 4 5 6 7
  1     2
  1     3
  1     4
  1     5
  1     6
  1     7
  1     8
  2     1
  2     2
  2     3
  2     4
  2     5
  2     6
  2     7
  2     8
Packets dropped on Transmit:
  queue     dropped  [cos-map]
  ---------------------------------------------
  1                       0  [0 1 ]
  2                       0  [2 3 4 ]
  3                       0  [6 7 ]
  4                       0  [5 ]
Packets dropped on Receive:
  BPDU packets:  0
  queue              dropped  [cos-map]
  ---------------------------------------------------
  1                       0  [0 1 2 3 4 5 6 7 ]
  2                       0  []
.
.
.
```

関連コマンド

コマンド	説明
mlsqoscos	ポートのデフォルトの MLS CoS 値を定義するか、またはポート上のすべての受信パケットにデフォルトの CoS 値を割り当てます。
mlsqosmap	MLS CoS/DSCP マップおよび DSCP/CoS マップを定義します。
mlsqostrust	MLS ポートの信頼状態を設定し、CoS または DSCP 値の検査によってトラフィックを分類します。
custom-queue-list	カスタム キュー リストをインターフェイスに割り当てます。
fair-queue(class-default)	デフォルト クラス ポリシーの一部として class-default クラスで使用するために予約するダイナミック キューの数を指定します。
fair-queue(WFQ)	インターフェイスに対する WFQ を有効にします。

コマンド	説明
priority-group	指定した優先リストをインターフェイスに割り当てます。
random-detectflow	フローベース WRED をイネーブルにします。
random-detect(interface)	WRED または DWRED をイネーブルにします。
random-detect(perVC)	per-VC WRED または per-VC DWRED をイネーブルにします。
showframe-relaypvc	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。
showqm-spport-data	QoS Manager スイッチ プロセッサに関する情報を表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

show mls qos statistics-export info

マルチレイヤ スイッチング（MLS）統計データ エクスポート ステータスおよび設定に関する情報を表示するには、EXEC モードで **showmlsqosstatistics-exportinfo** コマンドを使用します。

show mls qos statistics-export info

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

このコマンドには、デフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

Quality of Service（QoS）統計データ エクスポートは、Optical Service Module（OSM）インターフェイスではサポートされていません。

例

次に、MLS 統計データ エクスポートのステータスおよび設定に関する情報を表示する例を示します。

```
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : @
Export Destination : 172.20.52.3, UDP port 514 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
--------------------------------------------------------------
class3
```

関連コマンド

コマンド	説明
mlsqosstatistics-export(globalconfiguration)	QoS 統計データのエクスポートをグローバルにイネーブルにします。
mlsqosstatistics-export(interfaceconfiguration)	ポート単位の QoS 統計データのエクスポートをイネーブルにします。
mlsqosstatistics-exportaggregate-policer	名前付き集約ポリサー上で QoS 統計データのエクスポートをイネーブルにします。
mlsqosstatistics-exportclass-map	クラスマップの QoS 統計データのエクスポートをイネーブルにします。
mlsqosstatistics-exportdelimiter	QoS 統計データのエクスポート フィールドのデリミタを設定します。
mlsqosstatistics-exportdestination	QoS 統計データのエクスポートの宛先ホストおよび UDP ポート番号を設定します。
mlsqosstatistics-exportinterval	ポートまたは集約ポリサー QoS 統計データの読み込み頻度およびエクスポート頻度を指定します。

show platform hardware acl entry global-qos

着信および発信アクセス コントロール リスト（ACL）TCAM（Ternary Content Addressable Memory）グローバル Quality of Service（QoS）エントリに関する情報を表示するには、特権 EXEC モードで **showplatformhardwareaclentryglobal-qos** コマンドを使用します。

show platform hardware acl entry global-qos {**in**|**out**} {**arp**|**ip**|**ipv6**|**mac**|**mpls**} **[detail]**

構文の説明

in	出力に着信エントリを表示します。
out	出力に発信エントリを表示します。
arp	エントリの Address Resolution Protocol を指定します。
ip	エントリのインターネット プロトコルを指定します。
ipv6	エントリのインターネット プロトコル バージョン 6 を指定します。
mac	エントリの MAC アドレスを指定します。
mpls	エントリのマルチプロトコル ラベル スイッチング プロトコルを指定します。
detail	エントリに関する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	変更箇所
12.2XJC	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 ベースのスイッチは、TCAM を使用して、ワイヤレート ACL および QoS 機能をサポートします。ACL およびポリシーを有効にしても、ACL が TCAM に完全にロードされている限り、スイッチのスイッチングまたはルーティングのパフォーマンスは低下しません。

さまざまなタイプの ACL および QoS ポリシーをハードウェアに実装するために、Cisco IOS ベースのスイッチはスーパバイザ エンジンでハードウェア ルックアップ テーブル（TCAM）およびさまざまなハードウェア レジスタを使用します。パケットが到着すると、スイッチはハードウェア テーブル ルックアップ（TCAM ルックアップ）を実行し、パケットを許可するか拒否するかを決定します。

例

showplatformhardwareaclentryglobal-qos コマンドの次の出力例は、着信 Address Resolution Protocol エントリの 1 つの結果を示しています。

```
Switch# show platform hardware acl entry global-qos in arp
```

```
0x0000000000000003 arp ip any any mac any
```

showplatformhardwareaclentryglobal-qos コマンドの次の出力例は、着信 Address Resolution Protocol エントリの詳細な結果を示しています（凡例では、出力に表示される可能性がある略語を定義しています）。

```
Switch# show platform hardware acl entry global-qos in arp detail
------------------------------------------------------------------------------------------------
ENTRY TYPE: A - ARP I - IPv4 M - MPLS O - MAC Entry S - IPv6(Six) C - Compaction L -
L2V4 Suffix: D - dynamic entry E - exception entry R - reserved entry
FIELDS: FS - first_seen/from_rp ACOS - acos/group_id F - ip_frag FF - frag_flag DPORT -
 dest_port SPORT - src_port LM - L2_miss GP - gpid_present ETYPE - enc_etype CEVLD -
ce_vlan_valid MM - mpls_mcast FN - exp_from_null IV - ip_hdr_vld MV - mpls_valid E_CAU
- exception_cause UK - U_key ACO - acos A/R - arp_rarp RR - req_repl GM -
global_acl_fmt_match D-S-S-A - dest_mac_bcast, src_snd_mac_same, snd_tar_mac_same,
arp_rarp_vld OM - ofe_mode SVLAN - Src_vlan
------------------------------------------------------------------------------------------------
```

A	INDEX	LABEL	A/R	RR	IP SA	IP DA	SRC MAC	D-S-S-A	GM	IM	OM	RSLT	CNT
ARV	963	8191	1	7	0.0.0.0	0.0.0.0	FFFF.FFFF.FFFF	1-1-1-1	1	1	0	0x0000000000000003	0
ARM	963	0x0000	0	0x0	0.0.0.0	0.0.0.0	0000.0000.0000	0-0-0-1	0	0	1		

コマンド	説明
mlsqosprotocol	**showplatformhardwareaclentryglobal-qos** コマンドによって表示される TCAM エントリを設定します。

show platform hardware pp active infrastructure pi npd rx policer

すべてのキューのパント ポリシング統計情報を表示するには、特権 EXEC モードで **show platform hardware pp active infrastructure pi npd rx policer** コマンドを使用します。

show platform hardware pp active infrastructure pi npd rx policer

構文の説明

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

無効（パント ポリサーに関する情報は表示されません）。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.5S	このコマンドが、Cisco ASR 903 ルータに追加されました。

使用上のガイドライン

すべてのキューのパント レートおよびバースト レート統計情報を表示し、パント ポリサー設定を検証するには、**show platform hardware pp active infrastructure pi npd rx policer** コマンドを使用します。

例

次に、**show platform hardware pp active infrastructure pi npd rx policer** コマンドの出力例を示します。

```
Router# show platform hardware pp active infrastructure pi npd rx policer

PUNT POLICER
Ring |          Queue Name |           Punt rate |          Burst rate
-----+---------------------+---------------------+--------------------
 0   |     SW FORWARDING Q |                 500 |                1000
 1   |  ROUTING PROTOCOL Q |                 500 |                1000
 2   |              ICMP Q |                 500 |                1000
 3   |             HOST Q  |                1000 |                2000
 4   |       ACL LOGGING Q |                 500 |                1000
 5   |               STP Q |                3000 |                6000
 6   |       L2 PROTOCOL Q |                1000 |                2000
 7   |     MCAST CONTROL Q |                1000 |                2000
 8   |         BROADCAST Q |                 500 |                1000
 9   |               REP Q |                3000 |                6000
10   |               CFM Q |                3000 |                6000
11   |           CONTROL Q |                1000 |                2000
12   |       IP MPLS TTL Q |                1000 |                2000
13   |     DEFAULT MCAST Q |                 500 |                1000
14   |  MCAST ROUTE DATA Q |                 500 |                1000
15   |    MCAST MISMATCH Q |                 500 |                1000
16   |          RPF FAIL Q |                 500 |                1000
```

```
17   |  ROUTING THROTTLE Q |                500 |                1000
18   |             MCAST Q |                500 |                1000
19   |          MPLS OAM Q |               1000 |                2000
20   |       IP MPLS MTU Q |                500 |                1000
21   |               PTP Q |               3000 |                6000
22   |         LINUX ND Q  |                500 |                1000
23   |         KEEPALIVE Q |               1000 |                2000
24   |              ESMC Q |               3000 |                6000
25   |          FPGA BFD Q |               3000 |                6000
26   |          FPGA CCM Q |               3000 |                6000
27   |          FPGA CFE Q |               3000 |                6000
28   |          L2PT DUP Q |               4000 |                8000
```

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 *195 : show platform hardware pp active infrastructure pi npd rx policer* フィールドの説明

フィールド	説明
Ring	キューを識別する一意の番号です。
Queue Name	キューの名前。
Punt rate	キューのパント レート（パケット/秒（pps））。
Burst rate	キューのバースト レート（パケット/秒（pps））。

関連コマンド

コマンド	説明
platform punt-police queue	キューのパント ポリシングを有効にし、キュー単位で最大パント レートおよびバースト レートを指定します。
show platform software infrastructure punt statistics	キューベースのパント ポリシングが有効になっているかどうかを表示します。

show platform hardware qfp active feature qos config global

QoS：パケットマーキング統計情報機能およびQoS：パケット一致統計情報機能が現在有効になっているかどうかを表示するには、特権 EXEC モードで **showplatformhardwareqfpactivefeatureqosconfigglobal** コマンドを使用します。

show platform hardware qfp active feature qos config global

構文の説明

hardware	ハードウェア（Hardware）
qfp	Quantum Flow Processor
active	アクティブ インスタンス
feature	機能固有の情報
qos	Quality of Service（QoS）情報
config	QoS 設定情報
global	グローバル設定

コマンド デフォルト

無効（QoS：パケットマーキング統計情報機能またはQoS：パケット一致統計情報機能の状態に関する情報は表示されません）。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.3S	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: パケット マーキング統計情報機能と QoS: パケット一致統計情報機能の両方とも、デフォルトでは無効になっています。それらが有効になっているかどうかを表示するには、**showplatformhardwareqfpactivefeatureqosconfigglobal** コマンドを使用します。

例

次の例は、QoS：パケット マーキング統計情報機能または QoS：パケット一致統計情報機能が有効になっているかどうかを確認する方法を示しています。

```
Router#
show platform hardware qfp active feature qos config global

Marker statistics are: enabled
Match per filter statistics are: enabled
```

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 *196 : show platform hardware qfp active feature qos config global* フィールドの説明

フィールド	説明
Marker statistics are:	QoS：パケット マーキング統計情報機能の状態（有効または無効）。
Match per filter statistics are:	QoS：パケット一致統計情報機能の状態（有効または無効）。

関連コマンド

コマンド	説明
platformqosmarker-statistics	ヘッダーを変更し、ローカル ルータ処理のカテゴリに分類されたパケットの数を表示します。
platformqosmatch-statisticsper-filter	ユーザ定義のフィルタに一致するパケットおよびバイトの数を表示します。

show platform lowq

各インターフェイスに設定された低優先度キューの数を表示するには、**showplatformlowq** コマンドを使用します。

showplatformlowq

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.0(1)S	このコマンドが導入されました。

使用上のガイドライン

低優先度キューのライン カードを使用している場合に、インターフェイスごとにキューの数を確認するには、**showplatformlowq** コマンドを使用します。ライン カードに設定されたキューがない場合は、低優先度キューが空であることを示すメッセージが表示されます。

例

次に、**showplatformlowq** コマンドの出力例を示します。

```
Router# show platform lowq
TenGigabitEthernet10/1
Input Queue count:8     Output Queue count:8    Total Queue count:16
```

次の表に、コマンドのフィールドの説明を示します。

フィールド	説明
Input Queue Count	インターフェイス上の入力低優先度キューの数。
Output Queue Count	インターフェイス上の出力低優先度キューの数。
Total Queue Count	入力および出力の低優先度キューの合計。

show platform qos policy-map

ルータに設定されているポリシー マップの種類および数を表示するには、特権 EXEC モードで **showplatformqospolicy-map** コマンドを使用します。

show platform qos policy-map

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(18)SXE	このコマンドが、Cisco Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータに導入されました。
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。

使用上のガイドライン

Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータでは、QoS ポリシー マップをすでに VLAN インターフェイス（**interfacevlan** コマンドで作成された論理インターフェイス）にアタッチしている場合、**matchinputvlan** で Quality of Service（QoS）ポリシー マップをインターフェイスにアタッチすることはできません。両方の種類のサービス ポリシーを使用する場合、ポリシー マップを追加するには、両方の種類のサービス ポリシーを削除する必要があります。

showplatformqospolicy-map コマンドは、ルータが現在 **interfacevlan** サービス ポリシーと **matchinputvlan** サービス ポリシー用に設定されているかどうかを示します。また、種類ごとにポリシー マップの数を示します。

例

次の例は、サービス ポリシーが VLAN インターフェイスにのみ設定されているルータを示しています。

```
Router# show platform qos policy-map

 service policy configured on int vlan: TRUE
 # of int vlan service policy instances: 3
 match input vlan service policy configured: FALSE
 # of match input vlan service policy instances: 0
```

次の例は、サービス ポリシーが VLAN インターフェイスに設定され、**matchinputvlan** でサービス ポリシーを設定したルータを示しています。この設定では、すべてのサービス ポリシーをそれぞれのインターフェイスから削除し、なんらかの種類のみを設定する必要があります。

```
Router# show platform qos policy-map

 service policy configured on int vlan: TRUE
```

```
# of int vlan service policy instances: 1
match input vlan service policy configured: TRUE
# of match input vlan service policy instances: 1
```

次の表では、**showplatformqospolicy-map** コマンドに表示される各フィールドについて説明します。

表 *197 : show platform qos policy-map* のフィールドの説明

フィールド	説明
service policy configured on int vlan	QoS ポリシー マップが VLAN インターフェイスに設定されているかどうかを示します。
# of int vlan service policy instances	VLAN インターフェイスに設定されている QoS ポリシー マップの数。
match input vlan service policy configured	**matchinputvlan** コマンドを使用する QoS ポリシー マップがインターフェイスに設定されているかどうかを示します。
# of match input vlan service policy instances	インターフェイスに設定されている **matchinputvlan** コマンドを使用している QoS ポリシー マップの数。

関連コマンド

コマンド	説明
matchinputvlan	特定の 仮想ローカル エリア ネットワーク（VLAN）ID を持つ着信パケットに一致するクラス マップを設定します。
matchqos-group	一致基準として特定の QoS グループ値を指定します。
mlsqostrust	保存する必要があるパケットの着信 QoS フィールドを決めるために、インターフェイスの信頼状態を設定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

コマンド	説明
showplatformqospolicy-map	ルータに設定されているポリシーマップのタイプと数を表示します。

show platform software infrastructure punt statistics

キューベースのパント ポリシングが有効になっているかどうかを表示するには、特権 EXEC モードで **show platform software infrastructure punt statistics** コマンドを使用します。

show platform software infrastructure punt 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

無効（パント ポリシング統計設定に関する情報は表示されません）。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.5S	このコマンドが、Cisco ASR 903 ルータに追加されました。

使用上のガイドライン

キュー上でキューベースのパント ポリシングが有効になっていることを検証するには、**show platform software infrastructure punt statistics** コマンドを使用します。この機能がインターフェイスで設定されている場合、コマンド出力にパント ポリシング統計情報が表示されます。

例

次に、**show platform software infrastructure punt statistics** コマンドの出力例を示します。

```
       Router# show platform software infrastructure punt statistics
UEA Punt Statistics

Global drops : 0

 Queue Name              | Rx count                   |  Drop count
-------------------------+----------------------------+-----------------------
 SW FORWARDING Q         | 0                          | 0
 ROUTING PROTOCOL Q      | 0                          | 0
 ICMP Q                  | 0                          | 0
 HOST Q                  | 57115                      | 0
 ACL LOGGING Q           | 0                          | 0
 STP Q                   | 0                          | 0
 L2 PROTOCOL Q           | 6571                       | 0
 MCAST CONTROL Q         | 208839                     | 0
 BROADCAST Q             | 4                          | 0
 REP Q                   | 0                          | 0
 CFM Q                   | 0                          | 0
 CONTROL Q               | 0                          | 0
 IP MPLS TTL Q           | 0                          | 0
 DEFAULT MCAST Q         | 0                          | 0
 MCAST ROUTE DATA Q      | 0                          | 0
 MCAST MISMATCH Q        | 0                          | 0
 RPF FAIL Q              | 0                          | 0
 ROUTING THROTTLE Q      | 87                         | 0
 MCAST Q                 | 0                          | 0
```

```
MPLS OAM Q              | 0                          | 0
IP MPLS MTU Q           | 0                          | 0
PTP Q                   | 0                          | 0
LINUX ND Q              | 0                          | 0
KEEPALIVE Q             | 0                          | 0
ESMC Q                  | 0                          | 0
FPGA BFD Q              | 0                          | 0
FPGA CCM Q              | 0                          | 0
FPGA CFE Q              | 0                          | 0
L2PT DUP Q              | 0                          | 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 *198 : show platform software infrastructure punt statistics* フィールドの説明

フィールド	説明
Queue Name	キューの名前。
Rx count	指定したキューの受信パケットの数。
Drop count	指定したキューのドロップされたパケットの数。

関連コマンド

コマンド	説明
platform punt-police queue	キューのパント ポリシングを有効にし、キュー単位で最大パント レートおよびバースト レートを指定します。
show platform hardware pp active infrastructure pi npd rx policer	すべてのキューのパント ポリシング統計情報を表示します。

show policy-manager events

ポリシー マネージャ イベント統計情報に関する詳細情報を表示するには、特権 EXEC モードで **showpolicy-managerevents** コマンドを使用します。

show policy-manager events

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(1)	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズ ルータで実装されました。

例

次に、**showpolicy-managerevents** コマンドの出力例を示します。

```
Router# show policy-manager events
Event Statistics
0          catastrophic
0          critical
0          high
0          medium
0          low
0          positive
The following events were discarded
0          unknown
Event buffer pool
Number of free event buffers = 300
Number of events awaiting processing by Policy Manager process = 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 *199 : show policy-manager events* フィールドの説明

フィールド	説明
catastrophic	壊滅的状態にあるイベントの合計数を表示します。
critical	重大状態にあるイベントの合計数を表示します。
high	重大度が高い状態のイベントの合計数を表示します。

フィールド	説明
medium	重大度が中程度の状態にあるイベントの合計数を表示します。
low	重大度が低い状態にあるイベントの合計数を表示します。
positive	安全なイベントの合計数を表示します。
Number of free event buffers	空いているイベント バッファの合計数を表示します。
Number of events awaiting processing by Policy Manager process	ポリシー マネージャによってまだ処理されていないイベントの数を表示します。

関連コマンド

コマンド	説明
showpolicy-managerpolicy	ポリシーマネージャのさまざまなポリシーを表示します。
showpolicy-managersubsystem	ポリシー マネージャのサブシステムを表示します。

show policy-manager policy

ポリシー マネージャ ポリシー データベースに関する情報を表示するには、特権 EXEC モードで **showpolicy-managerpolicy** コマンドを使用します。

Cisco IOS SX、T、および XE Trains
show policy-manager policy [{*policy-id*|**detail**|**subsystem** *subsystem-name* [{**detail**|**policy-name** *name*}]}]

Cisco IOS SR Train
show policy-manager policy [{*policy-id*|**detail**|**event-id**|**policy-id**|**subsystem** *subsystem-name* [{**detail**|**policy-name** *name*}]}]

構文の説明

policy-id	（任意）指定されたポリシー ID を持つポリシーに関する情報を表示します。指定できる範囲は 1 ～ 4294967295 です。
detail	（任意）詳細なポリシー データベース情報を表示します。
subsystem	（任意）指定されたサブシステムに関する情報を表示します。
subsystem-name	（任意）サブシステムの名前。
policy-name	（任意）指定されたポリシーに関する情報を表示します。
name	（任意）ポリシーの名前。
event-id	（任意）イベント ID テーブルに関する情報を表示します。
policy-id	（任意）ポリシー ID テーブルに関する情報を表示します。

コマンド デフォルト

引数やキーワードを指定しないと、すべてのポリシーに関する情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(24)T	このコマンドは、Cisco IOS Release 12.4(24)T よりも前のリリースに導入されました。
12.2(33)SRC	このコマンドは、変更され、Cisco IOS Release 12.2(33)SRC よりも前のリリースに統合されました。**event-id** キーワードおよび **policy-id** キーワードが追加されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI. よりも前のリリースに統合されました。

リリース	変更箇所
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。

例

次は、**showpolicy-managerpolicy** コマンドの出力例です。フィールドの説明は自明です。

```
Router# show policy-manager policy
Status (S) codes:
A = active
D = deactivated
S ID    Subsystem                Name
```

関連コマンド

コマンド	説明
showpolicy-managerevents	ポリシー マネージャ イベント統計情報に関する詳細な情報を表示します。
showpolicy-managersubsystem	ポリシー マネージャのサブシステムを表示します。

show policy-map

指定されたサービス ポリシー マップのすべてのクラスまたは既存のポリシー マップのすべてのクラスの設定を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showpolicy-map** コマンドを使用します。

show policy-map [*policy-map*]

構文の説明

policy-map	（任意）全設定を表示するサービス ポリシー マップの名前最大 40 文字までの名前を指定できます。

コマンド デフォルト

すべての既存のポリシー マップ コンフィギュレーションが表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。
12.0(7)S	このコマンドが、Cisco IOS Release 12.0(7)S に統合されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.2(4)T	2 レート トラフィック ポリシングに対してバースト パラメータおよび関連付けられたアクションを表示するようにこのコマンドは変更されました。
12.2(8)T	このコマンドは、Policer Enhancement（Multiple Actions 機能）および重み付けランダム早期検出（WRED）（明示的輻輳通知（ECN）機能）のために変更されました。
12.2(13)T	次の点が変更されました。 • パーセントベース ポリシングおよびシェーピング機能のために出力が変更されました。 • このコマンドはモジュラ QoS コマンドライン インターフェイス（MQC）無条件パケット廃棄機能の一部として変更されました。トラフィック クラスは、特定のクラスに属するパケットを廃棄するように設定されます。 • このコマンドは、拡張パケット マーキング機能のために変更されました。マッピング テーブル（テーブルマップ）を使用して、packet-marking の値を変換し、送信できます。

リリース	変更箇所
12.2(15)T	フレーム リレーの音声適応トラフィック シェーピング情報の表示をサポートするように変更されました。
12.0(28)S	このコマンドの出力が変更され、QoS（パーセントベース ポリシング機能）が、認定（適合）バースト サイズ（bc）および超過（ピーク）バースト サイズ（be）をミリ秒（ms）単位で表示するようになりました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
12.2(28)SB	このコマンドは Cisco IOS Release 12.2(28)SB に統合され、レイヤ 2 トンネル プロトコル バージョン 3（L2TPv3）トンネル マーキングに関する情報を表示するように変更されました。
12.2(31)SB2	このコマンドは、トラフィック クラスに関して設定された帯域幅残量割合および ATM オーバーヘッド アカウンティングを表示するように機能拡張され、Cisco 10000 シリーズ ルータ PRE3 に実装されました。
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。
12.2(33)SRC	Cisco 7600 シリーズ ルータのサポートが追加されました。
12.4(15)T2	このコマンドは、Generic Routing Encapsulation（GRE）トンネル マーキングに関する情報を表示するように変更されました。 （注） このリリースの場合、Cisco MGX ルート プロセッサ モジュール（RPM-XF）プラットフォームだけで GRE トンネル マーキングがサポートされます。
12.2(33)SB	このコマンドは、GRE トンネル マーキングに関する情報を表示するように変更され、Cisco 7300 シリーズ ルータのサポートが追加されました。このコマンドの出力は、PRE3 用と PRE4 用の Cisco 10000 シリーズ ルータで変更されました。
Cisco IOS XE 2.1	このコマンドは Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ ルータ上に実装されました。
12.4(20)T	このコマンドが変更されました。モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）を使用した階層型キューイング フレームワーク（HQF）のサポートが追加されました。

使用上のガイドライン

showpolicy-map コマンドは、**policy-map** コマンドを使用して作成されたポリシー マップの設定を表示します。ポリシー マップがインターフェイスに付加されているかどうかにかかわら

ず、**showpolicy-map** コマンドを使用して、既存のサービス ポリシー マップを構成するすべてのクラス設定を表示できます。コマンドは次を表示します。

- インターフェイスで ECN がイネーブルである場合にかぎり、ECN マーキング情報。
- 輻輳時にクラスキューに割り当てるために未使用（過剰）帯域幅の量を計算するように設定および使用されている場合は、帯域幅残量割合設定および統計情報。

Cisco 10000 シリーズ ルータ

Cisco IOS リリース 12.2(33)SB では、ポリシーが階層型ポリシーの場合、show policy-map コマンドの出力が以前のリリースのものとは若干異なります。

たとえば、Cisco IOS リリース 12.2(33)SB では、show policy-map コマンドで階層型ポリシーを指定すると、出力が次のように表示されます。

```
Router# show policy-map Bronze
policy-map bronze
 class class-default
 shape average 34386000
 service-policy Child
```

Cisco IOS リリース 12.2(31)SB では、show policy-map コマンドで階層型ポリシーを指定すると、出力が次のように表示されます。

```
Router# show policy-map Gold
policy-map Gold
 Class class-default
 Average Rate Traffic Shaping
 cir 34386000 (bps)
 service-policy Child2
```

Cisco IOS リリース 12.2(33)SB の場合、show policy-map コマンドの出力には、次の出力例に示すように、ポリシング アクションが個別の行に表示されます。

```
Router# show policy-map Premium
Policy Map Premium
 Class P1
 priority
 police percent 50 25 ms 0 ms
 conform-action transmit
 exceed-action transmit
 violate-action drop
```

Cisco IOS リリース 12.2(31)SB の場合、show policy-map コマンドの出力には、次の出力例に示すように、ポリシング アクションが 1 つの行に表示されます。

```
Router# show policy-map Premium
Policy Map Premium
 Class P2
 priority
 police percent 50 25 ms 0 ms conform-action transmit exceed-action transmit violate-
action drop
```

例

このセクションでは、代表的な**showpolicy-map**コマンドの出力例を示します。使用されるインターフェイスまたはプラットフォーム、および、イネーブルにされたオプション（Weighted Fair Queueing（WFQ）など）によって、表示される出力は次に示すものと若干異なります。

重み付け均等化キューイング：例

次に、po1 という名前のサービス ポリシー マップの内容を表示する例を示します。この例では、WFQ は有効になっています。

```
Router# show policy-map po1
Policy Map po1
 Weighted Fair Queueing
    Class class1
       Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class5
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class6
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class7
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class8
         Bandwidth 937 (kbps)  Max thresh 64 (packets)
```

次に、ルータ上のすべてのポリシー マップの内容を表示する例を示します。ここでも、WFQ は有効になっています。

```
Router# show policy-map

Policy Map poH1
 Weighted Fair Queueing
    Class class1
       Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class5
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class6
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class7
Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class8
         Bandwidth 937 (kbps)  Max thresh 64 (packets)
Policy Map policy2
 Weighted Fair Queueing
    Class class1
       Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 300  (kbps)  Max thresh 64 (packets)
    Class class3
```

```
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class5
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class6
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
```

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 *200 : show policy-map* フィールドの説明：*WFQ* 用に設定

フィールド	説明
Policy Map	ポリシー マップ名です。
Class	クラス名。
Bandwidth	クラスに割り当てる帯域幅の量（kbps 単位）。
Max thresh	パケット数での最大しきい値。

フレームリレー音声適応型トラフィック シェーピング：例

次の **show-policymap** コマンドの出力例は、フレームリレー音声適応型トラフィック シェーピングがポリシーマップ MQC-SHAPE-LLQ1 の class-default クラスに設定され、非アクティブ化タイマーが 30 秒に設定されていることを示しています。

```
Router# show policy-map
  Policy Map VSD1
    Class VOICE1
      Strict Priority
      Bandwidth 10 (kbps) Burst 250 (Bytes)
    Class SIGNALS1
      Bandwidth 8 (kbps) Max Threshold 64 (packets)
    Class DATA1
      Bandwidth 15 (kbps) Max Threshold 64 (packets)
  Policy Map MQC-SHAPE-LLQ1
    Class class-default
      Traffic Shaping
         Average Rate Traffic Shaping
                 CIR 63000 (bps) Max. Buffers Limit 1000 (Packets)
                 Adapt to 8000 (bps)
                 Voice Adapt Deactivation Timer 30 Sec
      service-policy VSD1
```

（注） Cisco IOS リリース 12.4(20)T では、ポリシー マップで設定されたインターフェイスがきわめて混雑している場合、各トラフィック クラスの帯域幅ステートメントの定義に従って暗黙的なポリサーがトラフィックを許可します。

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 *201 : show policy-map* フィールドの説明：フレームリレー音声適応型トラフィック シェーピング用に設定

フィールド	説明
Strict Priority	このクラスのトラフィックに割り当てられたキューイングの優先順位を示します。
Burst	トラフィック バースト サイズ（バイト）を指定します。
Traffic Shaping	トラフィック シェーピングが有効になっていることを示します。
Average Rate Traffic Shaping	有効なトラフィック シェーピングの種類を示します。選択肢は、[ピーク レート トラフィック シェーピング（Peak Rate Traffic Shaping）] または [平均レート トラフィック シェーピング（Average Rate Traffic Shaping）] です。
CIR	設定情報レート（CIR）（bps）。
Max. Buffers Limit	最大メモリ バッファ サイズ（パケット単位）。
Adapt to	シェーピングがアクティブな場合のトラフィック レート。
Voice Adapt Deactivation Timer	フレームリレー音声適応型トラフィック シェーピングが設定され、非アクティブ化タイマーが 30 秒に設定されていることを示します。
service-policy	ポリシー マップ「MQC-SHAPE-LLQ1」に設定されているサービス ポリシーの名前。

トラフィック ポリシング：例

次は、**showpolicy-map** コマンドのサンプル出力です。この出力例は、policy1 というポリシー マップの内容を示しています。policy 1 では、設定情報レート（CIR）に基づくトラフィック ポリシングが 20 パーセントに設定されており、bc および be がミリ秒単位で指定されています。トラフィック ポリシング設定の一部として、オプションの一致（conform）、超過（exceed）、および違反（violate）アクションが指定されています。

```
Router# show policy-map policy1
  Policy Map policy1
    Class class1
     police cir percent 20 bc 300 ms pir percent 40 be 400 ms
       conform-action transmit
       exceed-action drop
       violate-action drop
```

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 *202 : show policy-map* フィールドの説明：トラフィック ポリシング用に設定

フィールド	説明
Policy Map	表示されているポリシー マップの名前
Class	表示されたポリシー マップ内に設定されたクラスの名前
police	帯域幅の割合に基づいたトラフィック ポリシングがイネーブルにされていることを示します。認定バースト（Bc）サイズおよび超過バースト（Be）サイズがミリ秒（ms）単位で設定されており、任意の適合アクション、超過アクションおよび違反アクションが指定されています。

2 レート トラフィック ポリシング：例

次に、2 レート トラフィック ポリシングが設定されている場合の **showpolicy-map** コマンドの出力例を示します。次のように、police というクラスに対して 2 レート トラフィック ポリシングが設定されています。そして、police というクラスは policy1 というポリシー マップに設定されています。500 kbps の平均認定レートと 1 Mbps のピーク レートにトラフィックを限定するために、2 レート トラフィック ポリシングが設定されています。

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# interface serial3/0
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
The following sample output shows the contents of the policy map called policy1 :
Router# show policy-map policy1

 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
   transmit exceed-action set-prec-transmit 2 violate-action drop
```

平均認定レート（500 kbps）に準拠するとしてマークされたトラフィックは、そのまま送信されます。500 kbps を超過しているものの 1 Mbps は超過していないとマークされたトラフィックは、IP precedence 2 でマークされてから送信されます。1 Mbps を超過するすべてのトラフィックは、ドロップされます。バースト パラメータは 10000 バイトに設定されています。

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 *203 : show policy-map* フィールドの説明：*2* レート トラフィック ポリシング用に設定

フィールド	説明
police	**police** コマンドがトラフィック ポリシングを有効にするように設定されていることを示します。また、パケットのマーキングに使用される、指定されたCIR、認定バースト サイズ（bc）、ピーク情報レート（PIR）、および、ピーク バースト（BE）サイズも表示します。
conform-action	指定した比率に適合するパケットに実行されるアクションを表示します。
exceed-action	指定した比率を超えるパケットに実行されるアクションを表示します。
violate-action	指定した比率に違反するパケットに実行されるアクションを表示します。

複数トラフィック ポリシング アクション：例

次に、Policer Enhancement（Multiple Actions 機能）が設定されている場合の **showpolicy-map** コマンドの出力例を示します。次の **showpolicy-map** コマンドの出力例には、「police」というサービス ポリシーの設定が表示されています。このサービス ポリシーでは、トラフィック ポリシングは、例に示した CIR または PIR に適合、超過、または違反としてマークされたパケットに対して複数のアクションを許可するように設定されています。

```
Router# show policy-map police
  Policy Map police
    Class class-default
     police cir 1000000 bc 31250 pir 2000000 be 31250
       conform-action transmit
       exceed-action set-prec-transmit 4
       exceed-action set-frde-transmit
       violate-action set-prec-transmit 2
       violate-action set-frde-transmit
```

指定されたCIR（1,000,000 bps）に適合しているパケットは適合パケットとしてマーキングされます。これらは変更なしに送信されます。

指定されたCIRを超過しているが、指定されたPIR（2,000,000 bps）を超えていないパケットは、超過パケットとしてマーキングされます。これらのパケットは、IP precedence レベルが 4 に、Discard Eligibility（DE）ビットが 1 に設定されて送信されます。

指定された PIR を超えているパケットは、違反パケットとしてマーキングされます。これらのパケットは、IP precedence レベルが 2 に、DE ビットが 1 に設定されて送信されます。

（注） アクションは、**police** コマンドの *action* 引数を使用して指定されます。使用可能なアクションの詳細については、**police** コマンドのリファレンス ページを参照してください。

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 *204 : show policy-map* フィールドの説明：複数のトラフィック ポリシング アクション用に設定

フィールド	説明
police	**police** コマンドがトラフィック ポリシングを有効にするように設定されていることを示します。また、パケットのマーキングに使用される、指定されたCIR、BC、PIR、および、BE も表示します。
conform-action	指定した比率に適合するパケットに実行されるアクションを表示します。
exceed-action	指定した比率を超えるパケットに実行されるアクションを表示します。
violate-action	指定した比率に違反するパケットに実行されるアクションを表示します。

明示的輻輳通知：例

次に、WRED - 明示的輻輳通知（ECN）機能が設定されている場合の **showpolicy-map** コマンドの出力例を示します。出力に含まれる「explicit congestion notification」という語（および ECN マーキング情報）は ECN が有効になっていることを示します。

```
Router# show policy-map
   Policy Map pol1
     Class class-default
       Weighted Fair Queueing
             Bandwidth 70 (%)
             exponential weight 9
             explicit congestion notification
             class    min-threshold    max-threshold    mark-probability
             ------------------------------------------------------------
             ------------------------------------------------------------

             0        -                -                1/10
             1        -                -                1/10
             2        -                -                1/10
             3        -                -                1/10
             4        -                -                1/10
             5        -                -                1/10
             6        -                -                1/10
             7        -                -                1/10
             rsvp     -                -                1/10
```

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 *205 : show policy-map* フィールドの説明：*ECN* 用に設定

フィールド	説明
explicit congestion notification	明示的輻輳通知がイネーブルであることを示します。
class	IP precedence 値
min-threshold	最小しきい値を表します。パケット数の WRED 最小しきい値。
max-threshold	最大しきい値を表します。パケット数の WRED 最大しきい値。

フィールド	説明
mark-probability	平均キューの深さが最大しきい値の場合にドロップされたパケットの割合。

モジュラ QoS CLI（MQC）の無条件パケット廃棄：例

次の例では、policy1 というポリシー マップの内容を表示しています。c1 というクラスに属するすべてのパケットが破棄されます。

```
Router# show policy-map
 policy1
 Policy Map policy1
  Class c1
   drop
```

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 *206 : show policy-map* フィールドの説明：*MQC* 無条件パケット廃棄用に設定

フィールド	説明
Policy Map	表示されているポリシー マップの名前
Class	表示されているポリシー マップ内のクラスの名前
drop	指定したクラスに属するすべてのパケットに対してパケット廃棄処理が設定されていることを示します。

パーセントベース ポリシングおよびシェーピング：例

次の例では、2 つのサービス ポリシー マップの内容を表示しています。1 つは policy1 で、もう 1 つは policy2 です。policy1 では、50% という CIR に基づいてトラフィック ポリシングが設定されています。policy2 では、35% という平均レートに基づいてトラフィック シェーピングが設定されています。

```
Router# show policy-map policy1
Policy Map policy1
 class class1
    police cir percent 50
Router# show policy-map policy2
Policy Map policy2
 class class2
    shape average percent 35
```

次の例では、po1 というサービス ポリシー マップの内容を表示しています。

```
Router# show policy-map po1
Policy Map po1
 Weighted Fair Queueing
    Class class1
Bandwidth 937 (kbps) Max thresh 64 (packets)
```

```
    Class class2
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
```

次に、ルータ上のすべてのポリシー マップの内容を表示する例を示します。

```
Router# show policy-map

Policy Map poH1
 Weighted Fair Queueing
    Class class1
       Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
Policy Map policy2
 Weighted Fair Queueing
    Class class1
       Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 300  (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
```

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 *207 : show policy-map* フィールドの説明：パーセントベース ポリシングおよびシェーピング用に設定

フィールド	説明
Policy Map	表示されているポリシー マップの名前
Weighted Fair Queueing	Weighted Fair Queueing（WFQ）がイネーブルにされていることを示します。
Class	表示されたポリシー マップ内に設定されたクラスの名前
Bandwidth	このクラスに設定された帯域幅（単位：kbps）
Max threshold	最大しきい値を表します。パケット数の WRED 最大しきい値。

拡張パケット マーキング：例

showpolicy-map コマンドの次の出力例では、policy1 および policy2 というポリシー マップの設定を表示しています。

policy1 では、table-map-cos1 というテーブル マップがサービス クラス（CoS）値に基づいて優先順位を決定するように設定されています。ポリシー マップ policy1 は、

table-map-cos1 というテーブル マップに定義されているパケット マーキングを変換して伝播します。

showpolicy-map コマンドの次の出力例では、policy1 および policy2 というサービス ポリシーの設定を表示しています。policy1 では、table-map1 というテーブル マップが CoS 値に従って優先順位を決定するように設定されています。policy2 では、table-map2 というテーブルマップが優先順位値に従って CoS 値を決定するように設定されています。

```
Router# show policy-map policy1
  Policy Map policy1
    Class class-default
      set precedence cos table table-map1
Router# show policy-map policy2
   Policy Map policy2
    Class class-default
      set cos precedence table table-map2
```

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。

表 *208 : show policy-map* フィールドの説明：拡張パケット マーキング用に設定

フィールド	説明
Policy Map	表示されているポリシー マップの名前
Class	表示されているポリシー マップ内のクラスの名前
set precedence cos table table-map1 または set cos precedence table table-map2	指定された値を設定するために使用する set コマンドの名前。 たとえば、set precedence cos table-map1 は、table-map1 というテーブル マップがテーブル マップに定義されている値に基づいて優先順位値を設定するように設定されていることを示しています。 また、set cos table table-map2 は、table-map2 というテーブル マップがテーブル マップに定義されている値に基づいて CoS 値を設定するように設定されていることを示しています。

帯域幅残量割合：例

次に、vlan10_policy という名前のポリシーマップの class-default クラスの帯域幅残量割合が 10 であることを示す show policy-map コマンドの出力例を示します。輻輳が発生すると、スケジューラは class-default トラフィックに他のサブインターフェイスに関して割り当てられている未使用の帯域幅の 10 倍を割り当てます。

```
Router# show policy-map vlan10_policy
  Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 10
      service-policy child_policy
```

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。

表 *209 : show policy-map* フィールドの設定：帯域幅残量割合用に設定

フィールド	説明
Policy Map	表示されているポリシー マップの名前
Class	表示されているポリシー マップ内のクラスの名前
Average Rate Traffic Shaping	平均レート トラフィック シェーピングが設定されていることを示します。
cir	トラフィックのシェーピングに使用される認定情報レート（CIR）
bandwidth remaining ratio	超過帯域幅の割り当てに使用される比率を示します。

ATM オーバーヘッド アカウンティング：例

show policy-map コマンドの次の出力例は、ATM オーバーヘッド アカウンティングが class-default クラスに対して有効であることを示しています。BRAS-DSLAM カプセル化は dot1q で、加入者カプセル化は AAL5 サービスの snap-rbe です。

```
Policy Map unit-test
Class class-default
Average Rate Traffic Shaping
cir 10% account dot1q aal5 snap-rbe
```

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 *210 : show policy-map* フィールドの説明：*ATM* オーバーヘッド アカウンティング用に設定

フィールド	説明
Average Rate	認定バースト（Bc）は、各間隔で送信される最大ビット数です。
cir 10%	設定情報レート（CIR）は、使用可能なインターフェイス帯域幅の 10% です。
dot1q	BRAS-DSLAM カプセル化は、802.1Q VLAN です。
aal5	DSLAM-CPE カプセル化タイプは、ATM アダプテーション層 5 サービスに基づいています。AAL5 は、コネクション型の可変ビット レート（VBR）サービスをサポートします。
snap-rbe	加入者カプセル化タイプ。

トンネル マーキング：例

この **showpolicy-map** コマンドの出力例では、文字列「ip precedence tunnel 4」はトンネリングされるパケット ヘッダーで IP プレシデンス値を 4 に設定するようにトンネル マーキング（L2TPv3 または GRE）が設定されていることを示しています。

（注） Cisco IOS リリース 12.4(15)T2 では、GRE トンネル マーキングは RPM-XF プラットフォームでのみサポートされています。

```
Router# show policy-map
Policy Map TUNNEL_MARKING
    Class MATCH_FRDE
      set ip precedence tunnel 4
```

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。

表 *211 : show policy-map* フィールドの説明：トンネル マーキング用に設定

フィールド	説明
Policy Map	表示されているポリシー マップの名前
Class	表示されているポリシー マップ内のクラスの名前
set ip precedence tunnel	トンネルマーキングが設定されていることを示します。

HQF：例 1

showpolicy-map コマンドの次の出力例では、test1 というポリシーマップの設定を表示しています。

```
Router# show policy-map test1
  Policy Map test1
    Class class-default
      Average Rate Traffic Shaping
      cir 1536000 (bps)
      service-policy test2
```

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。

表 *212 : show policy-map* フィールドの説明：*HQF* 用に設定

フィールド	説明
Policy Map	表示されているポリシー マップの名前
Class	表示されているポリシー マップ内のクラスの名前
Average Rate Traffic Shaping	平均レート トラフィック シェーピングが設定されていることを示します。
cir	設定情報レート（CIR）（bps）。
service-policy	ポリシーマップ「test1」に設定されているサービス ポリシーの名前。

HQF：例 2

showpolicy-map コマンドの次の出力例では、test2 というポリシー マップの設定を表示しています。

```
Router# show policy-map test2
  Policy Map test2
    Class RT
      priority 20 (%)
    Class BH
      bandwidth 40 (%)
      queue-limit 128 packets
    Class BL
      bandwidth 35 (%)
       packet-based wred, exponential weight 9

      dscp    min-threshold    max-threshold    mark-probablity
      ------------------------------------------------------------
      af21 (18)     100              400              1/10
      default (0)   -                -                1/10
```

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。

表 *213 : show policy-map* フィールドの説明：*HQF* 用に設定

フィールド	説明
Policy Map	表示されているポリシー マップの名前
Class	表示されているポリシー マップ内のクラスの名前
Average Rate Traffic Shaping	平均レート トラフィック シェーピングが設定されていることを示します。
priority	このクラスのトラフィックに割り当てられたキューイングの優先順位のパーセンテージを示します。
bandwidth	このクラスのトラフィックに割り当てられた帯域幅比率を示します。
queue-limit	このトラフィック クラスのパケットにおけるキュー制限を示します。
packet-based wred, exponential weight	ランダム検出が適用され、使用される単位がパケットであることを示します。指数加重は、WRED で使用される平均キュー サイズを計算するための係数です。

フィールド	説明
dscp	DiffServ コード ポイント（DSCP）。有効な値は次のとおりです。 • 0 ～ 63：DSCP の数値。デフォルト値は 0 です。 • af1 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）プレシデンス値。 • default：デフォルト DSCP 値。 • ef：Expedited Forwarding（EF; 完全優先転送）DSCP 値。
min-threshold	最小しきい値を表します。パケット数の WRED 最小しきい値。
max-threshold	最大しきい値を表します。パケット数の WRED 最大しきい値。
mark-probability	平均キューの深さが最大しきい値の場合にドロップされたパケットの割合。

関連コマンド

Command	Description
bandwidth	ポリシーマップに属するクラスに対して割り当てられる帯域幅を指定、または変更し、ATM オーバーヘッドアカウンティングをイネーブルにします。
bandwidthremainingratio	未使用の帯域幅の量を計算して、輻輳時にキューに割り当てるために、クラス キューおよびサブインターフェイス レベル キューの帯域幅残量割合を指定します。
class(policymap)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定します。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
drop	特定のクラスに属するパケットを廃棄するトラフィック クラスを設定します。
police	トラフィック ポリシングを設定します。
police(tworates)	2 レート、CIR および PIR を使用してトラフィック ポリシングを設定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
random-detectecn	ECN をイネーブルにします。

Command	Description
shape	指定されたアルゴリズムに従って指示されたビット レートにトラフィックをシェーピングし、ATM オーバーヘッド アカウンティングをイネーブルにします。
showpolicy-mapclass	指定されたポリシー マップの指定されたクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。
showrunning-config	ルータの現在の設定を表示します。設定すると、コマンド出力にATMオーバーヘッドアカウンティングに関する情報が含まれます。
showtable-map	指定されたテーブルマップまたはすべてのテーブルマップの設定を表示します。
table-map(valuemapping)	1 つの packet-marking 値を別の値にマッピングおよび変換するための、マッピング テーブルを作成します。

show policy-map class

指定したポリシー マップの指定したクラスの設定を表示するには、EXEC モードで **showpolicy-mapclass** コマンドを使用します。

show policy-map *policy-map* **class** *class-name*

構文の説明

policy-map	表示するクラス設定が含まれているポリシーマップの名前。
class-name	設定を表示するクラスの名前。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。
12.0(7)S	このコマンドが、Cisco IOS Release 12.0(7)S に統合されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
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。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

showpolicy-mapclass コマンドを使用すると、任意のサービス ポリシー マップについて、そのサービス ポリシー マップがインターフェイスにアタッチされているかどうかにかかわらず、単一のクラス設定を表示できます。

例

次に、po1 というポリシー マップに属する class7 というクラスの設定を表示する例を示します。

```
Router# show policy-map po1 class class7


Class class7
 Bandwidth 937 (kbps) Max Thresh 64 (packets)
```

関連コマンド

Command	Description
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

show policy-map control-plane

集約または分散コントロール プレーン サービス用にコントロール プレーンにアタッチされたポリシー マップ内のあるトラフィック クラスまたはすべてのトラフィック クラスについて設定および統計情報を表示するには、特権 EXEC モードで **showpolicy-mapcontrol-plane** コマンドを使用します。

Cisco 3660、3800、7200、7400、および 7500 シリーズ ルータ
show policy-map control-plane [**type policy-type**] [{**all**|**slot** *slot-number*}] [{**host**|**transit**|**cef-exception**}] [{**input** [**class** *class-name*]|**output** [**class** *class-name*]}]

Cisco 7600 および ASR 1000 シリーズ ルータ
show policy-map control-plane [all] [{**input** [**class** *class-name*]|**output** [**class** *class-name*]}]

構文の説明

type *policy-type*	（任意）目的の統計情報があるポリシー マップ タイプ（たとえば、ポート フィルタやキューのしきい値）を指定します。
all	（任意）集約および分散コントロール プレーン（CP）サービスで使用される QoS コントロール プレーン ポリシーをすべて表示します。
slot *slot-number*	（任意）指定されたライン カード上で分散 CP サービスを実行するのに使用される Quality of Service（QoS）ポリシーに関する情報を表示します。
host	（任意）ホスト サブインターフェイスのポリシー マップおよびクラス マップ統計情報を表示します。
transit	（任意）中継サブインターフェイスのポリシー マップおよびクラス マップ統計情報を表示します。
cef-exception	（任意）CEF 例外サブインターフェイスのポリシーマップおよびクラスマップ統計情報を表示します。
input	（任意）適用されている入力ポリシーの統計情報を表示します。
output	（任意）付加された出力ポリシーの統計を表示します。 （注） output キーワードは、Cisco IOS リリース 12.3(4)T およびそれ以降の Cisco IOS 12.3T リリースでのみサポートされています。
class *class-name*	（任意）設定および統計情報を表示するクラスの名前。

コマンド デフォルト

コントロール プレーンのポリシー マップに属するすべてのクラスについて情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(18)S	このコマンドが導入されました。
12.3(4)T	このコマンドが、Cisco IOS Release 12.3(4)T に統合されました。**output** キーワードのサポートが追加されました。
12.0(29)S	このコマンドが、Cisco IOS Release 12.0(29)S に統合されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
12.0(30)S	分散 CP サービスをサポートするために **slot***slot-number* パラメータが追加されました。
12.4(4)T	**type***policy-type* キーワードと引数の組み合わせ、および **host**、**transit**、**cef-exception** の各キーワードのサポートが追加されました。
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。
Cisco IOS XE Release 2.2	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

showpolicy-mapcontrol-plane コマンドは、集約および分散コントロール プレーン ポリシング サービスの情報を表示します。このサービスは、ルート プロセッサのプロセス レベルに送信されるコントロール プレーン（CP）パケットの数またはレートを管理します。

指定されたラインカードについて分散コントロールプレーンサービスの情報が表示されます。分散 CP サービスは、ライン カードの分散スイッチ エンジンで実行され、ライン カード上のすべてのインターフェイスから集約 CP サービス（ルータ上のすべてのライン カードから受信した CP パケットの場合）が実行されているルート プロセッサに送信された CP トラフィックを管理します。

例

次に、ポリシー マップ TEST がコントロール プレーンに関連付けられている例を示します。このポリシー マップでは、クラス マップ TEST と一致するトラフィックはポリシングされますが、それ以外のすべてのトラフィック（「class-default」というクラス マップと一致するトラフィック）はそのまま通過することが許可されます。

```
Router# show policy-map control-plane

Control Plane
Service-policy input:TEST
Class-map:TEST (match-all)
      20 packets, 11280 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:access-group 101
      police:
        8000 bps, 1500 limit, 1500 extended limit
        conformed 15 packets, 6210 bytes; action:transmit
        exceeded 5 packets, 5070 bytes; action:drop
        violated 0 packets, 0 bytes; action:drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map:class-default (match-any)
```

```
105325 packets, 11415151 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match:any
```

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 *214 : show policy-map control-plane* のフィールドの説明

フィールド	説明
クラスまたはサービス ポリシーに関連付けられたフィールド	
Service-policy input	コントロールプレーンに適用される入力サービス ポリシーの名前（このフィールドには、出力サービス ポリシーが設定されていればそれも表示されます。）
Class-map	表示されるトラフィックのクラス。トラフィックは、設定されるクラスごとに表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
offered rate	パケットがクラスに着信するレート（kbps）
drop rate	クラスからパケットがドロップされるレート（単位：kbps）。ドロップ レートは、offered rate から正常に送信されたパケット数を引いて計算されます。
Match	指定したトラフィック クラスの一致基準。 使用可能なさまざまな一致基準オプションの詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Applying QoS Features Using the MQC」モジュールを参照してください。
トラフィック ポリシングに関連付けられたフィールド	
police	**police** コマンドがトラフィック ポリシングを有効にするように設定されていることを示します。
conformed	指定したレートに適合するパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。
exceeded	指定したレートを超えるパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。

フィールド	説明
violated	指定したレートに違反するパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。

関連コマンド

コマンド	説明
control-plane	コントロール プレーン コンフィギュレーション モードで、コントロール プレーン宛てのトラフィックをポリシングする QoS ポリシーを適用します。
service-policy(control-plane)	集約コントロール プレーン サービスまたは分散コントロール プレーン サービス用に、ポリシー マップをコントロール プレーンにアタッチします。

show policy-map interface

インターフェイスに付加された入力ポリシーおよび出力ポリシーの統計情報と設定を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show policy-map interface** コマンドを使用します。

非同期転送モード（ATM）共有ポート アダプタ（SPA）
show policy-map interface *slot/subslot/port* **.**[*subinterface*]

Cisco CMTS ルータ
show policy-map interface *interface-type slot/subslot/port*

Cisco 3660、3845、7200、7400、7500、Cisco ASR 903 シリーズ ルータ、および Cisco ASR 1000 シリーズ ルータ
show policy-map interface *type type-parameter* [**vc** [*vpi*]**[/]***vci*] [**dlci** *dlci*] [{**input**|**output**}] [**class** *class-name*]

Cisco 6500 シリーズ スイッチ
show policy-map interface [{*interface-type interface-number*|**vlan** *vlan-id*}] **[detailed]** [{**input**|**output**} [**class** *class-name*]]
show policy-map interface [**port-channel** *channel-number* [**class** *class-name*]]

Cisco 7600 シリーズ ルータ
show policy-map interface [{*interface-type interface-number*|**null 0**|**vlan** *vlan-id*}] [{**input**|**output**}]

構文の説明

slot	（CMTS および ATM 共有ポート アダプタのみ）シャーシ スロット番号。スロット情報については該当するハードウェア マニュアルを参照してください。SPA インターフェイス プロセッサ（SIP）については、プラットフォーム固有の SPA ハードウェア インストレーション ガイドまたはプラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Identifying Slots and Subslots for SIPs and SPAs」トピックを参照してください。
/subslot	（CMTS および ATM 共有ポート アダプタのみ）SPA がインストールされている場合の SPA インターフェイス プロセッサ（SIP）の第 2 スロット番号。サブスロット情報については、プラットフォーム固有の SPA ハードウェア インストレーション ガイドおよびプラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Specifying the Interface Address on an SPA」トピックを参照してください。
port	（CMTS および ATM 共有ポート アダプタのみ）ポート番号またはインターフェイス番号。ポート情報については該当するハードウェア マニュアルを参照してください。SPA については、プラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Specifying the Interface Address」トピックを参照してください。

.subinterface	（ATM 共有ポート アダプタのみ、任意）サブインターフェイス番号。期間に優先する番号は、このサブインターフェイスが属する番号に一致する必要があります。指定できる範囲は 1 ～ 4,294,967,293 です。
type	ポリシー設定が表示されるサブインターフェイスのインターフェイス タイプ。
type-parameter	インターフェイス タイプまたはサブインターフェイス タイプに関連付けられたポート、コネクタ、インターフェイス カード番号、クラス マップ名やその他のパラメータ。
vc	（任意）ATM インターフェイスの場合にだけ、指定された PVC のポリシー設定を表示します。
vpi /	（任意）この相手先固定接続（PVC）の ATM ネットワーク仮想パス識別子（VPI）。Cisco 7200 および 7500 シリーズ ルータで、この値範囲は 0 ～ 255 です。 *vpi* および *vci* 引数は両方を 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。 前方スラッシュ（/）と *vpi* 値の両方がない場合、*vpi* 値のデフォルトは 0 です。この値が省略されたときは、指定された ATM インターフェイスまたはサブインスタンスの仮想回線（VC）の情報が表示されます。
vci	（任意）この PVC の ATM ネットワーク仮想チャネル識別子（VCI）。この値は 0 ～ 1 の範囲で、**atmvc-per-vp** コマンドによってこのインターフェイスに対して設定された最大値未満です。一般的に、0 ～ 31 の低いほうの値は、特定のトラフィック（F4 Operation, Administration, and Maintenance（OAM）、相手先選択接続（SVC）シグナリング、統合ローカルマネジメントインターフェイス（ILMI）など）のために予約されており、使用できません。 VCI は、ATM セルのヘッダーの 16 ビット フィールドです。VCI 値はローカルにだけ意味があるため、単一リンク上でだけ一意であり、ATM ネットワーク全体では一意ではありません。 *vpi* および *vci* 引数は両方を 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。
dlci	（任意）ポリシー設定が表示される特定の PVC を示します。
dlci	（任意）インターフェイスで使用される、特定のデータリンク接続識別子（DLCI）番号。DLCI が指定された場合、対応する PVC のポリシー設定が表示されます。
input	（任意）入力ポリシーに添付された統計情報が表示されることを示します。
output	（任意）出力ポリシーに添付された統計情報が表示されることを示します。

class *class-name*	（任意）指定したクラスの QoS ポリシー アクションを表示します。
interface-type	（任意）インターフェイス タイプ。有効な値は、**atm**、**ethernet**、**fastethernet**、**ge-wan gigabitethernet**、**pos**、**pseudowire**、および **tengigabitethernet** です。
interface-number	（任意）モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
vlan *vlan-id*	（任意）VLAN ID を指定します。有効値の範囲は 1 ～ 4094 です。
detailed	（任意）その他の統計情報を表示します。
port-channel *channel-number*	（任意）EtherChannel ポートチャネル インターフェイスを表示します。
null0	（任意）null インターフェイスを指定します。有効値は 0 だけです。

コマンド デフォルト

指定されたインターフェイスまたはサブインターフェイス、あるいはそのインターフェイス上の特定の相手先固定接続（PVC）のすべてのサービス ポリシーに設定されているすべてのクラスのパケット統計情報を表示します。

ATM 共有ポート アダプタで使用した場合、このコマンドに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（#）

ATM 共有ポート アダプタ（SPA）

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。
12.0(7)S	このコマンドが、Cisco IOS Release 12.0(7)S に統合されました。
12.0(28)S	このコマンドが変更され、QoS（パーセントベース ポリシング機能）が、認定（適合）バースト（bc）サイズおよび超過（ピーク）バースト（be）サイズを計算する場合にミリ秒を含めるようになりました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。

リリース	変更箇所
12.1(2)T	このコマンドは、インターフェイス上のすべてのフレーム リレー PVC のポリシー、または、DLCI が指定された場合は指定された PVC のポリシーに関する情報を表示するように変更されました。また、このコマンドは、Quality of Service（QoS）設定アクションによってマーキングされたパケットの合計数を表示するように変更されました。
12.1(3)T	このコマンドはクラスごとのアカウンティング統計情報を表示するように変更されました。
12.2(4)T	このコマンドは、2 レート トラフィック ポリシングのために変更され、バースト パラメータと関連するアクションを表示します。
12.2(8)T	このコマンドは、Policer Enhancement（Multiple Actions 機能）および WRED（明示的輻輳通知（ECN）機能）のために変更されました。 Policer Enhancement（Multiple Actions 機能）の場合、このコマンドは特定のレートに対する適合パケット、超過パケットおよび違反パケットに設定された複数のアクションを表示するように変更されました。 WRED（明示的輻輳通知（ECN）機）の場合、このコマンドは ECN マーキング情報を表示します。
12.2(13)T	次の点が変更されました。 • このコマンドは、パーセントベース ポリシング機能とシェーピング機能のために、変更されました。 • このコマンドは、クラスベースの RTP および TCP ヘッダー圧縮のために変更されました。 • このコマンドはモジュラ QoS コマンドライン インターフェイス（MQC）無条件パケット廃棄機能の一部として変更されました。ポリシー マップのトラフィック クラスは、特定のクラスに属するパケットを廃棄するように設定されます。 • このコマンドは、クラスマップ内のトラフィックの一致基準として、フレーム リレー DLCI 番号を表示するように変更されました。 • このコマンドは、クラスマップ内のトラフィックの一致基準として、レイヤ 3 パケット長を表示するように変更されました。 • このコマンドは、拡張パケット マーキング機能のために変更されました。マッピング テーブル（テーブル マップ）を使用して、packet-marking の値を変換し、送信できます。
12.2(14)SX	このコマンドが変更されました。このコマンドのサポートが Cisco 7600 シリーズ ルータに追加されました。

リリース	変更箇所
12.2(15)T	このコマンドは、フレーム リレーの音声適応トラフィック シェーピング情報を表示するように変更されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
12.3(14)T	このコマンドは、帯域幅見積もりパラメータを表示するように変更されました。
12.2(18)SXE	このコマンドが、Cisco IOS Release 12.2(18)SXE に統合されました。このコマンドは、ATM 共有ポート アダプタの集約 WRED 統計情報を表示するように変更されました。構文、デフォルト値、および、コマンド モードが変更されたことに注意してください。これらの変更には、「ATM Shared Port Adapter」のラベルが付けられています。
12.4(4)T	このコマンドが変更されました。Flexible Packet Matching（FPM）をサポートするため、**typeaccess-control** キーワードが追加されました。
12.2(28)SB	このコマンドが Cisco IOS Release 12.2(28)SB に統合され、次の変更が実施されました。 • このコマンドは、フレーム リレーインターフェイスまたは PVC のレガシー QoS パラメータまたは階層型キューイング フレームワーク（HQF）パラメータのいずれかを表示するように変更されました。 • このコマンドは、レイヤ 2 トンネル プロトコル バージョン 3（L2TPv3）トンネル マーキングに関する情報を表示するように変更されました。
12.2(31)SB2	次の点が変更されました。 • このコマンドは、設定されたプライオリティ サービスの各レベルに対する統計情報、および、帯域幅残量割合に関する情報を表示するように拡張され、Cisco 10000 シリーズ ルータ PRE3 に実装されました。 • このコマンドは、VLAN ID 番号に基づく一致パケットの統計情報を表示するように変更されました。Cisco IOS Release 12.2(31)SB2 の時点で、VLAN ID 番号に基づく一致パケットは、Cisco 10000 シリーズ ルータだけでサポートされます。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。

リリース	変更箇所
12.4(15)T2	このコマンドは、Generic Routing Encapsulation（GRE）トンネル マーキングに関する情報を表示するように変更されました。 （注） このリリースの時点で、Cisco MGX ルート プロセッサ モジュール（RPM-XF）プラットフォームだけで GRE トンネル マーキングがサポートされます。
12.2(33)SB	このコマンドは、GRE トンネル マーキングに関する情報を表示するように変更され、Cisco 7300 シリーズ ルータのサポートが追加されました。
Cisco IOS XE 2.1	このコマンドは Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ ルータ上に実装されました。
12.4(20)T	このコマンドが変更されました。モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）を使用した階層型キューイング フレームワーク（HQF）のサポートが追加されました。
12.2(33)SXI	このコマンドは、Catalyst 6500 シリーズ スイッチに実装され、プライオリティ機能の厳密なレベルおよびレベルごとのカウントを表示するように変更されました。
12.2(33)SRE	このコマンドは、MQC ポリシング ポリシー マップで bc 値および be 値をインターフェイスの MTU サイズに自動的に丸めるように変更されました。
Cisco IOS XE Release 2.6	コマンド出力は、サブスクライバ QoS 統計に関する情報を表示するように変更されました。
12.2(54)SG	このコマンドは、ポリサー統計情報の該当するカウントのみを表示するように変更されました。
12.2(33)SCF	このコマンドが、Cisco IOS リリース 12.2(33)SCF に統合されました。
Cisco IOS XE リリース 3.7S	このコマンドが Cisco ASR 903 シリーズ ルータに実装されました。
Cisco IOS XE Release 3.8S	このコマンドが変更されました。*pseudowire* インターフェイス タイプが追加されました。
Cisco IOS XE Release 3.8S	このコマンドが変更されました。Cisco 1000 シリーズ ルータに *pseudowire* インターフェイス タイプが追加されました。
Cisco IOS Release 15.3(1)S	このコマンドが変更されました。*pseudowire* インターフェイス タイプが追加されました。

使用上のガイドライン **Cisco 3660、3845、7200、7400、7500、Cisco ASR 903 シリーズ ルータ、および Cisco ASR 1000 シリーズ ルータ**

show policy-map interface コマンドは、指定されたインターフェイスのクラスのパケット統計情報、または、サービス ポリシーがインターフェイスまたは PVC に付加されている場合にかぎり、指定された PVC のクラスのパケット統計情報を表示します。

show policy-map interface コマンド入力後に表示されたカウンタは、インターフェイス上に輻輳がある場合にだけ更新されます。

show policy-map interface コマンドは、インターフェイスでフレーム リレー トラフィック シェーピング（FRTS）が有効になっている場合にのみ、フレーム リレー PVC に関するポリシー情報を表示します。

show policy-map interface コマンドは、インターフェイスで ECN が有効になっている場合にのみ、ECN マーキング情報を表示します。

HQF でシェーピングがアクティブかどうかを判断するには、**show policy-map interface** コマンド出力の「(queue depth/total drops/no-buffer drops)」行でキューの深さフィールドをチェックします。

Cisco IOS リリース 12.4(20)T 以降の HQF イメージでは、トラフィック シェーピング クラスの遅延パケット カウンタおよび遅延バイト カウンタは削除されました。

Cisco 7600 シリーズ ルータおよび Catalyst 6500 シリーズ スイッチ

pos、atm、および ge-wan インターフェイスは、スーパバイザ エンジン 720 が搭載された Cisco 7600 シリーズ ルータまたは Catalyst シリーズ スイッチではサポートされません。

スーパバイザ エンジン 2 が搭載された Cisco 7600 シリーズ ルータおよび Catalyst 6500 シリーズ スイッチでは、パケット カウンタが表示されます。

スーパバイザ エンジン 720 が搭載された Cisco 7600 シリーズ ルータおよび Catalyst 6500 シリーズ スイッチでは、バイト カウンタが表示されます。

ポリシング済みカウンタ情報は出力されず、代わりに 0 が表示されます（0 パケット、0 バイトなど）。ドロップおよび転送されたポリシング済みカウンタ情報を表示するには、**show mls qos** コマンドを入力します。

Cisco 7600 シリーズ ルータでは、OSM WAN インターフェイスに限り、ポリシー マップ内にポリシングを設定すると、ハードウェア カウンタは表示されますが、class-default カウンタは表示されません。ポリシー マップ内にポリシングを設定しないと、class-default カウンタが表示されます。

Catalyst 6500 シリーズ スイッチでは、**show policy-map interface** コマンドはプライオリティ機能の厳密なレベルおよびレベルごとのカウントを表示します。

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

HQF

HQF を設定すると、**show policy-map interface** コマンドは追加のフィールドを表示します。これには、DiffServ コード ポイント（DSCP）値、WRED 統計情報（バイト）、WRED による送信済みパケット、クラスごとにパケット出力/バイト出力を表示するカウンタなどがあります。

例

このセクションでは、代表的な **show policy-map interface** コマンドの出力例を示します。使用されるインターフェイスまたはプラットフォーム、および、イネーブルにされたオプションによって、表示される出力は次に示すものと若干異なります。

シリアル インターフェイス上の重み付け均等化キューイング（WFQ）：例

show policy-map interface コマンドの次の出力例では、（次に示すように設定された）mypolicy というサービス ポリシーのアタッチ先となるシリアル 3/1 インターフェイスの統計情報を表示しています。このインターフェイスでは、重み付け均等化キューイング（WFQ）は有効になっています。コマンド出力に共通して表示される主なフィールドの説明は、次の表を参照してください。

```
policy-map mypolicy
 class voice
  priority 128
 class gold
  bandwidth 100
 class silver
  bandwidth 80
  random-detect
Router# show policy-map interface serial3/1 output

 Serial3/1
  Service-policy output: mypolicy
    Class-map: voice (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 5
      Weighted Fair Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 128 (kbps) Burst 3200 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0
    Class-map: gold (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 2
      Weighted Fair Queueing
        Output Queue: Conversation 265
        Bandwidth 100 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
    Class-map: silver (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 1
      Weighted Fair Queueing
        Output Queue: Conversation 266
        Bandwidth 80 (kbps)
        (pkts matched/bytes matched) 0/0
```

```
        (depth/total drops/no-buffer drops) 0/0/0
         exponential weight: 9
         mean queue depth: 0
class     Transmitted       Random drop      Tail drop    Minimum Maximum  Mark
          pkts/bytes        pkts/bytes       pkts/bytes    thresh  thresh  prob
0             0/0               0/0              0/0           20      40  1/10
1             0/0               0/0              0/0           22      40  1/10
2             0/0               0/0              0/0           24      40  1/10
3             0/0               0/0              0/0           26      40  1/10
4             0/0               0/0              0/0           28      40  1/10
5             0/0               0/0              0/0           30      40  1/10
6             0/0               0/0              0/0           32      40  1/10
7             0/0               0/0              0/0           34      40  1/10
rsvp          0/0               0/0              0/0           36      40  1/10
Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

シリアル インターフェイス上のトラフィック シェーピング：例

show policy-map interface コマンドの次の出力例では、（次に示すように設定された）p1 というサービス ポリシーのアタッチ先となるシリアル 3/2 インターフェイスの統計情報を表示しています。このインターフェイス上では、トラフィック シェーピングがイネーブルにされています。コマンド出力に共通して表示される主なフィールドの説明は、次の表を参照してください。

（注） Cisco IOS リリース 12.4(20)T 以降の HQF イメージでは、トラフィック シェーピング クラスの遅延パケット カウンタおよび遅延バイト カウンタは削除されました。

```
policy-map p1
 class c1
  shape average 320000
Router# show policy-map interface serial3/2 output

 Serial3/2
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0
      Traffic Shaping
        Target    Byte   Sustain   Excess    Interval  Increment Adapt
        Rate      Limit  bits/int  bits/int  (ms)      (bytes)   Active
        320000    2000   8000      8000      25        1000      -
        Queue     Packets   Bytes     Packets   Bytes     Shaping
        Depth                         Delayed   Delayed   Active
        0         0         0         0         0         no
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

次の表では、出力によく表示される重要なフィールドについて説明します。表のフィールドは、関連する QoS 機能に従ってグループ化されています。サービス ポリシー出力

名、クラスマップ名、および、一致基準情報に続いて、丸カッコに囲まれた数字が表示されます。この番号は、Cisco 内部だけで使用されるものであり、無視できます。

表 *215 : show policy-map interface* のフィールドの説明

フィールド	説明
クラスまたはサービス ポリシーに関連付けられたフィールド	
Service-policy output	指定されたインターフェイスまたはVCに適応されている出力サービス ポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
packets and bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。 （注） 発信インターフェイス全体でパケットが圧縮されている場合、パケット圧縮によって達成された改善パケット レートは、offered rate には反映されません。また、パケットがトンネルの組み合わせ（例：Generic Routing Encapsulation（GRE）トンネルおよび IP Security（IPSec）トンネル）に入る前に圧縮されている場合、offered rate は、一般にトンネル カプセル化に関連付けられたすべての追加オーバーヘッドを含みません。offered rate は、設定に応じて、オーバーヘッドを含まない、*1* つのトンネル カプセル化だけのオーバーヘッドを含む、または、すべてのトンネル カプセル化のオーバーヘッドを含むのいずれかです。GREおよびIPSecトンネル設定の多くで、offered rate は、GRE トンネル カプセル化のオーバーヘッドだけを含みます。
drop rate	クラスからパケットがドロップされるレート（単位：kbps）。ドロップ レートは、offered rate から正常に送信されたパケット数を引いて計算されます。

フィールド	説明
（注） 分散アーキテクチャ プラットフォーム（Cisco 7500 シリーズ プラットフォームなど）では、offered rate カウンタとドロップ レート カウンタの差として計算される送信レートの値が、散発的に平均から 20 % またはそれ以上逸脱することがあります。独立したトラフィック分析装置によって対応するバーストが示されないにもかかわらず、発生することがあります。	
Match	トラフィックのクラスに指定された一致基準。選択要素には、IP precedence、IP Diffserv コード ポイント（DSCP）値、マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）値、アクセス グループ、および、QoS グループなどの基準があります。使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
キューイングに対応付けられているフィールド（イネーブルの場合）	
Output queue	このトラフィックのクラスに割り当てられている Weighted Fair Queueing（WFQ）カンバセーション。
Bandwidth	このクラスに設定されている帯域幅（kbps または割合のいずれか）、および、バーストサイズ

フィールド	説明
pkts matched/bytes matched	キューに入れられた、このクラスに一致するパケット数（バイト単位でも表示）。この数は、任意の時点でキューイングされた一致パケットの合計数を表します。このクラスに一致するパケットは、輻輳が存在するときだけキューイングされます。パケットがクラスに一致しているが、ネットワークが混雑していないためにキューイングされなかった場合、それらのパケットはこの合計に含まれません。しかし、プロセス スイッチングが使用されている場合は、ネットワークが混雑していない場合でもパケット数は常に加算されます。
depth/total drops/no-buffer drops	このクラスに対して廃棄されたパケット数。No-buffer は、パケットをサービスするメモリ バッファが存在しないことを示します。
Weighted Random Early Detection（WRED）に対応付けられているフィールド（イネーブルである場合）	
exponential weight	WRED パラメータ グループのために平均キュー サイズの計算に使用される指数。
mean queue depth	インターフェイスの実際のキューの深さおよび指数重み付け定数に基づいたキューの深さの平均。これは、変動する平均です。最小しきい値および最大しきい値と、この値とを比較してドロップの是非を決定します。
class	IP precedence レベル。
Transmitted pkts/bytes	WRED を通過し、WRED にドロップされなかったパケット数（バイト単位でも表示）。 （注） パケットを格納するのに十分なメモリがバッファにない場合、パケットが WRED を通過した後でドロップされます。バッファに十分なメモリがないためにドロップされた（「ノーバッファ ドロップ」とも呼ばれる）パケットは、WRED パケット カウンタに算入されます。
Random drop pkts/bytes	キューの深さの平均が、指定された IP precedence レベルの最小しきい値と最大しきい値の間である場合に、ランダムにドロップされたパケット数（バイト単位でも表示）。
Tail drop pkts/bytes	キューの深さの平均が、指定された IP precedence レベルの最大しきい値を上回る場合に、ランダムにドロップされたパケット数（バイト単位でも表示）。

フィールド	説明
Minimum thresh	最小しきい値を表します。パケット数のWRED最小しきい値。
Maximum thresh	最大しきい値を表します。パケット数のWRED最大しきい値。
Mark prob	マーク確率。平均キューの深さが最大しきい値の場合にドロップされたパケットの割合。
トラフィック シェーピングと対応付けられたフィールド（イネーブルである場合）	
Target Rate	シェーピング トラフィックに使用されるレート。
Byte Limit	インターバルあたりの送信最大バイト数。次のように計算されます。 ((Bc+Be) /8) x 1
Sustain bits/int	認定バースト（Bc）レート。
Excess bits/int	超過バースト（Be）レート。
Interval (ms)	ミリ秒（ms）単位の時間間隔の値。
Increment (bytes)	各時間間隔の間にトラフィック シェーピングのトークンバケット内に受信したクレジット数（単位：バイト）。
Queue Depth	トラフィック シェーパーの現在のキューの深さ。
Packets	トラフィック シェーパー システムに入ったパケットの合計数。
Bytes	トラフィック シェーパー システムに入ったバイト合計数。
Packets Delayed	送信される前に、トラフィック シェーパーのキュー内で遅延したパケットの合計数。
Bytes Delayed	送信される前に、トラフィック シェーパーのキュー内で遅延したバイトの合計数。
Shaping Active	トラフィック シェーパーがアクティブかどうかを示します。たとえば、トラフィック シェーパーがアクティブであり、送信されたトラフィックがトラフィック シェーピング レートを上回る場合、フィールドに「yes」が表示されます。

ATM 共有ポート アダプタ上の優先順位ベース集約 WRED：例

show policy-map interface コマンドの次の出力例では、（次に示すように設定された）prec-aggr-wred というサービス ポリシーのアタッチ先となるインターフェイス 4/1/0.10 の ATM 共有ポート アダプタの統計情報を表示しています。このインターフェイスでは集約 WRED が有効になっているため、クラススルー マーク確率統計情報がサブクラスで集約されます。コマンド出力に共通して表示される主なフィールドの説明は、次の表を参照してください。

```
Router(config)# policy-map prec-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect aggregate
Router(config-pmap-c)# random-detect precedence values 0 1 2 3 minimum thresh 10
maximum-thresh 100 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 4 5 minimum-thresh 40 maximum-thresh
 400 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 6 minimum-thresh 60 maximum-thresh
 600 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 7 minimum-thresh 70 maximum-thresh
 700 mark-prob 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface ATM4/1/0.10 point-to-point
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# pvc 10/110
Router(config-if)# service-policy output prec-aggr-wred


Router# show policy-map interface atm4/1/0.10

 ATM4/1/0.10: VC 10/110 -
  Service-policy output: prec-aggr-wred
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 0
        class       Transmitted     Random drop      Tail drop     Minimum   Maximum
Mark
 pkts/bytes pkts/bytes pkts/bytes thresh thresh prob

        0  1  2  3       0/0               0/0              0/0           10     100
1/10
        4  5             0/0               0/0              0/0           40     400
1/10
        6                0/0               0/0              0/0           60     600
1/10
        7                0/0               0/0              0/0           70     700
1/10
```

ATM 共有ポート アダプタ上の DSCP ベース集約 WRED：例

show policy-map interface コマンドの次の出力例では、（次に示すように設定された）dscp-aggr-wred というサービス ポリシーのアタッチ先となるインターフェイス 4/1/0.11 の ATM 共有ポート アダプタの統計情報を表示しています。このインターフェ

イスでは集約 WRED が有効になっているため、クラススルー マーク確率統計情報がサブクラスで集約されます。コマンド出力に共通して表示される主なフィールドの説明は、次の表を参照してください。

```
Router(config)# policy-map dscp-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
 10 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 0 1 2 3 4 5 6 7 minimum-thresh 10
maximum-thresh 20 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 8 9 10 11 minimum-thresh 10 maximum-thresh
 40 mark-prob 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface ATM4/1/0.11 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
Router(config-subif)# pvc 11/101
Router(config-subif)# service-policy output dscp-aggr-wred
Router# show policy-map interface atm4/1/0.11

 ATM4/1/0.11: VC 11/101 -
  Service-policy output: dscp-aggr-wred
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        Exp-weight-constant: 0 (1/1)
        Mean queue depth: 0
        class       Transmitted     Random drop      Tail drop     Minimum   Maximum
Mark
                   pkts/bytes pkts/bytes pkts/bytes thresh thresh prob
        default          0/0               0/0              0/0            1      10
1/10
        0  1  2  3
        4  5  6  7       0/0               0/0              0/0           10      20
1/10
        8  9  10 11      0/0               0/0              0/0           10      40
1/10
```

次の表では、集約 WRED が ATM 共有ポート アダプタ用に設定されている場合に、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 *216 : show policy-map interface* フィールドの説明：*ATM* 共有ポート アダプタ上で集約 *WRED* 用に設定

フィールド	説明
exponential weight	重み付けランダム早期検出（WRED）パラメータ グループのために平均キュー サイズの計算に使用される指数。
mean queue depth	インターフェイスの実際のキューの深さおよび指数重み付け定数に基づいたキューの深さの平均。これは、変動する平均です。最小しきい値および最大しきい値と、この値とを比較してドロップの是非を決定します。

フィールド	説明
（注） 集約重み付けランダム早期検出（WRED）が有効になっている場合、次の WRED 統計情報がそれぞれのサブクラス（IP プレシデンスまたは DiffServ コード ポイント（DSCP）値）に基づいて集約されます。	
class	IP プレシデンス レベルまたは DiffServ コード ポイント（DSCP）値。
Transmitted pkts/bytes	WRED を通過し、WRED にドロップされなかったパケット数（バイト単位でも表示）。 （注） パケットを格納するのに十分なメモリがバッファにない場合、パケットが WRED を通過した後でドロップされます。バッファに十分なメモリがないためにドロップされた（「ノーバッファ ドロップ」とも呼ばれる）パケットは、WRED パケット カウンタに算入されます。
Random drop pkts/bytes	キューの深さの平均が、指定された IP プレシデンス レベルまたは DSCP 値の最小しきい値と最大しきい値の間である場合に、ランダムにドロップされたパケット数（バイト単位でも表示）。
Tail drop pkts/bytes	キューの深さの平均が、指定された IP プレシデンス レベルまたは DSCP 値の最大しきい値を上回る場合に、ランダムにドロップされたパケット数（バイト単位でも表示）。
Minimum thresh	最小しきい値を表します。パケット数の WRED 最小しきい値。
Maximum thresh	最大しきい値を表します。パケット数の WRED 最大しきい値。
Mark prob	マーク確率。平均キューの深さが最大しきい値の場合にドロップされたパケットの割合。

フレームリレー音声適応型トラフィック シェーピング：例

次は、フレームリレー音声適応型トラフィック シェーピングが現在アクティブで、非アクティブ化タイマーが 29 秒残っている出力例です。トラフィック シェーピングがアクティブで、非アクティブ化タイマーが設定されている場合、DLCI 201 の現在の送信レートは minCIR ですが、音声パケットが 29 秒間検出されないと、送信レートが CIR に回復します。

（注） Cisco IOS リリース 12.4(20)T 以降の HQF イメージでは、トラフィック シェーピング クラスの遅延パケット カウンタおよび遅延バイト カウンタは削除されました。

```
Router# show policy interface Serial3/1.1

 Serial3/1.1:DLCI 201 -
  Service-policy output:MQC-SHAPE-LLQ1

    Class-map:class-default (match-any)
      1434 packets, 148751 bytes
      30 second offered rate 14000 bps, drop rate 0 bps
      Match:any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
            63000/63000     1890   7560      7560      120       945

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                        Delayed   Delayed   Active
        BECN   0         1434      162991    26        2704      yes
        Voice Adaptive Shaping active, time left 29 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。次の表で説明していない重要なフィールドについては、前述（「show policy-map interface フィールドの説明」）の表で説明しています。

表 *217 : show policy-map interface* フィールドの説明：フレームリレー音声適応型トラフィック シェーピング用に設定

フィールド	説明
Voice Adaptive Shaping active/inactive	フレーム リレー音声適応型トラフィック シェーピングがアクティブか非アクティブかを示します。
time left	フレーム リレー音声適応型トラフィック シェーピングの非アクティブ化タイマーの残り秒数。

2 レート トラフィック ポリシング：例

次に、2 レート トラフィック ポリシングが設定されている場合の **show policy-map interface** コマンドの出力例を示します。次の例では、1.25 Mbps のトラフィックがポリサー クラスに送信（「提供」）されます。

```
Router# show policy-map interface serial3/0


 Serial3/0
  Service-policy output: policy1
   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps
   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
```

2 レート トラフィック ポリサーにより、500 kbps のトラフィックが適合とマーク付けされ、500 kbps のトラフィックが超過とマーク付けされ、250 kbps のトラフィックが指定されたレートに違反とマーク付けされています。適合とマーク付けされているパケットはそのまま送信され、超過とマーク付けされているパケットは、IP precedence 2 とマーク付けされて送信されます。指定されたレートに違反するとマーク付けされているパケットはドロップされます。

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 *218 : 2* レート トラフィック ポリシングの場合に設定される *show policy-map interface* のフィールドの説明

フィールド	説明
police	**police** コマンドがトラフィック ポリシングを有効にするように設定されていることを示します。また、パケットのマーキングに使用される、指定された CIR、認定バースト サイズ、ピーク情報レート（PIR）、および、ピーク バースト サイズも表示します。
conformed	指定した比率に適合するパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。
exceeded	指定した比率を超えるパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。
violated	指定した比率に違反するパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。

複数トラフィック ポリシング アクション：例

次に、Policer Enhancement（Multiple Actions 機能）が設定されている場合の **show policy-map** コマンドの出力例を示します。**show policy-map interface** コマンドの出力例では、（次に示すように設定された）「police」というサービス ポリシーのアタッチ先となるシリアル 3/2 インターフェイスの統計情報を表示しています。

```
policy-map police
 class class-default
  police cir 1000000 pir 2000000
   conform-action transmit
   exceed-action set-prec-transmit 4
   exceed-action set-frde-transmit
   violate-action set-prec-transmit 2
   violate-action set-frde-transmit

Router# show policy-map interface serial3/2

Serial3/2: DLCI 100 -
Service-policy output: police
    Class-map: class-default (match-any)
      172984 packets, 42553700 bytes
      5 minute offered rate 960000 bps, drop rate 277000 bps
      Match: any
     police:
         cir 1000000 bps, bc 31250 bytes, pir 2000000 bps, be 31250 bytes
       conformed 59679 packets, 14680670 bytes; actions:
         transmit
exceeded 59549 packets, 14649054 bytes; actions:
         set-prec-transmit 4
         set-frde-transmit
       violated 53758 packets, 13224468 bytes; actions:
         set-prec-transmit 2
         set-frde-transmit
       conformed 340000 bps, exceed 341000 bps, violate 314000 bps
```

次に、**show policy-map interface** コマンドの出力例を示します。

- 59679 個のパケットが、適合パケット（つまり、CIR に適合するパケット）としてマーキングされ、変更なしに送信されました。
- 59549 個のパケットが、超過パケット（つまり、CIR を超えているが、PIR を超えないパケット）としてマーキングされました。したがって、これらのパケットの IP Precedence 値は、IP Precedence レベル 4 に変更され、Discard Eligibility（DE）ビットは 1 に設定され、パケットはこのように変更された状態で送信されました。
- 53758 個のパケットが違反パケット（つまり、PIR を超えているパケット）としてマーキングされました。したがって、これらのパケットの IP プレシデンス値は、IP プレシデンス 2 に変更され、DE ビットは 1 に設定され、パケットはこのように変更された状態で送信されました。

（注） アクションは、**police** コマンドの *action* 引数を使用して指定されます。使用可能なアクションの詳細については、**police** コマンドのリファレンス ページを参照してください。

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 *219 :* 複数トラフィック ポリシング アクションの場合に設定される *show policy-map interface* のフィールドの説明

フィールド	説明
police	**police** コマンドがトラフィック ポリシングを有効にするように設定されていることを示します。また、パケットのマーキングに使用される、指定されたCIR、適合バーストサーズ（BC）、PIR、およびピーク バースト サイズ（BE）も表示します。
conformed, packets, bytes, actions	指定されたレートに適合するとしてマーキングされたパケット数（バイト単位でも表示）とパケットに実施されたアクションを表示します。複数のアクションがある場合は、アクションごとに別々にリストされます。
exceeded, packets, bytes, actions	指定されたレートに超過するとしてマーキングされたパケット数（バイト単位でも表示）とパケットに実施されたアクションを表示します。複数のアクションがある場合は、アクションごとに別々にリストされます。
violated, packets, bytes, actions	指定されたレートに違反するとしてマーキングされたパケット数（バイト単位でも表示）とパケットに実施されたアクションを表示します。複数のアクションがある場合は、アクションごとに別々にリストされます。

明示的輻輳通知：例

次に、WRED - 明示的輻輳通知（ECN）機能が設定されている場合の **show policy-map interface** コマンドの出力例を示します。出力に含まれる「explicit congestion notification」という語は ECN が有効になっていることを示します。

```
Router# show policy-map interface Serial4/1

 Serial4/1
  Service-policy output:policy_ecn
        Class-map:prec1 (match-all)
          1000 packets, 125000 bytes
          30 second offered rate 14000 bps, drop rate 5000 bps
          Match:ip precedence 1
          Weighted Fair Queueing
            Output Queue:Conversation 42
            Bandwidth 20 (%)
```

```
        Bandwidth 100 (kbps)
        (pkts matched/bytes matched) 989/123625
    (depth/total drops/no-buffer drops) 0/455/0
         exponential weight:9
         explicit congestion notification
         mean queue depth:0
class    Transmitted  Random drop  Tail drop   Minimum     Maximum     Mark
         pkts/bytes   pkts/bytes    pkts/bytes threshold   threshold   probability
  0        0/0          0/0          0/0          20          40         1/10
  1      545/68125      0/0          0/0          22          40         1/10
  2        0/0          0/0          0/0          24          40         1/10
  3        0/0          0/0          0/0          26          40         1/10
  4        0/0          0/0          0/0          28          40         1/10
  5        0/0          0/0          0/0          30          40         1/10
  6        0/0          0/0          0/0          32          40         1/10
  7        0/0          0/0          0/0          34          40         1/10
rsvp       0/0          0/0          0/0          36          40         1/10
class    ECN Mark
        pkts/bytes
  0      0/0
  1     43/5375
  2      0/0
  3      0/0
  4      0/0
  5      0/0
  6      0/0
  7      0/0
rsvp     0/0
```

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 *220 : show policy-map interface* フィールドの説明：*ECN* 用に設定

フィールド	説明
explicit congestion notification	明示的輻輳通知がイネーブルであることを示します。
mean queue depth	インターフェイスの実際のキューの深さおよび指数重み付け定数に基づいたキューの深さの平均。これは移動平均です。最小しきい値および最大しきい値と、この値とを比較してドロップの是非を決定します。
class	IP precedence 値
Transmitted pkts/bytes	WRED を通過し、WRED にドロップされなかったパケット数（バイト単位でも表示）。 （注） パケットを格納するのに十分なメモリがバッファにない場合、パケットが WRED を通過した後でドロップされます。バッファに十分なメモリがないためにドロップされた（「ノーバッファ ドロップ」とも呼ばれる）パケットは、WRED パケット カウンタに算入されます。

フィールド	説明
Random drop pkts/bytes	キューの深さの平均が、指定された IP プレシデンス値の最小しきい値と最大しきい値の間である場合に、ランダムにドロップされたパケット数（バイト単位でも表示）。
Tail drop pkts/bytes	キューの深さの平均が、指定された IP プレシデンス値の最大しきい値を上回る場合に、ランダムにドロップされたパケット数（バイト単位でも表示）。
Minimum threshold	パケット数の WRED 最小しきい値。
Maximum threshold	パケット数の WRED 最大しきい値。
Mark probability	平均キューの深さが最大しきい値の場合にドロップされたパケットの割合。
ECN Mark pkts/bytes	ECNによってマークされたパケットの数（バイト単位でも表示）。

クラスベースの RTP および TCP ヘッダー圧縮：例

show policy-map interface コマンドの次の出力例は、「p1」というポリシー マップ内の「prec2」というクラスに対して RTP ヘッダー圧縮が設定されていることを示しています。

show policy-map interface コマンド出力には、設定されたヘッダー圧縮の種類（RTP）、「p1」というポリシーマップのアタッチ先となるインターフェイス（シリアル4/1）、パケットの合計数、圧縮されたパケットの数、保存されたパケットの数、送信されたパケットの数、およびパケットが圧縮されたレート（1 秒あたりのビット数（bps））が表示されます。

この例では、User Datagram Protocol（UDP）/RTP ヘッダー圧縮が設定され、出力の最後に圧縮統計情報が含まれています。

```
Router# show policy-map interface Serial4/1

Serial4/1
Service-policy output:p1
    Class-map:class-default (match-any)
      1005 packets, 64320 bytes
      30 second offered rate 16000 bps, drop rate 0 bps
      Match:any
compress:
          header ip rtp
          UDP/RTP Compression:
          Sent:1000 total, 999 compressed,
                41957 bytes saved, 17983 bytes sent
                3.33 efficiency improvement factor
                99% hit ratio, five minute miss rate 0 misses/sec, 0 max
                 rate 5000 bps
```

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 *221 : show policy-map interface* フィールドの説明：クラスベース *RTP* および *TCP* ヘッダー圧縮用に設定

フィールド	説明
Service-policy output	指定されたインターフェイスまたはVCに適応されている出力サービスポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。 （注） 発信インターフェイス全体でパケットが圧縮されている場合、パケット圧縮によって達成された改善パケット レートは、offered rate には反映されません。また、パケットがトンネルの組み合わせ（例：Generic Routing Encapsulation（GRE）トンネルおよび IP Security（IPSec）トンネル）に入る前に圧縮されている場合、offered rate は、一般にトンネル カプセル化に関連付けられたすべての追加オーバーヘッドを含みません。offered rate は、設定に応じて、オーバーヘッドを含まない、*1* つのトンネル カプセル化だけのオーバーヘッドを含む、または、すべてのトンネル カプセル化のオーバーヘッドを含むのいずれかです。GRE および IPSec トンネル設定の多くで、offered rate は、GRE トンネル カプセル化のオーバーヘッドだけを含みます。
UDP/RTP Compression	クラスに対して RTP ヘッダー圧縮が設定されていることを示します。
Sent total	送信される各パケットの数（圧縮パケットとフルヘッダー パケットの両方）。
Sent compressed	送信された圧縮パケットの数。
bytes saved	保存された合計バイト数（つまり、送信する必要がないバイト数）。
bytes sent	送信した合計バイト数（圧縮パケットとフルヘッダー パケットの両方）。
efficiency improvement factor	ヘッダー圧縮の結果向上した帯域幅効率のパーセンテージ。たとえば、RTP ストリームの場合、効率改善係数が 2.9（つまり 290%）にもなる場合があります。

フィールド	説明
hit ratio	これは、主にトラブルシューティング目的で使用され、コンテキスト データベースで検出されたパケットのパーセンテージを表します。ほとんどの場合、このパーセンテージは高くなります。
five minute miss rate	過去 5 分間に検出された新規トラフィック フローの数。
misses/sec max	1 秒あたりに検出された新規トラフィック フローの平均数、およびこれまでの新規トラフィック フローの最大レート。
rate	パケット圧縮後の実際のトラフィック レート（1 秒あたりのビット数）。

（注） サービス ポリシー出力名、および、クラスマップ名に続いて、丸カッコに囲まれた数字が表示されます。この番号は、Cisco 内部だけで使用されるものであり、無視できます。

モジュラ QoS CLI（MQC）の無条件パケット廃棄：例

show policy-map interface コマンドの次の出力例では、「policy1」というポリシーマップのアタッチ先となるシリアル 2/0 インターフェイスの統計情報を表示しています。「c1」というクラスに属するすべてのパケットに対して廃棄処理が指定されています。この例では、そのクラスに 32,000 bps のトラフィックが送信（「提供」）され、そのいずれもドロップされます。このため、ドロップ レートが 32000 bps になっています。

```
Router# show policy-map interface

 Serial2/0
Serial2/0
 Service-policy output: policy1
   Class-map: c1 (match-all)
      10184 packets, 1056436 bytes
      5 minute offered rate 32000 bps, drop rate 32000 bps
      Match: ip precedence 0
      drop
```

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 *222 : show policy-map interface* フィールドの説明：*MQC* 無条件パケット廃棄用に設定

フィールド	説明
Service-policy output	指定されたインターフェイスまたは VC に適応されている出力サービス ポリシーの名前。

フィールド	説明
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。 （注） 発信インターフェイス全体でパケットが圧縮されている場合、パケット圧縮によって達成された改善パケット レートは、offered rate には反映されません。また、パケットがトンネルの組み合わせ（例：Generic Routing Encapsulation（GRE）トンネルおよび IP Security（IPSec）トンネル）に入る前に圧縮されている場合、offered rate は、一般にトンネル カプセル化に関連付けられたすべての追加オーバーヘッドを含みません。offered rate は、設定に応じて、オーバーヘッドを含まない、*1* つのトンネル カプセル化だけのオーバーヘッドを含む、または、すべてのトンネル カプセル化のオーバーヘッドを含むのいずれかです。GREおよびIPSecトンネル設定の多くで、offered rate は、GRE トンネル カプセル化のオーバーヘッドだけを含みます。
drop rate	クラスからパケットがドロップされるレート（単位：kbps）。ドロップ レートは、offered rate から正常に送信されたパケット数を引いて計算されます。

フィールド	説明
（注） 分散アーキテクチャプラットフォーム（Cisco 7500 など）では、offered rate カウンタとドロップレート カウンタの差として計算される送信レートの値が、散発的に平均から 20 % またはそれ以上逸脱することがあります。独立したトラフィック分析装置によって対応するバーストが示されないにもかかわらず、発生することがあります。	
Match	トラフィックのクラスに指定された一致基準。選択要素には、Layer 3 パケット長、IP プレシデンス、IP DSCP 値、MPLS EXP 値、アクセス グループ、QoS グループなどの基準があります。使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
drop	指定したクラスに属するすべてのパケットに対してパケット廃棄処理が設定されていることを示します。

（注） サービス ポリシー出力名、および、クラスマップ名に続いて、丸カッコに囲まれた数字が表示されます。この番号は、Cisco 内部だけで使用されるものであり、無視できます。

パーセントベース ポリシングおよびシェーピング：例

show policy-map interface コマンドの次の出力例は、帯域幅の 20% に基づいた CIR を使用して設定されたトラフィック ポリシングを示しています。CIR およびミリ秒（ms）単位の認定バースト（BC）も表示に含まれています。

```
Router# show policy-map interface Serial3/1
```

```
Service-policy output: mypolicy
  Class-map: gold (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
    police:
        cir 20 % bc 10 ms
        cir 2000000 bps, bc 2500 bytes
        pir 40 % be 20 ms
        pir 4000000 bps, be 10000 bytes
   conformed 0 packets, 0 bytes; actions:
    transmit
   exceeded 0 packets, 0 bytes; actions:
     drop
    violated 0 packets, 0 bytes; actions:
     drop
    conformed 0 bps, exceed 0 bps, violate 0 bps
```

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。サービス ポリシー出力名、および、クラス マップ名に続いて、丸カッコに囲まれた数字が表示されます。この番号は、Cisco 内部だけで使用されるものであり、無視できます。

表 *223 :* パーセントベース ポリシングおよびシェーピングの場合に設定される *show policy-map interface* のフィールドの説明.

フィールド	説明
Service-policy output	指定されたインターフェイスまたはVCに適応されている出力サービス ポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-anyなど）もトラフィック クラスの横に表示されます。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。 （注） 発信インターフェイス全体でパケットが圧縮されている場合、パケット圧縮によって達成された改善パケット レートは、offered rateには反映されません。また、パケットがトンネルの組み合わせ（例：Generic Routing Encapsulation（GRE）トンネルおよびIP Security（IPSec）トンネル）に入る前に圧縮されている場合、offered rate は、一般にトンネル カプセル化に関連付けられたすべての追加オーバーヘッドを含みません。offered rate は、設定に応じて、オーバーヘッドを含まない、*1* つのトンネル カプセル化だけのオーバーヘッドを含む、または、すべてのトンネル カプセル化のオーバーヘッドを含むのいずれかです。GRE および IPSec トンネル設定の多くで、offered rate は、GRE トンネル カプセル化のオーバーヘッドだけを含みます。

フィールド	説明
police	帯域幅の割合に基づいたトラフィック ポリシングがイネーブルにされていることを示します。帯域幅の割合、CIR およびミリ秒単位の認定バースト（BC）も表示します。
conformed, actions	指定されたレートに適合するとしてマーキングされたパケット数とバイト数、および、パケットに実施されたアクションを表示します。
exceeded, actions	指定されたレートを超過するとしてマーキングされたパケット数とバイト数、および、パケットに実施されたアクションを表示します。

トラフィック シェーピング：例

次の **show policy-map interface** コマンドの出力例では、（次のとおり）シリアル 3/2 インターフェイスの統計情報が表示されています。このインターフェイス上でトラフィック シェーピングがイネーブルにされており、帯域幅の 20% の平均レートが指定されています。

（注） Cisco IOS リリース 12.4(20)T 以降の HQF イメージでは、トラフィック シェーピング クラスの遅延パケット カウンタおよび遅延バイト カウンタは削除されました。

```
Router# show policy-map interface Serial3/2

Serial3/2
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Traffic Shaping
        Target/Average      Byte   Sustain    Excess      Interval  Increment  Adapt
        Rate              Limit  bits/int  bits/int    (ms)     (bytes)   Active
         20 %                        10 (ms)    20 (ms)
        201500/201500       1952   7808       7808        38         976       -
        Queue     Packets   Bytes     Packets   Bytes     Shaping
        Depth                         Delayed   Delayed   Active
        0         0         0         0         0         no
```

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。サービス ポリシー出力名、クラスマップ名、および、一致基準情報に続いて、丸カッコに囲まれた数字が表示されます。この番号は、Cisco 内部だけで使用されるものであり、無視できます。

表 *224 : show policy-map interface* フィールドの説明：パーセントベース ポリシングおよびシェーピング（トラフィック シェーピングは有効）用に設定

フィールド	説明
Service-policy output	指定されたインターフェイスまたは VC に適応されている出力サービス ポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。 （注） 発信インターフェイス全体でパケットが圧縮されている場合、パケット圧縮によって達成された改善パケット レートは、offered rate には反映されません。また、パケットがトンネルの組み合わせ（例：Generic Routing Encapsulation（GRE）トンネルおよび IP Security（IPSec）トンネル）に入る前に圧縮されている場合、offered rate は、一般にトンネル カプセル化に関連付けられたすべての追加オーバーヘッドを含みません。offered rate は、設定に応じて、オーバーヘッドを含まない、*1* つのトンネル カプセル化だけのオーバーヘッドを含む、または、すべてのトンネル カプセル化のオーバーヘッドを含むのいずれかです。GRE および IPSec トンネル設定の多くで、offered rate は、GRE トンネル カプセル化のオーバーヘッドだけを含みます。
drop rate	クラスからパケットがドロップされるレート（単位：kbps）。ドロップ レートは、offered rate から正常に送信されたパケット数を引いて計算されます。
Match	トラフィックのクラスに指定された一致基準。選択要素には、Layer 3 パケット長、IP precedence、IP DSCP 値、MPLS EXP 値、アクセス グループ、Quality of Service（QoS）グループなどの基準があります。使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
Traffic Shaping	帯域幅の割合に基づいたトラフィック シェーピングがイネーブルにされていることを示します。
Target/Average Rate	シェーピング トラフィックに使用されるレート（割合）およびそのレートに一致するパケット数。

フィールド	説明
Byte Limit	インターバルあたりの送信最大バイト数。次のように計算されます。 ((Bc+Be) /8) x 1
Sustain bits/int	認定バースト（Bc）レート。
Excess bits/int	超過バースト（Be）レート。
Interval (ms)	ミリ秒（ms）単位の時間間隔の値。
Increment (bytes)	各時間間隔の間にトラフィック シェーピングのトークン バケット内に受信したクレジット数（単位：バイト）。
Adapt Active	適応可能なシェーピングがイネーブルであるかどうかを示します。
Queue Depth	トラフィック シェーパーの現在のキューの深さ。
Packets	トラフィック シェーパー システムに入ったパケットの合計数。
Bytes	トラフィック シェーパー システムに入ったバイト合計数。
Packets Delayed	送信される前に、トラフィック シェーパーのキュー内で遅延したパケットの合計数。 （注） Cisco IOS リリース 12.4(20)T では、このカウンタは削除されました。
Bytes Delayed	送信される前に、トラフィック シェーパーのキュー内で遅延したバイトの合計数。 （注） Cisco IOS リリース 12.4(20)T では、このカウンタは削除されました。
Shaping Active	トラフィック シェーパーがアクティブかどうかを示します。たとえば、トラフィック シェーパーがアクティブであり、送信されたトラフィックがトラフィック シェーピング レートを上回る場合、フィールドに「yes」が表示されます。

レイヤ 3 パケット長に基づくパケット分類：例

show policy-map interface コマンドの次の出力例では、「mypolicy」というサービス ポリシーのアタッチ先となるイーサネット 4/1 インターフェイスのパケット統計情報を表示しています。レイヤ3パケット長は、「class1」というクラスにトラフィックの一致基準として指定されています。

```
Router# show policy-map interface Ethernet4/1
```

```
Ethernet4/1
Service-policy input: mypolicy
  Class-map: class1 (match-all)
     500 packets, 125000 bytes
     5 minute offered rate 4000 bps, drop rate 0 bps
     Match: packet length min 100 max 300
     QoS Set
       qos-group 20
         Packets marked 500
```

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。サービス ポリシー入力名、クラス マップ名、および一致基準情報に続いて、丸カッコに囲まれた数字が表示されます。この番号は、Cisco内部だけで使用されるものであり、無視できます。

表 *225 : show policy-map interface* フィールドの説明：レイヤ *3* パケット長に基づくパケット分類用に設定

フィールド	説明
Service-policy input	指定されたインターフェイスまたはVCに適用されている入力サービス ポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-anyなど）もトラフィック クラスの横に表示されます。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。 （注） 発信インターフェイス全体でパケットが圧縮されている場合、パケット圧縮によって達成された改善パケット レートは、offered rateには反映されません。また、パケットがトンネルの組み合わせ（例：Generic Routing Encapsulation（GRE）トンネルおよびIP Security（IPSec）トンネル）に入る前に圧縮されている場合、offered rate は、一般にトンネル カプセル化に関連付けられたすべての追加オーバーヘッドを含みません。offered rate は、設定に応じて、オーバーヘッドを含まない、*1* つのトンネル カプセル化だけのオーバーヘッドを含む、または、すべてのトンネル カプセル化のオーバーヘッドを含むのいずれかです。GRE および IPSec トンネル設定の多くで、offered rate は、GRE トンネル カプセル化のオーバーヘッドだけを含みます。
drop rate	クラスからパケットがドロップされるレート（単位：kbps）。ドロップ レートは、offered rate から正常に送信されたパケット数を引いて計算されます。
Match	トラフィックのクラスに指定された一致基準。選択要素には、Layer 3 パケット長、IP プレシデンス、IP DSCP 値、MPLS EXP 値、アクセス グループ、QoS グループなどの基準があります。

フィールド	説明
QoS Set, qos-group, Packets marked	QoS グループに基づくクラスベース パケット マーキングが設定されていることを示します。qos-group 番号やマーク済みパケットの数などがあります。

拡張パケット マーキング：例

show policy-map interface コマンドの次の出力例は、FastEthernet サブインターフェイスにアタッチされたサービス ポリシーを示しています。この例では、「policy1」というサービス ポリシーがアタッチされています。「policy1」では、「table-map1」というテーブル マップが設定されています。「table-map1」の値は、優先順位値を対応するサービス クラス（CoS）値にマップするために使用します。

```
Router# show policy-map interface

 FastEthernet1/0.1
  Service-policy input: policy1
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        precedence cos table table-map1
          Packets marked 0
```

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。サービス ポリシー入力名およびクラス マップ名に続いて、丸カッコに囲まれた数字が表示されます。この番号は、Cisco 内部だけで使用されるものであり、無視できます。

表 *226 : show policy-map interface* フィールドの説明：拡張パケット マーキング用に設定

フィールド	説明
Service-policy input	指定されたインターフェイスまたは VC に適用されている入力サービス ポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（kbps）。

フィールド	説明
Match	トラフィックのクラスに指定された一致基準。選択要素には、優先順位、IP Diffserv コード ポイント（DSCP）値、マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）値、アクセス グループ、Quality of Service（QoS）グループ（セット）などの基準があります。使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
QoS Set	特定のクラスに対して QoS グループ（セット）が設定されていることを示します。
precedence cos table table-map1	テーブル マップ（「table-map1」）が優先順位値を決定するために使用されていることを示します。テーブル マップに定義されている CoS の値に従って、優先順位値が設定されます。
Packets marked	特定のクラスにおけるマーク済みパケットの合計数。

トラフィック ポリシング：例

次は、**show policy-map interface** コマンドの出力例です。このサンプルには、トラフィック ポリシングがイネーブルにされている、シリアル 2/0 インターフェイスの統計情報が表示されています。認定（適合）バースト（bc）、および超過（ピーク）バーストがミリ秒単位（ms）で指定されています。

```
Router# show policy-map interface serial2/0

 Serial2/0
  Service-policy output: policy1 (1050)
    Class-map: class1 (match-all) (1051/1)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0  (1052)
      police:
          cir 20 % bc 300 ms
          cir 409500 bps, bc 15360 bytes
          pir 40 % be 400 ms
          pir 819000 bps, be 40960 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
    Class-map: class-default (match-any) (1054/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1055)
        0 packets, 0 bytes
        5 minute rate 0 bps
```

この例では、CIR および PIR は、bps で表示され、認定バースト（bc）、および超過バースト（be）の両方が、ビットで表示されます。

CIR、PIR、bc、および be は、以下に説明する式に基づいて計算されます。

CIR の計算式：例

CIR を計算する場合は、次の式を使用します。

- 指定された CIR パーセンテージ（**show policy-map** コマンドの出力に表示）× インターフェイスの帯域幅（BW）（**show interfaces** コマンドの出力に表示）= 1 秒あたりの合計ビット数

シリアル 2/0 インターフェイスの **show interfaces** コマンドの出力によると、インターフェイスの帯域幅（BW）は 2048 kbps です。

```
Router# show interfaces serial2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

CIR の計算には次の値を使用します。

20 % X 2048 kbps = 409600 bps

PIR の計算式：例

PIR を計算する場合は、次の式を使用します。

- 指定された PIR パーセンテージ（**show policy-map** コマンドの出力に表示）× インターフェイスの帯域幅（BW）（**show interfaces** コマンドの出力に表示）= 1 秒あたりの合計ビット数

シリアル 2/0 インターフェイスの **show interfaces** コマンドの出力によると、インターフェイスの帯域幅（BW）は 2048 kbps です。

```
Router# show interfaces serial2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

次の値が PIR の計算に使用されます。

40 % X 2048 kbps = 819200 bps

（注） この合計と **show policy-map interface** コマンドの出力に表示される合計との違いは、丸め計算または特定のインターフェイス設定に関する違いが原因です。

認定バースト（bc）の計算式：例

bc を計算する場合は、次の式を使用します。

- ミリ秒単位の bc（**show policy-map** コマンドで識別）x ビット/秒単位の CIR = 合計バイト数

次の値が bc の計算に使用されます。

300 ms X 409600 bps = 15360 バイト

超過バースト（be）の計算式：例

bc および be を計算する場合は、次の式を使用します。

- ミリ秒単位の be（**show policy-map** コマンドで識別）x ビット/秒単位の PIR = 合計バイト数

次の値が be の計算に使用されます。

400 ms X 819200 bps = 40960 バイト

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 *227 : show policy-map interface* のフィールドの説明

フィールド	説明
Service-policy output	指定されたインターフェイスまたはVCに適応されている出力サービス ポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-anyなど）もトラフィック クラスの横に表示されます。
packets and bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。
drop rate	クラスからパケットがドロップされるレート（単位：kbps）。ドロップレートは、offered rate から正常に送信されたパケット数を引いて計算されます。

フィールド	説明
Match	トラフィックのクラスに指定された一致基準。選択要素には、Layer 3 パケット長、IP precedence、IP Diffserv コード ポイント（DSCP）値、マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）値、アクセス グループ、および、Quality of Service（QoS）グループなどの基準があります。使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
police	トラフィック ポリシングがイネーブルにされていることを示します。表示には、CIR と PIR（帯域幅の割合と bps の両方）、および、bc と be（バイト数およびミリ秒単位）が含まれます。任意の適合アクション、超過アクションおよび違反アクションがあれば表示され、それらの任意のアクションに関係する統計情報が表示されます。

帯域幅の推定：例

show policy-map interface コマンドの次の出力例では、Quality of Service（QoS）ターゲットの帯域幅の推定を生成したファスト イーサネット 0/1 インターフェイスの統計情報を表示しています。

[帯域幅の推定（Bandwidth Estimation）] セクションは、QoS ターゲットの帯域幅の推定が定義されていることを示しています。これらのターゲットには、ミリ秒単位のパケット損失レート、パケット遅延レート、およびタイムフレームが含まれています。[信頼度（Confidence）] とは、ターゲットの drop-one-in 値（パーセンテージ）のことです。[Corvil Bandwidth] とは、帯域幅の推定（キロビット/秒）のことです。

ドロップ ターゲットまたは遅延ターゲットを指定しないと、出力に「何も指定がないため、フォールバックして 500 個のうち 1 個のパケットのみをドロップします（none specified, falling back to drop no more than one packet in 500）」と表示されます。

```
Router# show policy-map interface FastEthernet0/1

 FastEthernet0/1
  Service-policy output: my-policy
    Class-map: icmp (match-all)
      199 packets, 22686 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      Bandwidth Estimation:
        Quality-of-Service targets:
          drop no more than one packet in 1000 (Packet loss < 0.10%)
          delay no more than one packet in 100 by 40 (or more) milliseconds
            (Confidence: 99.0000%)
        Corvil Bandwidth: 1 kbits/sec
    Class-map: class-default (match-any)
      112 packets, 14227 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Bandwidth Estimation:
```

```
        Quality-of-Service targets:
          <none specified, falling back to drop no more than one packet in 500
        Corvil Bandwidth: 1 kbits/sec
```

HQF を有効にしたシェーピング：例

show policy-mapinterface コマンドの次の出力例は、シェーピングがアクティブであり（キューの深さフィールドを参照）、シリアル 4/3 インターフェイスで HQF が有効になっていることを示しています。すべてのトラフィックはclass-default キューに分類されます。

（注） Cisco IOS リリース 12.4(20)T 以降の HQF イメージでは、トラフィック シェーピング クラスの遅延パケット カウンタおよび遅延バイト カウンタは削除されました。

```
Router# show policy-map interface serial4/3

 Serial4/3
  Service-policy output: shape
    Class-map: class-default (match-any)
      2203 packets, 404709 bytes
      30 second offered rate 74000 bps, drop rate 14000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 64/354/0
      (pkts output/bytes output) 1836/337280
      shape (average) cir 128000, bc 1000, be 1000
      target shape rate 128000
        lower bound cir 0,  adapt to fecn 0
      Service-policy : LLQ
        queue stats for all priority classes:

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
        Class-map: c1 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Priority: 32 kbps, burst bytes 1500, b/w exceed drops: 0
        Class-map: class-default (match-any)
          2190 packets, 404540 bytes
          30 second offered rate 74000 bps, drop rate 14000 bps
          Match: any
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 63/417/0
          (pkts output/bytes output) 2094/386300
```

VLAN ID 番号に基づいて照合されたパケット：例

（注） Cisco IOS リリース 12.2(31)SB2 の時点で、VLAN ID 番号に基づく一致パケットは、Catalyst 1000 プラットフォームでのみサポートされています。

次に、VLAN ID 番号に基づいてパケットを照合し、分類する設定例を示します。この設定例では、VLAN ID 番号 150 に一致するパケットが「class1」というクラスに配置されます。

```
Router# show class-map

Class Map match-all class1 (id 3)
Match vlan 150
```

class1 はその後、「policy1」というポリシー マップの一部として設定されます。ポリシー マップは、ファスト イーサネット サブインターフェイス 0/0.1 にアタッチされます。

show policy-map interface コマンドの次の出力例では、ファスト イーサネット サブインターフェイス 0/0.1 にアタッチされたポリシー マップのパケット統計情報を表示しています。表示される統計情報は、class1 が設定されている policy1 のものです。

```
Router# show policy-map interface

FastEthernet0/0.1
! Policy-map name.
Service-policy input: policy1
! Class configured in the policy map.
Class-map: class1 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
! VLAN ID 150 is the match criterion for the class.
Match: vlan 150
police:
cir 8000000 bps, bc 512000000 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0 bps, exceed 0 bps
Class-map: class-default (match-any)
10 packets, 1140 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any
10 packets, 1140 bytes
5 minute rate 0 bps
```

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。サービス ポリシー入力名およびクラス マップ名に続いて、丸カッコに囲まれた数字が表示されます。この番号は、Cisco 内部だけで使用されるものであり、無視できます。

表 *228 : show policy-map interface* フィールドの説明：*VLAN ID* 番号に基づいて照合されたパケット

フィールド	説明
Service-policy input	指定されたインターフェイスまたは VC に適用されている入力サービス ポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（kbps）。
Match	トラフィックのクラスに指定された一致基準。選択要素には、VLAN ID 番号、優先順位、IP Diffserv コードポイント（DSCP）値、マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）値、アクセス グループ、Quality of Service（QoS）グループ（セット）などの基準があります。使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。

Cisco 7600 シリーズ ルータ：例

次の例は、Cisco 7600 シリーズ ルータ上のインターフェイスにアタッチされているすべての入力ポリシーおよび出力ポリシーの統計情報および設定を表示する方法を示しています。

```
Router# show policy-map interface

 FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class ipp5
    police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
policed-dscp-transmit
```

次の例は、Cisco 7600 シリーズ ルータ上にある特定のインターフェイスの入力ポリシー統計情報および設定を表示する方法を示しています。

```
Router# show policy-map interface fastethernet 5/36 input

 FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
```

```
      5 minute rate 0 bps
      match: ip precedence 5
  class ipp5
    police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
olliced-dscp-transmit
```

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 *229 : show policy-map interface* フィールドの説明：*Cisco 7600* シリーズ ルータ

フィールド	説明
service-policy input	指定されたインターフェイスに適用されている入力サービス ポリシーの名前。
class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-anyなど）もトラフィック クラスの横に表示されます。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
minute rate	クラスに着信するパケットのレート（kbps）。
match	トラフィックのクラスに指定された一致基準。選択要素には、VLAN ID 番号、優先順位、IP Diffserv コードポイント（DSCP）値、マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）値、アクセス グループ、Quality of Service（QoS）グループ（セット）などの基準があります。使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
class	Precedence 値.
police	**police** コマンドがトラフィック ポリシングを有効にするように設定されていることを示します。

Cisco 7200 シリーズ ルータ：例

次の例は、MQC ポリシング ポリシー マップで **bc** 値および **be** 値を Cisco 7200 シリーズルータ上のインターフェイスの MTU サイズに自動的に丸める処理を示しています。丸めが行われるのは、bc 値および be 値がインターフェイスの MTU サイズよりも小さい場合のみです。

```
Router# show policy-map interface

Service-policy output: p2
Service-policy output: p2
    Class-map: class-default (match-any)
      2 packets, 106 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
```

```
    Match: any
      2 packets, 106 bytes
      30 second rate 0 bps
    police:
        cir 10000 bps, bc 4470 bytes
        pir 20000 bps, be 4470 bytes
      conformed 0 packets, 0 bytes; actions:
        transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      violated 0 packets, 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps, violate 0000 bps
```

シリアル インターフェイス上の複数のプライオリティ キュー：例

show policy-map interface コマンドの次の出力例は、複数のプライオリティ キューを設定していると表示される統計情報の種類を示しています。使用しているインターフェイスおよび有効にしているオプションによっては、表示される出力が次に示す出力と若干異なる場合があります。

```
Router# show policy-map interface

Serial2/1/0
Service-policy output: P1
Queue statistics for all priority classes:
.
.
.
Class-map: Gold (match-all)
0 packets, 0 bytes   /*Updated for each priority level configured.*/
5 minute offered rate 0 bps, drop rate 0 bps
Match: ip precedence 2
Priority: 0 kbps, burst bytes 1500, b/w exceed drops: 0
Priority Level 4:
0 packets, 0 bytes
```

帯域幅残量割合：例

show policy-map interface コマンドの次の出力例は、クラス キューに帯域幅残量割合が設定されていることを示しています。例に示すように、precedence_0、precedence_1、precedence_2 の各クラスにはそれぞれ 20、40、60 の帯域幅残量割合があります。

```
Router# show policy-map interface GigabitEthernet1/0/0.10

  Service-policy output: vlan10_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
```

```
shape (average) cir 1000000, bc 4000, be 4000
target shape rate 1000000
bandwidth remaining ratio 10
Service-policy : child_policy
  Class-map: precedence_0 (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 0
    Queueing
    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    shape (average) cir 500000, bc 2000, be 2000
    target shape rate 500000
    bandwidth remaining ratio 20
  Class-map: precedence_1 (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 1
    Queueing
    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    shape (average) cir 500000, bc 2000, be 2000
    target shape rate 500000
    bandwidth remaining ratio 40
  Class-map: precedence_2 (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 2
    Queueing
    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    shape (average) cir 500000, bc 2000, be 2000
    target shape rate 500000
    bandwidth remaining ratio 60
  Class-map: class-default (match-any)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps

    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
```

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 *230 : show policy-map interface* フィールドの説明：帯域幅残量割合用に設定

フィールド	説明
Service-policy output	指定されたインターフェイスに適用されている出力サービスポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。

フィールド	説明
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
bandwidth remaining ratio	超過帯域幅の割り当てに使用される比率を示します。

トンネル マーキング：例

show policy-map interface コマンドの出力例で、文字列「ip dscp tunnel 3」はトンネル型パケットのヘッダーの DSCP 値を 3 に設定するように L2TPv3 トンネル マーキングが設定されていることを示しています。

```
Router# show policy-map interface

 Serial0
  Service-policy input: tunnel
    Class-map: frde (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: fr-de
      QoS Set
        ip dscp tunnel 3
          Packets marked 0
    Class-map: class-default (match-any)
      13736 packets, 1714682 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        13736 packets, 1714682 bytes
        30 second rate 0 bps
```

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 *231 : show policy-map interface* フィールドの説明：トンネル マーキング用に設定

フィールド	説明
service-policy input	指定されたインターフェイスに適用されている入力サービス ポリシーの名前。
class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。
drop rate	クラスからパケットがドロップされるレート（単位：kbps）。ドロップ レートは、offered rate から正常に送信されたパケット数を引いて計算されます。

フィールド	説明
match	トラフィックのクラスに指定された一致基準。この例では、フレーム リレー廃棄適性（DE）ビットは一致基準として指定されています。 使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
ip dscp tunnel	トンネル マーキングがトンネル型パケット ヘッダーの DSCP 値を 3 に設定するように設定されていることを示します。

ATM のトラフィック シェーピング オーバーヘッド アカウンティング：例

次の show policy-map interface コマンドの出力は、ATM オーバーヘッド アカウンティングがシェーピングに対してイネーブルになっているが、帯域幅に対してディセーブルになっていることを示しています。

```
Router# show policy-map interface

Service-policy output:unit-test
Class-map: class-default (match-any)
100 packets, 1000 bytes
30 second offered rate 800 bps, drop rate 0 bps
Match: any
shape (average) cir 154400, bc 7720, be 7720
target shape rate 154400
overhead accounting: enabled
bandwidth 30% (463 kbps)
overhead accounting: disabled
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(packets output/bytes output) 100/1000
```

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 *232 : show policy-map interface* フィールドの説明：*ATM* のトラフィック シェーピング オーバーヘッド アカウンティング用に設定

フィールド	説明
service-policy output	指定されたインターフェイスに適用されている出力サービス ポリシーの名前。
class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。

フィールド	説明
drop rate	クラスからパケットがドロップされるレート（単位：kbps）。ドロップレートは、offered rate から正常に送信されたパケット数を引いて計算されます。
match	トラフィックのクラスに指定された一致基準。この例では、フレーム リレー廃棄適性（DE）ビットは一致基準として指定されています。 使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
target shape rate	トラフィック シェーピングが指定したレートで有効になっていることを示します。
overhead accounting	トラフィック シェーピングのオーバーヘッド アカウンティングが有効か無効かを示します。
bandwidth	トラフィック キューイングに割り当てられた帯域幅のパーセンテージを示します。
overhead accounting:	トラフィック キューイングのオーバーヘッド アカウンティングが有効か無効かを示します。

HQF：例

show policy-map interface コマンドの次の出力には、ファスト イーサネット インターフェイス 0/0 の設定が表示されます。

（注） Cisco IOS リリース 12.4(20)T 以降のリリースの HQF イメージでは、トラフィック シェーピング クラスの遅延パケット カウンタおよび遅延バイト カウンタは削除されました。

```
Router# show policy-map interface FastEthernet0/0
 FastEthernet0/0

  Service-policy output: test1

    Class-map: class-default (match-any)
      129 packets, 12562 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 129/12562
      shape (average) cir 1536000, bc 6144, be 6144
      target shape rate 1536000
```

```
Service-policy : test2

  queue stats for all priority classes:

    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0

  Class-map: RT (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip dscp ef (46)
    Priority: 20% (307 kbps), burst bytes 7650, b/w exceed drops: 0


  Class-map: BH (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip dscp af41 (34)
    Queueing
    queue limit 128 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    bandwidth 40% (614 kbps)

  Class-map: BL (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip dscp af21 (18)
    Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    bandwidth 35% (537 kbps)
      Exp-weight-constant: 9 (1/512)
      Mean queue depth: 0 packets
      dscp     Transmitted   Random drop   Tail drop   Minimum   Maximum   Mark
               pkts/bytes    pkts/bytes    pkts/bytes  thresh    thresh    prob

      af21     0/0           0/0           0/0         100       400       1/10

  Class-map: class-default (match-any)
    129 packets, 12562 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: any

    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 129/12562
```

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 *233 : show policy-map interface* フィールドの説明：*HQF* 用に設定

フィールド	説明
FastEthernet	インターフェイスの名前。
service-policy output	指定されたインターフェイスに適用されている出力サービス ポリシーの名前。

フィールド	説明
class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-anyなど）もトラフィック クラスの横に表示されます。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。
drop rate	クラスからパケットがドロップされるレート（単位：kbps）。ドロップレートは、offered rateから正常に送信されたパケット数を引いて計算されます。
Match	トラフィックのクラスに指定された一致基準。 （注） 使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
Queueing	キューイングが有効になっていることを示します。
queue limit	ポリシー マップで設定されているクラス ポリシー用にキューで維持できるパケットの最大数。
bandwidth	トラフィック キューイングに割り当てられた帯域幅のパーセンテージを示します。
dscp	DiffServ コード ポイント（DSCP）。有効な値は次のとおりです。 • 0 ～ 63：DSCP 値（数値）。デフォルト値は 0 です。 • af1 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）優先順位値。 • default：デフォルトの DSCP 値。 • ef：完全優先転送（EF）DSCP 値。

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータのアカウント QoS 統計情報：例

次の例は、サブスクライバ統計情報用として、Cisco IOS XE リリース 2.6 以降の QoS：ポリシー集約拡張機能に関連付けられた新規出力フィールドを示しています。この新規出力フィールドは、「アカウント QoS 統計情報（Account QoS Statistics）」というラベルで始まります。

```
Router# show policy-map interface port-channel 1.1

Port-channel1.1
   Service-policy input: input_policy
     Class-map: class-default (match-any)
       0 packets, 0 bytes
       5 minute offered rate 0000 bps, drop rate 0000 bps
       Match: any
       QoS Set
       dscp default
       No packet marking statistics available
   Service-policy output: Port-channel_1_subscriber
     Class-map: EF (match-any)
       105233 packets, 6734912 bytes
       5 minute offered rate 134000 bps, drop rate 0000 bps
       Match: dscp ef (46)
       Match: access-group name VLAN_REMARK_EF
       Match: qos-group 3
       Account QoS statistics
         Queueing
           Packets dropped 0 packets/0 bytes
       QoS Set
       cos 5
       No packet marking statistics available
       dscp ef
       No packet marking statistics available
     Class-map: AF4 (match-all)
       105234 packets, 6734976 bytes
       5 minute offered rate 134000 bps, drop rate 0000 bps
       Match: dscp cs4 (32)
       Account QoS statistics
         Queueing
           Packets dropped 0 packets/0 bytes
       QoS Set
       cos 4
       No packet marking statistics available
     Class-map: AF1 (match-any)
       315690 packets, 20204160 bytes
       5 minute offered rate 402000 bps, drop rate 0000 bps
       Match: dscp cs1 (8)
       Match: dscp af11 (10)
       Match: dscp af12 (12)
       Account QoS statistics
         Queueing
           Packets dropped 0 packets/0 bytes
       QoS Set
       cos 1
       No packet marking statistics available
     Class-map: class-default (match-any) fragment Port-channel_BE
       315677 packets, 20203328 bytes
       5 minute offered rate 402000 bps, drop rate 0000 bps
       Match: any
       Queueing
         queue limit 31250 bytes
         (queue depth/total drops/no-buffer drops) 0/0/0
         (pkts output/bytes output) 315679/20203482
         bandwidth remaining ratio 1
```

Cisco Catalyst 4000 シリーズ ルータ：例

次の例は、ポリサー統計情報（パケットカウントおよびバイトカウント）を表示する方法を示しています。出力には、適切なカウント（パケットまたはバイト）のみが実数で表示されます。

```
Router# show policy-map interface GigabitEthernet 3/1 input

GigabitEthernet3/1
  Service-policy input: in1
    Class-map: p1 (match-all)
      0 packets
      Match:  precedence 1
           QoS Set
             ip precedence 7
      police:
          cir 20 %
          cir 200000000 bps, bc 6250000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps
    Class-map: class-default (match-any)
      10000000 packets
      Match: any
      police:
          cir 20 %
          cir 200000000 bps, bc 6250000 bytes
        conformed 174304448 bytes; actions:
          transmit
        exceeded 465695552 bytes; actions:
          drop
        conformed 4287000 bps, exceed 11492000 bps
```

Cisco CMTS ルータ：例

次の例は、インターフェイスにアタッチされている入力サービス ポリシーおよび出力サービス ポリシーの統計情報および設定を表示する方法を示しています。

```
Router# show policy-map interface GigabitEthernet 1/2/0

Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *23:02:40.857 pst Thu Mar 3 2011

 GigabitEthernet1/2/0

  Service-policy input: policy-in

    Class-map: class-exp-0 (match-all)
      6647740 packets, 9304674796 bytes
      30 second offered rate 3234000 bps, drop rate 0 bps
      Match: mpls experimental topmost 0
      QoS Set
        precedence 3
          Packets marked 6647740
```

```
  Class-map: class-default (match-any)
    1386487 packets, 1903797872 bytes
    30 second offered rate 658000 bps, drop rate 0 bps
    Match: any

Service-policy output: policy-out

  Class-map: class-pre-1 (match-all)
    2041355 packets, 2857897000 bytes
    30 second offered rate 986000 bps, drop rate 0 bps

    Match: ip precedence 1
    QoS Set
      mpls experimental topmost 1
        Packets marked 2041355

  Class-map: class-default (match-any)
    6129975 packets, 8575183331 bytes
    30 second offered rate 2960000 bps, drop rate 0 bps
    Match: any
```

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 *234 : show policy-map interface* フィールドの説明：*Cisco Catalyst 4000* シリーズ ルータ

フィールド	説明
class-map	トラフィック クラスを表示します。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-anyなど）もトラフィック クラスの横に表示されます。
conformed	指定した比率に適合するパケットに実行されるアクションを表示します。また、アクションが実施されたパケット数とバイト数も表示します。
切断	指定したクラスに属するすべてのパケットに対してパケット廃棄処理が設定されていることを示します。
exceeded	指定した比率を超えるパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。
match	トラフィックのクラスに指定された一致基準。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
police	**police** コマンドがトラフィック ポリシングを有効にするように設定されていることを示します。また、パケットのマーキングに使用される、指定された CIR、適合バースト サイズ、最大情報レート（PIR）、およびピークバースト サイズも表示します。
QoS Set	特定のクラスに対して QoS グループ（セット）が設定されていることを示します。
service-policy input	指定されたインターフェイスに適用されている入力サービス ポリシーの名前。

擬似回線ポリシー マップ情報の表示：例

次の例は、擬似回線インターフェイス用に設定されたクラス マップを表示する方法を示しています。

```
Router# show policy-map interface pseudowire2
 pseudowire2
  Service-policy output: pw_brr

    Class-map: prec1 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 1
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 1

    Class-map: prec2 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 2
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 2

    Class-map: prec3 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 3
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 3

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 4
Device#
```

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 *235 : show policy-map* フィールドの説明：擬似回線ポリシー マップ情報

フィールド	説明
bandwidth	トラフィック キューイングに割り当てられた帯域幅のパーセンテージを示します。

フィールド	説明
Class-map	トラフィック クラスを表示します。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
Match	トラフィックのクラスに指定された一致基準。
packets、bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
Queueing	キューイングが有効になっていることを示します。
queue limit	ポリシー マップで設定されているクラス ポリシー用にキューで維持できるパケットの最大数。
service-policy output	指定されたインターフェイスに適用されている出力サービス ポリシーの名前。

関連コマンド

Command	Description
bandwidthremainingratio	未使用の帯域幅の量を計算して、輻輳時にキューに割り当てるために、クラス キューおよびサブインターフェイスレベル キューの帯域幅残量割合を指定します。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
compressionheaderip	特定のクラスに RTP または TCP IP ヘッダー圧縮を設定します。
drop	特定のクラスに属するパケットを廃棄するトラフィック クラスを設定します。
matchfr-dlci	クラス マップの一致基準としてフレームリレー DLCI 番号を指定します。
matchpacketlength(class-map)	IP ヘッダーのレイヤ 3 パケットの長さをクラス マップ内の一致条件として指定します。
police	トラフィック ポリシングを設定します。
police(percent)	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
police(tworates)	2 レート、CIR および PIR を使用してトラフィック ポリシングを設定します。
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

Command	Description
priority	トラフィック クラスには、低遅延動作が指定されなければならないことを指定し、複数のプライオリティ キューを設定します。
random-detectecn	ECN をイネーブルにします。
shape(percent)	インターフェイスで使用可能な帯域幅の割合（%）に基づいて、平均レート トラフィック シェーピングとピーク レート トラフィック シェーピングを指定します。
showclass-map	すべてのクラス マップおよびその一致基準を表示します。
showframe-relaypvc	フレームリレー インターフェイス対応 PVC に関する統計情報を表示します。
showinterfaces	ルータまたはアクセス サーバ上に設定されているすべてのインターフェイスの統計情報を表示します。
showmlsqos	MLS QoS 情報を表示します。
showpolicy-map	指定されたサービス ポリシーマップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapclass	指定されたポリシーマップの指定されたクラスの設定を表示します。
showtable-map	指定されたテーブルマップまたはすべてのテーブルマップの設定を表示します。
table-map(valuemapping)	1 つの packet-marking 値を別の値にマッピングおよび変換するための、マッピング テーブルを作成します。

show policy-map interface brief

インターフェイスにアタッチされたアクティブなポリシーマップのみに関する情報を表示するには、特権 EXEC モードで **showpolicy-mapinterfacebrief** コマンドを使用します。

show policy-map interface [{**input**|**output**}] **brief** [*policy-map-name*] [**vrf** [*vrf-id*]] **[timestamp]**

構文の説明

input	（任意）アクティブな入力ポリシーマップに関する情報のみが表示されることを示します。
output	（任意）アクティブな出力ポリシーマップに関する情報のみが表示されることを示します。
brief	すべてのアクティブなポリシーマップ（入力ポリシーマップと出力ポリシーマップの両方）およびポリシーマップのアタッチ先となるインターフェイスの名前が表示されることを示します。アクティブな入力ポリシーマップがまず表示され、その後に出力ポリシー マップが続きます。
policy-map-name	（任意）表示されるアクティブなポリシー マップの名前。
vrf	（任意）バーチャルプライベートネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスのアクティブなポリシー マップが表示されることを示します。
vrf-id	（任意）特定の VRF 識別子。
timestamp	（任意）ポリシーマップがアタッチされた日付と時刻が表示され、併せてポリシー マップをアタッチしたユーザの ID も表示されることを示します。

コマンド デフォルト

オプションのキーワードや引数を指定しないと、すべてのポリシーマップ（アクティブでないものも含む）が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(28)SB	このコマンドが導入されました。
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。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

showpolicy-mapinterfacebrief コマンドは、アクティブなポリシー マップおよびそれらのポリシーマップのアタッチ先となるインターフェイスの名前を表示します。アクティブなポリシーマップとは、インターフェイスにアタッチされるポリシー マップのことです。

オプションのキーワードおよび引数を使用すると、VPN、タイムスタンプ、およびユーザ ID について表示される情報を調整できます。

オプションのキーワードや引数を指定しないと、すべてのポリシーマップ（アクティブでないものも含む）が表示されます。

報告される VPN 情報

showpolicy-mapinterfacebrief コマンドは、VPN を使用するアプリケーションの VRF インターフェイスに使用できます。VRF インターフェイスを指定するには、*vrf-id* 引数を指定した **vrf** キーワードを使用します。

報告されるタイムスタンプおよびユーザ ID 情報

showpolicy-mapinterfacebrief コマンドでオプションの **timestamp** キーワードを使用すると、ポリシーマップがインターフェイスにアタッチされた時刻と日付が表示されます。時刻と日付の情報の他に、インターフェイスにポリシーマップをアタッチした個人の名前（つまり、ユーザ ID）も表示されます。

（注） ネットワーク ソフトウェアをリロード（再インストール）すると、ネットワーク上のインターフェイスにアタッチされたポリシーマップについて取得されたタイムスタンプ情報（時刻と日付の情報）は保持されません。代わりに、表示される日付と時刻の情報は、ソフトウェアがリロードされた日付と時刻になります。

ユーザ情報を取得する方法

表示に含まれるユーザ情報は、ルータにログインする際に入力した情報から取得されます。たとえば、SSHセキュアシェルユーティリティを使用してルータにログインする場合は、通常、ユーザ名とパスワードを入力します。ただし、常にユーザ情報を取得できるとは限りません。ユーザ情報を取得できないインスタンスには、次のものがあります。

- すべてのルータでログイン時にユーザ情報が必要になるわけではありません。このため、ルータにログインするときにユーザ名を入力するように求められない場合があります。
- DOS 環境で Telnet ユーティリティを使用してコンソール ポートに接続している場合、ユーザ情報を入力する必要はありません。
- システムの制約やその他の要因により、ユーザ情報を取得できません。

ユーザ情報を取得できない場合、「by unknown」という語句が表示されます。

階層的なポリシー マップ情報

階層的なポリシー マップ構造の場合、親ポリシー マップに関する情報のみが表示されます。子ポリシー マップに関する情報は表示されません。

ATM PVCs

ATM 相手先固定接続（PVC）では、ATM PVC が正常に機能していない場合（つまり、ATM PVC が「ダウン」している場合）、ポリシー マップはインターフェイスに関連付けられたままになりません。このため、ATM PVC がダウンし、ポリシー マップがインターフェイスにアタッチされている場合、**showpolicy-mapinterfacebrief** コマンドはコマンド出力にポリシーマップに関する情報を含めません。

例

showpolicy-mapinterfacebrief コマンドが表示する情報は、指定するオプションのキーワードおよび引数によって異なります。

以降のセクションでは、コマンドで使用される重要なキーワードと引数の組み合わせをリストし、それらに対応して表示される情報について説明します。

show policy-map interface brief コマンドの例

showpolicy-mapinterfacebrief コマンドは、アタッチされたすべてのポリシー マップ（入力ポリシーマップと出力ポリシーマップの両方）を表示し、併せてポリシーマップのアタッチ先となるインターフェイスに関する情報も表示します。入力ポリシーマップがまず表示され、その後に出力ポリシー マップが続きます。

```
Service-policy input: policyname1
interface s2/0/1
interface s6/0/0
Service-policy output: policyname1interface s2/0/1 interface s6/0/0
```

show policy-map interface brief timestamp コマンドの例

showpolicy-mapinterfacebrieftimestamp コマンドは、アタッチされたすべてのポリシーマップ（入力ポリシー マップと出力ポリシー マップの両方）を表示し、併せてポリシーマップのアタッチ先となるインターフェイスに関する情報も表示します。入力ポリシー マップがまず表示され、その後に出力ポリシー マップが続きます。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシーマップをアタッチした個人のユーザ ID も表示します。

```
Service-policy input: parentpolicy1
Service-policy input: childpolicy1
interface s2/0/1 - applied 20:43:04 on 25/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
Service-policy output: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
```

show policy-map interface brief policy-map-name コマンドの例

showpolicy-mapinterfacebrief*policy-map-name* コマンドは、入力ポリシー マップまたは出力ポリシーマップとしてアタッチされているポリシーマップを表示し、併せてポリ

シー マップのアタッチ先となるインターフェイスに関する情報も表示します。*policy-map-name* 引数で指定されているポリシー マップのみが表示されます。

たとえば、**showpolicy-mapinterfacebriefpolicyname1** コマンドの表示は次のようになります。

```
Service-policy input: policyname1
interface s2/0/1
interface s6/0/0
Service-policy output: policyname1
interface s1/0/2
interface s3/0/0
```

show policy-map interface brief policy-map-name timestamp コマンドの例

showpolicy-mapinterfacebrief*policy-map-name***timestamp** コマンドは、入力ポリシーマップまたは出力ポリシーマップとしてアタッチされているポリシーマップを表示し、併せてポリシー マップのアタッチ先となるインターフェイスに関する情報も表示します。*policy-map-name* 引数で指定されているポリシー マップのみが表示されます。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシーマップをアタッチした個人のユーザ ID も表示します。

たとえば、**showpolicy-mapinterfacebriefpolicyname2timestamp** コマンドの表示は次のようになります。

```
Service-policy input: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
Service-policy output: policyname2
interface s4/0/2 - applied 12:47:04 on 24/12/01 by user1
interface s7/0/1 - applied 14:43:04 on 25/12/01 by user1
```

show policy-map interface output brief コマンドの例

showpolicy-mapinterfaceoutputbrief コマンドは、アタッチされた出力ポリシー マップを表示し、併せてそれらのアタッチ先となるインターフェイスに関する情報も表示します。

```
Service-policy output: policyname1
```

show policy-map interface output brief timestamp コマンドの例

showpolicy-mapinterfaceoutputbrieftimestamp コマンドは、アタッチされた出力ポリシーマップを表示し、併せてそれらのアタッチ先となるインターフェイスに関する情報も表示します。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシーマップをアタッチした個人のユーザ ID も表示します。

```
Service-policy output: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
```

show policy-map interface input brief コマンドの例

showpolicy-mapinterfaceinputbrief コマンドは、アタッチされた入力ポリシーマップを表示し、併せてそれらのアタッチ先となるインターフェイスに関する情報も表示します。

```
Service-policy input: policyname2
interface s2/0/2
interface s6/0/1
```

show policy-map interface input brief timestamp コマンドの例

showpolicy-mapinterfaceinputbrieftimestamp コマンドは、アタッチされた入力ポリシーマップを表示し、併せてそれらのアタッチ先となるインターフェイスに関する情報も表示します。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシーマップをアタッチした個人のユーザ ID も表示します。

```
Service-policy input: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
```

show policy-map interface output brief policy-map-name コマンドの例

showpolicy-mapinterfaceoutputbrief*policy-map-name* コマンドは、アタッチされた出力ポリシーマップを表示し、併せてそのアタッチ先となるインターフェイスに関する情報も表示します。*policy-map-name* 引数で指定されているポリシーマップのみが表示されます。

たとえば、**showpolicy-mapinterfaceoutputbriefpolicyname1** コマンドの表示は次のようになります。

```
Service-policy output: policyname1
interface s2/0/1
interface s6/0/0
```

show policy-map interface output brief policy-map-name timestamp コマンドの例

showpolicy-mapinterfaceoutputbrief*policy-map-name***timestamp** コマンドは、アタッチされた出力ポリシーマップを表示し、併せてそのアタッチ先となるインターフェイスに関する情報も表示します。*policy-map-name* 引数で指定されているポリシーマップのみが表示されます。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシーマップをアタッチした個人のユーザ ID も表示します。

たとえば、**showpolicy-mapinterfaceoutputbriefpolicyname2timestamp** コマンドの表示は次のようになります。

```
Service-policy output: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
```

show policy-map interface input brief policy-map-name コマンドの例

showpolicy-mapinterfaceinputbrief*policy-map-name* コマンドは、アタッチされた入力ポリシーマップを表示し、併せてそのアタッチ先となるインターフェイスに関する情報も表示します。*policy-map-name* 引数で指定されているポリシーマップのみが表示されます。

たとえば、**showpolicy-mapinterfaceinputbriefpolicyname1** コマンドの表示は次のようになります。

```
Service-policy input: policyname1
interface s2/0/1
interface s6/0/0
```

show policy-map interface input brief policy-map-name timestamp コマンドの例

showpolicy-mapinterfaceinputbrief*policy-map-name***timestamp** コマンドは、アタッチされた入力ポリシーマップを表示し、併せてそのアタッチ先となるインターフェイスに関する情報も表示します。*policy-map-name* 引数で指定されているポリシーマップのみが表示されます。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシーマップをアタッチした個人のユーザ ID も表示します。

たとえば、**showpolicy-mapinterfaceinputbriefpolicyname2timestamp** コマンドの表示は次のようになります。

```
Service-policy input: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
```

show policy-map interface brief vrf コマンドの例

showpolicy-mapinterfacebriefvrf コマンドは、すべてのポリシーマップ（入力ポリシーマップと出力ポリシーマップの両方）を表示し、併せてポリシーマップのアタッチ先となるインターフェイスおよび VRF に関する情報も表示します。

```
Service-policy input: policyname1
VRFA   interface s2/0/1
VRFB   interface s6/0/0
Service-policy output: policyname2
VRFC   interface s2/0/2
VRFB   interface s6/0/1
```

show policy-map interface brief vrf timestamp コマンドの例

showpolicy-mapinterfacebriefvrftimestamp コマンドは、すべてのポリシー マップ（入力ポリシー マップと出力ポリシー マップの両方）を表示し、併せてポリシー マップのアタッチ先となるインターフェイスおよび VRF に関する情報も表示します。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシーマップをアタッチした個人のユーザ ID も表示します。

```
Service-policy input: policyname1
VRFA   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
VRFB   interface s6/0/0 - applied 21:47:04 on 23/12/01 by user1
Service-policy output: policyname2
VRFC   interface s2/0/3 - applied 20:47:04 on 23/12/01 by user1
VRFD   interface s6/0/2 - applied 20:49:04 on 21/12/01 by user1
```

ネットワーク構成によっては、ポリシー マップが初期状態でインターフェイスにアタッチされ、その後インターフェイスをVRFインターフェイスとして機能するように設定できる場合があります。この種類のネットワーク構成では、タイムスタンプ情報にはポリシーマップをインターフェイスにアタッチした時間が表示されます。この表示には、インターフェイスがVRFインターフェイスとして機能するように設定された時間は含まれません。ポリシーマップがインターフェイスにアタッチされた時間のみを表示するというのは、次の段落で説明されている他のネットワーク構成のシナリオにも当てはまります。

ネットワーク構成にはこの他に、次のシナリオで説明するように、VRF が複数のインターフェイスにアタッチされているものもあります。

- ポリシーマップがインターフェイスとVRFのどちらにもアタッチされています。このネットワーク構成では、すべてのインターフェイスが次のようにVRFの表示でポリシー マップ名の下に表示されます。

```
Service-policy input: policyname1
VRF1 interface s2/0/1 - applied 21:47:37 on 23/12/01 by user1
     interface atm0/0 - applied 11:37:57 on 21/11/01 by user1
```

- ポリシー マップが特定の VRF のアタッチ先となるどのインターフェイスにもアタッチされていません。このネットワーク構成では、そのポリシー マップが設定されている VRF インターフェイスのみが表示されます。

show policy-map interface brief policy-map-name vrf timestamp コマンドの例

showpolicy-mapinterfacebrief*policy-map-name***vrftimestamp** コマンドは、入力ポリシー マップまたは出力ポリシー マップとしてアタッチされているポリシー マップを表示し、併せてポリシー マップのアタッチ先となるインターフェイスおよび VRF に関する情報も表示します。*policy-map-name* 引数で指定されているポリシー マップのみが表示されます。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシー マップをアタッチした個人のユーザ ID も表示します。

たとえば、**showpolicy-mapinterfacebriefpolicyname1vrftimestamp** コマンドの表示は次のようになります。

```
Service-policy input: policyname1
VRF1   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
Service-policy output: policyname1
VRF2   interface s6/0/1 - applied 21:47:04 on 23/12/01 by user1
```

show policy-map interface brief policy-map-name vrf vrf-id timestamp コマンドの例

showpolicy-mapinterfacebrief*policy-map-name***vrf***vrf-id***timestamp** コマンドは、すべてのポリシー マップ（入力ポリシー マップと出力ポリシー マップの両方）を表示し、併せてポリシー マップのアタッチ先となるインターフェイスおよび VRF に関する情報も表示します。*policy-map-name* 引数および *vrf-id* 引数で指定されているポリシー マップと VRF のみが表示されます。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシー マップをアタッチした個人のユーザ ID も表示します。

たとえば、**showpolicy-mapinterfacebriefpolicyname1vrfVRFAtimestamp** コマンドの表示は次のようになります。

```
Service-policy input: policyname1
VRFA   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
Service-policy output: policyname1
VRFA   interface s6/0/1 - applied 21:47:04 on 23/12/01 by user1
```

show policy-map interface output brief vrf コマンドの例

showpolicy-mapinterfaceoutputbriefvrf コマンドは、アタッチされた出力ポリシー マップを表示し、併せてポリシーマップのアタッチ先となるインターフェイスおよびVRFに関する情報も表示します。

```
Service-policy output: policyname2
VRFC   interface s2/0/2
VRFA   interface s6/0/1
```

show policy-map interface output brief vrf timestamp コマンドの例

showpolicy-mapinterfaceoutputbriefvrftimestamp コマンドは、アタッチされた出力ポリシーマップを表示し、併せてポリシーマップのアタッチ先となるインターフェイスおよび VRF に関する情報も表示します。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシーマップをアタッチした個人のユーザ ID も表示します。

```
Service-policy output: policyname2
VRFC   interface s2/0/2 - applied 21:47:04 on 23/12/01 by user1
VRFA   interface s6/0/1 - applied 21:47:04 on 23/12/01 by user1
```

show policy-map interface input brief vrf コマンドの例

showpolicy-mapinterfaceinputbriefvrf コマンドは、アタッチされた入力ポリシー マップを表示し、併せてポリシーマップのアタッチ先となるインターフェイスおよびVRFに関する情報も表示します。

```
Service-policy input: policyname1
VRFA   interface s2/0/1
VRFB   interface s6/0/0
Service-policy input: policyname2
VRFC   interface s2/0/2
VRFB   interface s6/0/1
```

show policy-map interface input brief vrf timestamp コマンドの例

showpolicy-mapinterfaceinputbriefvrftimestamp コマンドは、アタッチされた入力ポリシーマップを表示し、併せてポリシーマップのアタッチ先となるインターフェイスおよび VRF に関する情報も表示します。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシーマップをアタッチした個人のユーザ ID も表示します。

```
Service-policy input: policyname1
VRFA   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
VRFB   interface s6/0/0 - applied 21:47:04 on 23/12/01 by user1
Service-policy input: policyname2
VRFC   interface s2/0/3 - applied 20:47:04 on 23/12/01 by user1
VRFD   interface s6/0/2 - applied 20:49:04 on 21/12/01 by user1
```

show policy-map interface input brief vrf vrf-id コマンドの例

showpolicy-mapinterfaceinputbriefvrf*vrf-id* コマンドは、アタッチされた入力ポリシーマップを表示し、併せてポリシーマップのアタッチ先となるインターフェイスおよびVRF に関する情報も表示します。*vrf-id* 引数で指定されている VRF にアタッチされたポリシー マップのみが表示されます。

たとえば、**showpolicy-mapinterfaceinputbriefvrfVRFA** コマンドの表示は次のようになります。

```
Service-policy input: policyname1
VRFA   interface s2/0/1
Service-policy input: policyname2
VRFA   interface s6/0/1
```

show policy-map interface output brief vrf vrf-id コマンドの例

showpolicy-mapinterfaceoutputbriefvrf*vrf-id* コマンドは、アタッチされた出力ポリシーマップを表示し、併せてポリシーマップのアタッチ先となるインターフェイスおよびVRF に関する情報も表示します。*vrf-id* 引数で指定されている VRF にアタッチされたポリシー マップのみが表示されます。

たとえば、**showpolicy-mapinterfaceoutputbriefvrfVRFB** コマンドの表示は次のようになります。

```
Service-policy output: policyname1
VRFB   interface s2/0/1
Service-policy output: policyname2
VRFB   interface s6/0/1
```

show policy-map interface input brief vrf vrf-id timestamp コマンドの例

showpolicy-mapinterfaceinputbriefvrf*vrf-id***timestamp** コマンドは、アタッチされた入力ポリシーマップを表示し、併せてポリシーマップのアタッチ先となるインターフェイスおよびVRF に関する情報も表示します。*vrf-id* 引数で指定されている VRF にアタッチされたポリシー マップのみが表示されます。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシーマップをアタッチした個人のユーザ ID も表示します。

たとえば、**showpolicy-mapinterfaceinputbriefvrfVRFAtimestamp** コマンドの表示は次のようになります。

```
Service-policy input: policyname1
VRFA   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
Service-policy input: policyname2
VRFA   interface s6/0/1 - applied 21:47:04 on 23/12/01 by user1
```

show policy-map interface output brief vrf vrf-id timestamp コマンドの例

showpolicy-mapinterfaceoutputbriefvrf*vrf-id***timestamp** コマンドは、アタッチされた出力ポリシーマップを表示し、併せてポリシーマップのアタッチ先となるインターフェイスおよび VRF に関する情報も表示します。*vrf-id* 引数で指定されている VRF にアタッチされたポリシー マップのみが表示されます。

timestamp キーワードは、ポリシー マップが特定のインターフェイスにアタッチされた時刻と日付を表示し、併せてインターフェイスにポリシーマップをアタッチした個人のユーザ ID も表示します。

たとえば、**showpolicy-mapinterfaceoutputbriefvrfVRFBtimestamp** コマンドの表示は次のようになります。

```
Service-policy output: policyname1
VRFB   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
Service-policy output: policyname2
VRFB   interface s6/0/1 - applied 21:47:04 on 23/12/01 by user1
```

次の表では、さまざまな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 *236 : show policy-map interface brief* フィールドの説明

フィールド	説明
Service-policy output: policyname2	出力ポリシー マップ名。
Service-policy input: policyname2	入力ポリシー マップ名。
interface s2/1/0	ポリシー マップのアタッチ先となるインターフェイス。
VRFA	ポリシー マップのアタッチ先となる VRF。
applied 21:47:04 on 23/12/01	インターフェイスまたは VRF にポリシー マップをアタッチした日付と時刻。
by user1	インターフェイスまたは VRF にポリシー マップをアタッチした個人のユーザ ID。

関連コマンド

コマンド	説明
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

show policy-map interface port-channel

EFP のポリシー マップ コンフィギュレーションを検証するには、**show policy-map interface port-channel** コマンドを使用します。

show policy-map interface port-channel

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

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
XE 3.18 SP	このコマンドのサポートが ASR 900 シリーズ ルータに追加されました。

例

次の例は、EFP のポリシー マップ コンフィギュレーションを検証する方法を示しています。

```
Router#show policy-map int po2 service instance 1 output
Port-channel2: EFP 1
Service-policy output: l1c
Class-map: qos4 (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 4
Queueing
queue limit 74472 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth 11% (110000 kbps)
Class-map: qos1 (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 1
Queueing
queue limit 68266 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth 12% (120000 kbps)
Class-map: qos2 (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 2
Queueing
queue limit 43115 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth 19% (190000 kbps)
Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
Queueing
queue limit 54613 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 0/0/0
```

```
 (pkts output/bytes output) 0/0
bandwidth 15% (150000 kbps)
```

show policy-map interface service group

メンバーがインターフェイスにアタッチされているサービス グループのポリシー マップ情報を表示するには、特権 EXEC モードで **showpolicy-mapinterfaceservicegroup** コマンドを使用します。

show policy-map interface *type number* **service group** [*service-group-identifier*]

構文の説明

type	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	インターフェイス番号。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。
service-group-identifier	（任意）サービス グループ番号。既存のサービス グループの番号を入力します。

コマンド デフォルト

サービス グループ番号を指定しないと、すべてのサービス グループのポリシー マップ情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRE	このコマンドが導入されました。

使用上のガイドライン

メンバーがインターフェイスまたはポート チャネルにアタッチされている 1 つ以上のサービス グループに関する情報を表示するには、**showpolicy-mapinterfaceservicegroup** コマンドを使用します。表示される情報には、インターフェイスまたはポート チャネルにアタッチされたポリシー マップ、それらのポリシー マップに設定されている QoS 機能（たとえば、トラフィック ポリシングやトラフィック キューイング）、対応するパケット統計情報などがあります。このコマンドを使用する前に、ポリシー マップおよびサービス グループを作成する必要があります。

例

次に、**showpolicy-mapinterfaceservicegroup** コマンドの例を示します。この例では、サービス グループ 1 を指定しています。サービス グループ 1 には、2 つのポリシー マップ（サービス ポリシー）policy1 と policy2 が含まれています。ポリシー 1 のポリシー マップでトラフィック ポリシングが有効になっています。ポリシー 2 のポリシー マップでトラフィック キューイングが有効になっています。

```
Router# show policy-map interface gigabitEthernet 9/5 service group 1

 GigabitEthernet9/5: Service Group 1
```

```
Service-policy input: policy1

  Class-map: class-default (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any
    police:
        cir 200000 bps, bc 6250 bytes
      conformed 0 packets, 0 bytes; actions:
        transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps

Service-policy output: policy2

Counters last updated 00:00:34 ago

  Class-map: class-default (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any
    Queueing
    queue limit 131072 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    bandwidth remaining ratio 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 *237 : show policy-map interface service group* フィールドの説明

フィールド	説明
GigabitEthernet9/5: Service Group 1	インターフェイスおよびサービス グループ番号。
Service-policy input: policy1 Service-policy output: policy2	サービス ポリシー（ポリシー マップ）名およびそのポリシーがインターフェイス上で入力方向にあるのか出力方向にあるのか。
police	トラフィック ポリシングが有効になっていることを示します。トラフィック ポリシングに関連付けられた統計情報も表示されます。
Queueing	トラフィック キューイング メカニズムが有効になっていることを示します。トラフィック キューイングに関連付けられた統計情報も表示されます。

関連コマンド

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

コマンド	説明
showpolicy-mapinterfaceserviceinstance	インターフェイスまたはポート チャネルの下に特定のサービス インスタンスのポリシー マップ情報を表示します。

show policy-map interface service instance

ポート チャネルの下に特定のサービス インスタンスのポリシー マップ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 policy-map interface service instance コマンドを使用します。

show policy-map interface x service instance y

構文の説明

x	インターフェイスまたはポート チャネルの番号。
y	サービス インスタンスの番号。

コマンド モード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(33)SRC	このコマンドが Cisco 7600 シリーズ ルータに追加されました。

例

次の例は、ポート チャネル 1 の下で特定のサービス インスタンス 1 上にある階層型ポリシーのポリシー マップ出力を示しています。

```
Router# show policy-map interface port-channel 1 service instance 1
Port-channel1: EFP 1
  Service-policy output: hqos-pc-brr
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 5000 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 20000000, bc 80000, be 80000
      target shape rate 20000000
      bandwidth remaining ratio 2
      Service-policy : flat-pc-brr
        Class-map: cos5 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps

          Match: cos  5
          Queueing
          queue limit 2500 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
          shape (average) cir 10000000, bc 40000, be 40000
          target shape rate 10000000
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
```

```
Match: any
Queueing
queue limit 2500 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 10000000, bc 40000, be 40000
target shape rate 10000000
```

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 *238 : show policy-map interface service instance* フィールドの説明。サービス ポリシー出力名、クラス マップ名、および一致基準情報に続いて、丸カッコに囲まれた数字が表示されます。この番号は、*Cisco*内部だけで使用されるものであり、無視できます。

フィールド	説明
クラスまたはサービス ポリシーに関連付けられたフィールド	
Service-policy output	指定されたインターフェイスまたはVCに適応されている出力サービス ポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
packets and bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。 （注） 発信インターフェイス全体でパケットが圧縮されている場合、パケット圧縮によって達成された改善パケット レートは、offered rate には反映されません。また、パケットがトンネルの組み合わせ（例：Generic Routing Encapsulation（GRE）トンネルおよびIP Security（IPSec）トンネル）に入る前に圧縮されている場合、offered rate は、一般にトンネル カプセル化に関連付けられたすべての追加オーバーヘッドを含みません。offered rate は、設定に応じて、オーバーヘッドを含まない、*1* つのトンネル カプセル化だけのオーバーヘッドを含む、または、すべてのトンネル カプセル化のオーバーヘッドを含むのいずれかです。GRE および IPSec トンネル設定の多くで、offered rate は、GRE トンネル カプセル化のオーバーヘッドだけを含みます。

フィールド	説明
drop rate	クラスからパケットがドロップされるレート（単位：kbps）。ドロップ レートは、offered rate から正常に送信されたパケット数を引いて計算されます。
Match	トラフィックのクラスに指定された一致基準。選択要素には、IP precedence、IP Diffserv コード ポイント（DSCP）値、マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）値、アクセス グループ、および、QoS グループなどの基準があります。使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
キューイングに対応付けられているフィールド（イネーブルの場合）	
Output queue	このトラフィックのクラスに割り当てられている Weighted Fair Queueing（WFQ）カンバセーション。
Bandwidth	このクラスに設定されている帯域幅（kbps または割合のいずれか）、および、バーストサイズ
pkts matched/bytes matched	キューに入れられた、このクラスに一致するパケット数（バイト単位でも表示）。この数は、任意の時点でキューイングされた一致パケットの合計数を表します。このクラスに一致するパケットは、輻輳が存在するときだけキューイングされます。パケットがクラスに一致しているが、ネットワークが混雑していないためにキューイングされなかった場合、それらのパケットはこの合計に含まれません。しかし、プロセス スイッチングが使用されている場合は、ネットワークが混雑していない場合でもパケット数は常に加算されます。
depth/total drops/no-buffer drops	このクラスに対して廃棄されたパケット数。No-buffer は、パケットをサービスするメモリ バッファが存在しないことを示します。
Weighted Random Early Detection（WRED）に対応付けられているフィールド（イネーブルである場合）	
exponential weight	WRED パラメータ グループのために平均キュー サイズの計算に使用される指数。

フィールド	説明
mean queue depth	インターフェイスの実際のキューの深さおよび指数重み付け定数に基づいたキューの深さの平均。これは、変動する平均です。最小しきい値および最大しきい値と、この値とを比較してドロップの是非を決定します。
class	IP precedence レベル。
Transmitted pkts/bytes	WRED を通過し、WRED にドロップされなかったパケット数（バイト単位でも表示）。 （注） パケットを格納するのに十分なメモリがバッファにない場合、パケットが WRED を通過した後でドロップされます。バッファに十分なメモリがないためにドロップされた（「ノーバッファ ドロップ」とも呼ばれる）パケットは、WRED パケット カウンタに算入されます。
Random drop pkts/bytes	キューの深さの平均が、指定された IP precedence レベルの最小しきい値と最大しきい値の間である場合に、ランダムにドロップされたパケット数（バイト単位でも表示）。
Tail drop pkts/bytes	キューの深さの平均が、指定された IP precedence レベルの最大しきい値を上回る場合に、ランダムにドロップされたパケット数（バイト単位でも表示）。
Minimum thresh	最小しきい値を表します。パケット数の WRED 最小しきい値。
Maximum thresh	最大しきい値を表します。パケット数の WRED 最大しきい値。
Mark prob	マーク確率。平均キューの深さが最大しきい値の場合にドロップされたパケットの割合。
トラフィック シェーピングと対応付けられたフィールド（イネーブルである場合）	
Target Rate	シェーピング トラフィックに使用されるレート。
Byte Limit	インターバルあたりの送信最大バイト数。次のように計算されます。 ((Bc+Be) /8) x 1
Sustain bits/int	認定バースト（Bc）レート。
Excess bits/int	超過バースト（Be）レート。
Interval (ms)	ミリ秒（ms）単位の時間間隔の値。

フィールド	説明
Increment (bytes)	各時間間隔の間にトラフィック シェーピングのトークン バケット内に受信したクレジット数（単位：バイト）。
Queue Depth	トラフィック シェーパーの現在のキューの深さ。
Packets	トラフィック シェーパー システムに入ったパケットの合計数。
Bytes	トラフィック シェーパー システムに入ったバイト合計数。
Packets Delayed	送信される前に、トラフィック シェーパーのキュー内で遅延したパケットの合計数。
Bytes Delayed	送信される前に、トラフィック シェーパーのキュー内で遅延したバイトの合計数。
Shaping Active	トラフィック シェーパーがアクティブかどうかを示します。たとえば、トラフィック シェーパーがアクティブであり、送信されたトラフィックがトラフィック シェーピング レートを上回る場合、フィールドに「yes」が表示されます。

関連コマンド

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

show policy-map mgre

特定の QoS ポリシーがトンネル エンドポイントに適用される際にそのポリシーの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 **showpolicy-mapmgre** コマンドを使用します。

show policy-map mgre [*tunnel-interface-name*] [*tunnel-destination overlay-address*]

構文の説明

tunnel-interface-name	（任意）トンネル インターフェイスの名前。
tunnel-destination overlay-address	（任意）トンネル宛先オーバーレイ アドレス（トンネル エンドポイント アドレスなど）。

コマンド デフォルト

すべての既存のポリシー マップ コンフィギュレーションが表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(22)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

トンネル宛先オーバーレイ アドレスを指定すると、特定のセッションからの出力を表示できます。

例

次に、**showpolicy-mapmgre** コマンドの出力例を示します。

```
Router# show policy-map mgre tunnel 0 192.168.1.2
Tunnel0  <--> 192.168.1.2
  Service-policy output: set_out
    Class-map: test (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      QoS Set
        precedence 3
          Packets marked 0
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

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 *239 : show policy-map mgre* フィールドの説明

フィールド	説明
Tunnel0	トンネル エンドポイントの名前。
192.168.1.2	トンネル宛先オーバーレイ アドレス。
Service-policy output	指定されたインターフェイスまたはVCに適応されている出力サービス ポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-anyなど）もトラフィック クラスの横に表示されます。
packets and bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（単位：kbps）。 （注） 発信インターフェイス全体でパケットが圧縮されている場合、パケット圧縮によって達成された改善パケット レートは、offered rateには反映されません。また、パケットがトンネルの組み合わせ（例：Generic Routing Encapsulation（GRE）トンネルおよびIP Security（IPSec）トンネル）に入る前に圧縮されている場合、offered rate は、一般にトンネル カプセル化に関連付けられたすべての追加オーバーヘッドを含みません。offered rate は、設定に応じて、オーバーヘッドを含まない、*1* つのトンネル カプセル化だけのオーバーヘッドを含む、または、すべてのトンネル カプセル化のオーバーヘッドを含むのいずれかです。GRE および IPSec トンネル設定の多くで、offered rate は、GRE トンネル カプセル化のオーバーヘッドだけを含みます。
drop rate	クラスからパケットがドロップされるレート（単位：kbps）。ドロップ レートは、offered rateから正常に送信されたパケット数を引いて計算されます。
Match	トラフィックのクラスに指定された一致基準。選択要素には、IP precedence、IP Diffserv コード ポイント（DSCP）値、マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）値、アクセス グループ、および、QoSグループなどの基準があります。使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
QoS Set, qos-group, Packets marked	QoS グループに基づくクラスベース パケット マーキングが設定されていることを示します。qos-group 番号やマーク済みパケットの数などがあります。

関連コマンド

Command	Description
ipnhrpgroup	スポークで NHRP グループを設定します。
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。
ipnhrpmapgroup	ハブで QoS ポリシー マッピングに NHRP グループを追加します。
showdmvpn	DMVPN 固有のセッション情報を表示します。
showipnhrp	NHRP マッピング情報を表示します。
showipnhrpgroup-map	ハブの NHRP グループ マッピングの詳細、およびマッピングで定義されている各 NHRP グループを使用しているトンネルのリストを表示します。

show policy-map multipoint

マルチポイント トンネル インターフェイスの特定の Quality of Service（QoS）に関する統計情報を表示するには、特権 EXEC モードで **showpolicy-mapmultipoint** コマンドを使用します。

show policy-map multipoint [**tunnel** *interface-number* [*tunnel-destination-address*]] [**input** [**class** *class-name*]] [**output** [**class** *class-name*]]

構文の説明

tunnel	（任意）トンネル インターフェイスを表示します。
interface-number	（任意）モジュールおよびポート番号。
tunnel-destination-address	（任意）トンネル宛先オーバーレイ アドレス（トンネルエンドポイント アドレスなど）。
input	（任意）入力ポリシーに添付された統計情報が表示されることを示します。
output	（任意）出力ポリシーに添付された統計情報が表示されることを示します。
class *class-name*	（任意）指定したクラスの QoS ポリシー アクションを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(22)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

マルチポイント トンネル インターフェイスの Quality of Service（QoS）ポリシー マップを表示するには、**showpolicy-mapmultipoint** コマンドを使用します。

例

次に、**showpolicy-mapmultipoint** コマンドの出力例を示します。

```
Router# show
policy-map multipoint
Interface Tunnel1 <--> 10.1.1.1
  Service-policy output: parent-policy-out
    Class-map: class-default (match-any)
      9839 packets, 869608 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 5000/710000
```

```
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      Service-policy : child-policy-out
        queue stats for all priority classes:
          Queueing
          queue limit 300 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 5000/710000
Interface Tunnel1 <--> 10.1.2.1
  Service-policy output: parent-policy-out
    Class-map: class-default (match-any)
      4723 packets, 479736 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      Service-policy : child-policy-out
        queue stats for all priority classes:

          queue limit 300 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

関連コマンド

コマンド	説明
showplatformqospolicy-map	ルータに設定されているポリシーマップのタイプと数を表示します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービスポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

show policy-map session

Subscriber Service Switch（SSS）セッションに有効な Quality of Service（QoS）ポリシー マップを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showpolicy-mapsession** コマンドを使用します。

show policy-map session [**uid** *uid-number*] [{**input class** *class-name*|**output class** *class-name*}]

構文の説明

uid	（任意）固有のセッション ID を定義します。
uid-number	（任意）固有のセッション ID。範囲は 1 ～ 65535 です。
input	（任意）固有のセッションのアップストリーム トラフィックを表示します。
output	（任意）固有のセッションのダウンストリーム トラフィックを表示します。
class	（任意）QoS ポリシー マップ定義に含まれるクラスを識別します。
class-name	（任意）QoS ポリシー マップ定義に含まれるクラス名。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.3(8)T	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。このコマンドも、セッションあたりのトラフィック シェーピングおよびトラフィック キューイングの統計情報（該当する場合）を含むように変更されました。
12.2(33)SRC	このコマンドは Cisco IOS Release 12.2(33)SRC に統合され、Cisco 7600 シリーズ ルータのサポートが追加されました。
12.2(33)SB	Cisco 7300 シリーズ ルータのサポートが追加されました。このコマンドも、ATM のトラフィック シェーピング オーバーヘッド アカウンティング統計情報（該当する場合）を含むように変更されました。

使用上のガイドライン

SSS セッションの入力ストリームおよび出力ストリームで固有のセッション ID の QoS ポリシー マップを検証するには、**uid** キーワードを指定した **showpolicy-mapsession** コマンドを使用します。特定のクラスの統計情報を表示するには、オプションの **class***class-name* キーワード引数の組み合わせを指定した **showpolicy-mapsession** コマンドを使用します。**class***class-name* キーワード引数の組み合わせを指定しないで **showpolicy-mapsession** コマンドを使用した場合は、QoS ポリシー マップに定義されているすべてのクラスの統計情報が表示されます。

例

このセクションでは、**showpolicy-mapsession** コマンドの出力例を示します。

（注） **showpolicy-mapsession** コマンドの出力は、ポリシー マップに設定されている QoS 機能によって異なります。たとえば、ポリシーマップにトラフィック シェーピングまたはトラフィック キューイングが設定されている場合、そのような機能の統計情報が含まれるので、それに応じて出力はこのセクションに示すものとは異なります。追加で自明のフィールドが表示されることもありますが、出力は非常によく似たものになります。

showpolicy-mapsession コマンドの次の例では、設定済みの QoS ポリシー マップについて下流方向に向かうトラフィックの QoS ポリシー マップ統計情報を表示します。

```
Router# show policy-map session uid 401 output
 SSS session identifier 401 -
  Service-policy output: downstream-policy
    Class-map: customer1234 (match-any)
      4464 packets, 249984 bytes
      5 minute offered rate 17000 bps, drop rate 0 bps
      Match: ip dscp cs1  cs2  cs3  cs4
        4464 packets, 249984 bytes
        5 minute rate 17000 bps
      QoS Set
        dscp af11
          Packets marked 4464
    Class-map: customer56 (match-any)
      2232 packets, 124992 bytes
      5 minute offered rate 8000 bps, drop rate 0 bps
      Match: ip dscp cs5  cs6
        2232 packets, 124992 bytes
        5 minute rate 8000 bps
      police:
          cir 20000 bps, bc 10000 bytes
          pir 40000 bps, be 10000 bytes
        conformed 2232 packets, 124992 bytes; actions:
          set-dscp-transmit af21
        exceeded 0 packets, 0 bytes; actions:
          set-dscp-transmit af22
        violated 0 packets, 0 bytes; actions:
          set-dscp-transmit af23
        conformed 8000 bps, exceed 0 bps, violate 0 bps
    Class-map: customer7 (match-any)
      1116 packets, 62496 bytes
      5 minute offered rate 4000 bps, drop rate 4000 bps
      Match: ip dscp cs7
        1116 packets, 62496 bytes
        5 minute rate 4000 bps
      drop
    Class-map: class-default (match-any)
      1236 packets, 68272 bytes
      5 minute offered rate 4000 bps, drop rate 0 bps
      Match: any
```

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 *240 : show policy-map session* フィールドの説明：下流方向のトラフィック

フィールド	説明
SSS session identifier	固有のセッション ID。
Service-policy output	指定されたインターフェイスまたは仮想回線（VC）に適用されている出力サービス ポリシーの名前。
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
packets and bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（bps）。 （注） 発信インターフェイス全体でパケットが圧縮されている場合、パケット圧縮によって達成された改善パケット レートは、offered rate には反映されません。また、パケットがトンネルの組み合わせ（例：Generic Routing Encapsulation（GRE）トンネルおよび IP Security（IPsec）トンネル）に入る前に圧縮されている場合、offered rate は一般にトンネル カプセル化に関連付けられたすべての追加オーバーヘッドを含みません。offered rate は、設定に応じて、オーバーヘッドを含まない、*1* つのトンネル カプセル化だけのオーバーヘッドを含む、または、すべてのトンネル カプセル化のオーバーヘッドを含むのいずれかです。GRE および IPsec トンネル設定の多くで、offered rate は GRE トンネル カプセル化のオーバーヘッドだけを含みます。
drop rate	クラスからパケットがドロップされるレート（bps）。ドロップ レートは、offered rate から正常に送信されたパケット数を引いて計算されます。
Match	トラフィックのクラスに指定された一致基準。選択要素には、IP precedence、IP Diffserv コード ポイント（DSCP）値、マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）値、アクセス グループ、および、QoS グループなどの基準があります。使用可能なさまざまな一致基準オプションの詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Applying QoS Features Using the MQC」モジュールを参照してください。
QoS Set	パケット マーキングが導入されていることを示します。
dscp	パケット マーキングに使用する値。
Packets marked	マークされたパケットの数。

フィールド	説明
police	**police** コマンドがトラフィック ポリシングを有効にするように設定されていることを示します。また、パケットのマーキングに使用される、指定された設定情報レート（CIR）、適合バースト（bc）サイズ、最大情報レート（PIR）、およびピーク バースト（be）サイズも表示します。
conformed	指定したレートに適合するパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。
exceeded	指定したレートを超えるパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。
violated	指定したレートに違反するパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。

showpolicy-mapsession コマンドの次の例では、設定済みのすべてのQoSポリシーマップについて上流方向に向かうトラフィックのQoSポリシーマップ統計情報を表示します。

```
Router# show policy-map
 session
 uid
 401
 input
 SSS session identifier 401 -
  Service-policy input: upstream-policy
    Class-map: class-default (match-any)
      1920 packets, 111264 bytes
      5 minute offered rate 7000 bps, drop rate 5000 bps
      Match: any
      police:
          cir 8000 bps, bc 1500 bytes
        conformed 488 packets, 29452 bytes; actions:
          transmit
        exceeded 1432 packets, 81812 bytes; actions:
          drop
        conformed 7000 bps, exceed 5000 bps
```

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 *241 : show policy-map session* フィールドの説明：上流方向のトラフィック

フィールド	説明
SSS session identifier	固有のセッション ID。
Service-policy input	指定されたインターフェイスまたはVCに適用されている入力サービス ポリシーの名前。

フィールド	説明
Class-map	表示されるトラフィックのクラス。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all、match-anyなど）もトラフィック クラスの横に表示されます。
packets and bytes	表示されているトラフィックのクラスに属すると確認されたパケット数（バイト単位でも表示）。
offered rate	クラスに着信するパケットのレート（bps）。 （注） 発信インターフェイス全体でパケットが圧縮されている場合、パケット圧縮によって達成された改善パケット レートは、offered rate には反映されません。また、パケットがトンネルの組み合わせ（例：Generic Routing Encapsulation（GRE）トンネルおよび IP Security（IPsec）トンネル）に入る前に圧縮されている場合、offered rate は一般にトンネル カプセル化に関連付けられたすべての追加オーバーヘッドを含みません。offered rate は、設定に応じて、オーバーヘッドを含まない、*1* つのトンネル カプセル化だけのオーバーヘッドを含む、または、すべてのトンネル カプセル化のオーバーヘッドを含むのいずれかです。GRE および IPsec トンネル設定の多くで、offered rate は GRE トンネル カプセル化のオーバーヘッドだけを含みます。
drop rate	クラスからパケットがドロップされるレート（bps）。ドロップ レートは、offered rate から正常に送信されたパケット数を引いて計算されます。
Match	トラフィックのクラスに指定された一致基準。選択要素には、IP precedence、IP Diffserv コード ポイント（DSCP）値、マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）値、アクセス グループ、および、QoS グループなどの基準があります。使用可能なさまざまな一致基準オプションの詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Applying QoS Features Using the MQC」モジュールを参照してください。
police	**police** コマンドがトラフィック ポリシングを有効にするように設定されていることを示します。また、パケットのマーキングに使用される、指定された設定情報レート（CIR）、適合バースト（bc）サイズ、最大情報レート（PIR）、およびピーク バースト（be）サイズも表示します。
conformed	指定したレートに適合するパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。
exceeded	指定したレートを超えるパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。
violated	指定したレートに違反するパケットに実行されるアクションを表示します。アクションが実施されたパケット数とバイト数を表示します。

セッションあたりのシェーピングおよびキューイング出力：例

次に、セッションあたりのトラフィック シェーピングおよびトラフィック キューイングが有効になっている場合の **showpolicy-mapsession** コマンドの出力例を示します。セッションあたりのトラフィック シェーピングおよびトラフィック キューイングが設定されている場合、出力にトラフィック シェーピングおよびトラフィック キューイングの統計情報が含まれます。

（注） QoS：LNS のセッションあたりのシェーピングおよびキューイング機能は、パケット マーキングをサポートしていません。つまり、この機能では **set** コマンドを使用してパケットをマークできません。このため、パケット マーキングに関連する統計情報は出力に含まれません。

```
Router# show policy-map session
uid 1 output
 SSS session identifier 1 -
  Service-policy output: parent
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 128 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 512000, bc 12800, be 12800
      target shape rate 512000
      Service-policy : child
        Class-map: prec0 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 38 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 30% (153 kbps)
  Class-map: prec2 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
          queue limit 44 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 212000, bc 7632, be 7632
          target shape rate 212000
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: any
            0 packets, 0 bytes
            30 second rate 0 bps
```

```
          queue limit 44 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

次の表では、出力に表示されるセッションあたりのトラフィック シェーピングおよびトラフィック キューイングに関連する重要なフィールドについて説明します。

表 *242 : show policy-map session* フィールドの説明：設定されたセッションあたりのトラフィック シェーピングおよびトラフィック キューイング

フィールド	説明
Queueing	トラフィック キューイングが有効になっていることを示します。
queue limit	パケットでのキュー制限を表示します。
キュー項目数	トラフィック シェーパーの現在のキューの深さ。
shape (average) cir, bc, be	平均レート トラフィック シェーピングが有効になっていることを示します。設定情報レート（CIR）、認定バースト（bc）レート、および超過バースト（be）レートをバイト単位で表示します。
target shape rate	トラフィック シェーピング レートをバイト単位で表示します。

ATM のトラフィック シェーピング オーバーヘッド アカウンティング：例

次の show policy-map session コマンドの出力は、ATM オーバーヘッド アカウンティングがシェーピングに対してイネーブルになっていることを示しています。

```
Router# show policy-map session
uid 2
output

SSS session identifier 2 -
Service-policy output:  ATM_OH_POLICY
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 2500 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 10000000, bc 40000, be 40000
      target shape rate 10000000
       Overhead Accounting Enabled
```

次の表では、表示される重要なフィールドについて説明します。

表 *243 : show policy-map session* フィールドの説明：設定された *ATM* のトラフィック シェーピング オーバーヘッド アカウンティング

フィールド	説明
target shape rate	トラフィック シェーピング レートをバイト単位で表示します。

フィールド	説明
Overhead Accounting Enabled	オーバーヘッドアカウンティングが有効になっていることを示します。

関連コマンド

コマンド	説明
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定のPVCに対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。
showssssession	SSS セッション ステータスを表示します。

show policy-map target service-group

メイン インターフェイスまたはポート チャネルでイーサネット仮想回線（EVC）、サブ インターフェイスまたはセッションをメンバーとするサービス グループについてポリシー マップ情報を表示するには、特権 EXEC モードで **showpolicy-maptargetservice-group** コマンドを使用します。

showpolicy-maptargetservice-group [*service-group-identifier*]

構文の説明

service-group-identifier	サービス グループ識別番号。

コマンド デフォルト

すでにあるすべてのサービス グループのポリシー マップ情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.1(1)S	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、サービス グループおよびポリシー マップを作成する必要があります。

例

次に、**showpolicy-maptargetservice-group** コマンドの出力例を示します。

```
Router# show policy-map target service-group 1000
Port-channel1: Service Group 1000
Service-policy output: policy1
Counters last updated 02:04:11 ago
Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 768 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 20000000, bc 80000, be 80000
      target shape rate 20000000
```

次の表では、**showpolicy-maptargetservice-group** コマンドに表示されるフィールドについて説明します。

表 *244 :* フィールドの説明

フィールド	説明
Port-channel: Service Group	インターフェイス タイプおよびサービス グループ番号を指定します。
Service-policy output	出力サービス ポリシー名を指定します。
Class-map	トラフィック クラスを指定します。
Queuing	トラフィック キューイング メカニズムが有効になっていることを示します。トラフィック キューイングの統計情報も表示されます。

関連コマンド

コマンド	説明
showpolicy-mapinterface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。
showpolicy-mapinterfaceserviceinstance	インターフェイスまたはポート チャネルの下に特定のサービス インスタンスのポリシー マップ情報を表示します。

show policy-map type access-control

特定のポリシー マップのアクセス制御を表示するには、特権 EXEC モードで **showpolicy-maptypeaccess-control** コマンドを使用します。

show policy-map type access-control [{[{*policy-map-name* [**class** *class-map-name*]|**apn** *index-number*}] **control-plane** [{**all**|**subinterface**}] [{**input** [**class** *class-map-name*]|**output** [**class** *class-map-name*]}]|**interface** *type number* [{**vc** *vpivci*|**vp** *vpi* [*subinterface*]|**input** [**class** *class-map-name*]|**output** [**class** *class-map-name*]}] **session** [**uid** *id*] [{**input** [**class** *class-map-name*]|**output** [*class class-map-name*]}]}]

Cisco ASR 1000 シリーズ
show policy-map type access-control [**control-plane** [{**all** [{**brief** {**timestamp**|**vrfs timestamp**}|**class** *class-map-name*|**service-instance** [*target-identifier*]}]|**interface** [*type number* [**service-instance** [*target-identifier*]]]|**session** [**uid [id]**] [{**input** [**class** *class-map-name*]|**output class** [*class-map-name*]}]}]]

構文の説明

policy-map name	（任意）ポリシー マップ名。
class *class-map-name*	（任意）指定したクラスの Quality of Service（QoS）ポリシー アクションを表示します。
apn *index-number*	（任意）アクセス ポイント名（APN）関連のポリシーに関する情報を表示します。
control-plane	（任意）コントロール プレーン ポリシー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 プレーン ポリシーを表示します。
subinterface	（任意）**cef-exception**、**host**、**transit** のいずれかのサブインターフェイスに関して個別のクラスの統計情報およびポリシー詳細を表示します。
input	（任意）アタッチされた入力ポリシーの統計情報が表示されることを示します。
output	（任意）アタッチされた出力ポリシーの統計情報が表示されることを示します。
interface[*typenumber*]	（任意）Cisco IOS QoS ポリシー インターフェイスに関する情報を表示します。
vc	（任意）指定された仮想チャネル（VC）のサービス ポリシーを表示します。

vpi /	（任意）この相手先固定接続（PVC）の仮想パス識別子（VPI）。スラッシュ記号（「/」）と VPI 値がない場合、VPI 値はデフォルトで 0 になります。Cisco 7200 および 7500 シリーズ ルータで、この値範囲は 0 ～ 255 です。*vpi* および *vci* 引数は両方を 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。
vci	（任意）この PVC の仮想チャネル識別子（VCI）。この値は 0 ～ 1 の範囲で、**atmvc-per-vp** コマンドによってこのインターフェイスに対して設定された最大値未満です。一般的に、0 ～ 31 の低いほうの値は、特定のトラフィック（F4 運用管理および保守（OAM）、相手先選択接続（SVC）シグナリング、統合ローカル管理インターフェイス（ILMI）など）のために予約されており、使用できません。
session	（任意）指定されたセッション QoS ポリシーに関する情報を表示します。
uid[*id*]	（任意）Subscriber Service Switch（SSS）固有の識別子に基づいて、ポリシー マップのセッション ユーザ識別子（uid）を表示します。
brief	（任意）ポリシー マップの簡単な説明を表示します。
timestamp	ポリシー マップがインターフェイスにアタッチされた時間を表示します。
vrfs	バーチャル プライベート ネットワーク（VPN）に関連付けられたインターフェイスに関する情報を表示します。
serviceinstance	（任意）インターフェイスのサービス インスタンスに関する情報を表示します。
target-identifier	（任意）サービス インスタンスのターゲット識別子。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(22)T	このコマンドが導入されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR アグリゲーション サービス 1000 シリーズ ルータに実装されました。
15.0(1)M	コマンドが変更されました。出力が変更され、暗号化フィルタ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

特定のポリシー マップのアクセス制御を表示するには、このコマンドを使用します。

例

次に、**showpolicy-maptypeaccess-control** コマンドの出力例を示します。フィールドの説明は自明です。

```
Router# show policy-map type access-control
Policy Map type access-control tcp_policy
    Class psirt1 (encrypted FPM filter)
      drop
    Class psirt2 (encrypted FPM filter)
      drop
    Class psirt11 (encrypted FPM filter)
      drop
  Policy Map type access-control udp_policy
    Class slammer
      drop
  Policy Map type access-control fpm-policy
    Class ip_tcp_stack
      service-policy tcp_policy
    Class ip_udp_stack
      service-policy udp_policy
```

関連コマンド

コマンド	説明
showplatformqospolicy-map	ルータに設定されているポリシーマップのタイプと数を表示します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

show policy-map type nat

ネットワーク アドレス変換（NAT）のポリシー マップを表示するには、特権 EXEC モードで **showpolicy-maptypeNAT** コマンドを使用します。

```
show policy-map nat policymap-name
[class classmap-name]
|apn index-number | interface type-number
[input class classmap-name]
|outputclass classmap-name
[session uid id]
input [class classmap-name] | output class classmap-name
```

構文の説明

policymap-name	（任意）ポリシー マップ名。
class *classmap-name*	（任意）指定したクラスの QoS ポリシー アクションを表示します。
apn *index-number*	（任意）アクセス ポイント名（APN）関連のポリシー情報を表示します。
interface[*typenumber*]	（任意）Cisco IOS Quality of Service（QoS）ポリシー インターフェイス情報を表示します。
session	（任意）セッション QoS ポリシー情報を表示します。
uid[*id*]	Subscriber Service Switch（SSS）固有の識別子に基づいて、ポリシー マップのセッション ユーザ識別子（uid）を表示します。
input	（任意）アタッチされた入力ポリシーの統計情報が表示されることを示します。
output	（任意）アタッチされた出力ポリシーの統計情報が表示されることを示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(11)T	このコマンドが導入されました。

例

次は、**showpolicy-maptypeNAT** コマンドの出力例です。

```
Router# show policy-map type NAT
Policy Map ipnat-policyxx-in2out
Class ipnat-default
```

```
Class ipnat-class-acl-1
Class ipnat-class-acl-2
Class ipnat-class-acl-3
Policy Map ipnat-policyxx-out2in
Class ipnat-default
```

関連コマンド

コマンド	説明
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービスポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。
showplatformqospolicy-map	ルータに設定されているポリシーマップのタイプと数を表示します。

show policy-map type port-filter

閉じているかリッスンされていない TCP/UDP ポートに移動するパケットのポリシングに関する情報を表示するには、特権 EXEC モードで **showpolicy-maptypeport-filter** コマンドを使用します。

show queue *interface-name interface-number queue-number* **vc** *vc vpi/vci*

構文の説明

policy-map-name	（任意）ポリシー マップ名。
class *class-map-name*	（任意）指定したクラスの QoS ポリシー アクションを表示します。
apn *index-number*	（任意）アクセス ポイント名（APN）関連のポリシー情報を表示します。
control-plane	（任意）コントロール プレーン ポリシー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 プレーン ポリシーを表示します。
subinterface	（任意）**cef-exception**、**host**、**transit** のいずれかのサブインターフェイスに関して個別のクラスの統計情報およびポリシー詳細を表示します。
interface[*typenumber*]	（任意）Cisco IOS QoS ポリシー インターフェイス情報を表示します。
	（任意）指定された仮想チャネル（VC）のサービス ポリシーを表示します。
vpi / **vc**	（任意）この PVC の仮想パス識別子（VPI）。「/」と vpi 値がない場合、vpi 値はデフォルトで 0 になります。Cisco 7200 および 7500 シリーズ ルータで、この値範囲は 0 ～ 255 です。vpi および vci 引数は両方を 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。
vci	（任意）この PVC の仮想チャネル識別子（VCI）。この値は 0 ～ 1 の範囲で、atm vc-per-vp コマンドによってこのインターフェイスに対して設定された最大値未満です。一般的に、0 ～ 31 の低いほうの値は、特定のトラフィック（F4 運用管理および保守（OAM）、相手先選択接続（SVC）シグナリング、統合ローカル管理インターフェイス（ILMI）など）のために予約されており、使用できません。
vp	（任意）指定された仮想パス（VP）のサービスポリシーを表示します。
session	（任意）セッション QoS ポリシー情報を表示します。
uid[*id*]	Subscriber Service Switch（SSS）固有の識別子に基づいて、ポリシー マップのセッション ユーザ識別子（uid）を表示します。
input	（任意）アタッチされた入力ポリシーの統計情報が表示されることを示します。

output	（任意）アタッチされた出力ポリシーの統計情報が表示されることを示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(22)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

ポート フィルタリング機能を使用すると、コントロールプレーン IP インプット キューで許可された指定済みプロトコルのパケットの数をキューしきい値によって制限した状態で、閉鎖状態または非待ち受け状態の TCP/UDP ポートに送信されたパケットをポリシングできます。

例

次の例は、**showpolicy-maptypeport-filter** コマンドの出力を示しています。

```
Router# show policy-map type port-filter
Policy Map type port-filter p1
Policy Map type port-filter p4
```

関連コマンド

コマンド	説明
showplatformqospolicy-map	ルータに設定されているポリシーマップのタイプと数を表示します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。

show protocol phdf

特定のプロトコル ヘッダー説明ファイル（PHDF）からプロトコル情報を表示するには、特権 EXEC モードで **showprotocolphdf** コマンドを使用します。

show protocol phdf *protocol-name*

構文の説明

protocol-name	ロードされた PHDF。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。
12.2(18)ZY	このコマンドは、Catalyst 6500 シリーズの Programmable Intelligent Services Accelerator（PISA）が搭載されているスイッチの Cisco IOS リリース 12.2(18)ZY に統合されました。

例

次の例は、スラマー パケット（UDP ポート 1434）の FPM トラフィック クラスを定義する方法を示しています。クラス マップ内に定義された一致基準は、IP 長が 404 バイト未満、UDP ポートが 1434 で、パターン 0x4011010 が IP ヘッダーの先頭から 224 バイトにあるスラマー パケットを対象としています。この例では、サービス ポリシー「fpm-policy」を定義して GigabitEthernet インターフェイスに適用する方法も示しています。show コマンドは、FPM 設定を検証するために発行されています。（PHDF は、XML 形式であるため、show コマンドの出力に表示されないことに注意してください。）

```
Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:udp.phdf
Router(config)# class-map type stack match-all ip-udp
Router(config-cmap)# description "match UDP over IP packets"
Router(config-cmap)# match field ip protocol eq 0x11 next udp
Router(config)# class-map type access-control match-all slammer
Router(config-cmap)# description "match on slammer packets"
Router(config-cmap)# match field udp dest-port eq 0x59A
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start 13-start offset 224 size 4 eq 0x4011010
Router(config)# policy-map type access-control fpm-udp-policy
Router(config-pmap)# description "policy for UDP based attacks"
Router(config-pmap)# class slammer
Router(config-pmap-c)# drop
Router(config)# policy-map type access-control fpm-policy
Router(config-pmap)# description "drop worms and malicious attacks"
Router(config-pmap)# class ip-udp
Router(config-pmap-c)# service-policy fpm-udp-policy
```

```
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input fpm-policy
Router# show protocols phdf ip
Protocol ID: 1
Protocol name: IP
Description: Definition-for-the-IP-protocol
Original file name: disk2:ip.phdf
Header length: 20
Constraint(s):
Total number of fields: 12
Field id: 0, version, IP-version
Fixed offset. offset 0
Constant length. Length: 4
Field id: 1, ihl, IP-Header-Length
Fixed offset. offset 4
Constant length. Length: 4
Field id: 2, tos, IP-Type-of-Service
Fixed offset. offset 8
Constant length. Length: 8
Field id: 3, length, IP-Total-Length
Fixed offset. offset 16
Constant length. Length: 16
Field id: 4, identification, IP-Identification
Fixed offset. offset 32
Constant length. Length: 16
Field id: 5, flags, IP-Fragmentation-Flags
Fixed offset. offset 48
Constant length. Length: 3
Field id: 6, fragment-offset, IP-Fragmentation-Offset
Fixed offset. offset 51
Constant length. Length: 13
Field id: 7, ttl, Definition-for-the-IP-TTL
Fixed offset. offset 64
Constant length. Length: 8
Field id: 8, protocol, IP-Protocol
Fixed offset. offset 72
Constant length. Length: 8
Field id: 9, checksum, IP-Header-Checksum
Fixed offset. offset 80
Constant length. Length: 16
Field id: 10, source-addr, IP-Source-Address
Fixed offset. offset 96
Constant length. Length: 32
Field id: 11, dest-addr, IP-Destination-Address
Fixed offset. offset 128
Constant length. Length: 32
Router# show protocols phdf udp
Protocol ID: 3
Protocol name: UDP
Description: UDP-Protocol
Original file name: disk2:udp.phdf
Header length: 8
Constraint(s):
Total number of fields: 4
Field id: 0, source-port, UDP-Source-Port
Fixed offset. offset 0
Constant length. Length: 16
Field id: 1, dest-port, UDP-Destination-Port
Fixed offset. offset 16
Constant length. Length: 16
Field id: 2, length, UDP-Length
Fixed offset. offset 32
Constant length. Length: 16
Field id: 3, checksum, UDP-Checksum
```

```
Fixed offset. offset 48
Constant length. Length: 16
```

関連コマンド

コマンド	説明
loadprotocol	PHDF をルータにロードします。

show qbm client

Quality of Service（QoS）帯域幅マネージャ（QBM）クライアント（アプリケーション）とその ID を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showqbmclient** コマンドを使用します。

show qbm client

構文の説明

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	変更箇所
12.2(33)SRC	このコマンドが導入されました。
Cisco IOS XE リリース 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

Cisco IOS ソフトウェアのサブセットが QBM に登録されていることを確認するには、**showqbmclient** コマンドを使用します。

Cisco IOS ソフトウェアのサブセットは、QBM 登録アプリケーションプログラミングインターフェイス（API）をコールし、ID を受信すると、QBM のクライアントになります。サブセットは、まだ登録されていない場合にはクライアントではありません。

例

次に、RSVP 集約が有効になっている場合の **showqbmclient** コマンドの出力例を示します。

```
Router# show qbm client
Client Name                              Client ID
RSVP BW Admit                            1
RSVP rfc3175 AggResv                     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 *245 : show qbm client* コマンドのフィールドの説明

フィールド	説明
Client Name	アプリケーションの名前。 • RSVP BW Admit：帯域幅が QBM 帯域幅プールに入ることを許可する場合に使用される RSVP QBM クライアント。 • RSVP rfc3175 AggResv：RFC 3175、*AggregationofRSVPforIPv4andIPv6Reservations* に定義されている RSVP 集約。 • このクライアントは、RSVP 集約予約用の QBM 帯域幅プールを作成および維持するために使用します。
Client ID	アプリケーションの識別子。クライアントごとに 1 つのクライアント ID が存在します。

関連コマンド

コマンド	説明
debugqbm	QBM オプションのデバッグ出力を有効にします。
showqbmpool	割り当てられた QBM プールおよび関連するオブジェクトを表示します。

show qbm pool

割り当てられた Quality of Service（QoS）帯域幅マネージャ（QBM）プールを表示し、それらが関連付けられているオブジェクトを識別するには、ユーザ EXEC モードまたは特権 EXEC モードで **showqbmpool** コマンドを使用します。

show qbm pool [**id** *pool-id*]

構文の説明

id *pool-id*	（任意）アドミッション コントロールを実行している指定された帯域幅プールの識別子を表示します。値は、0x0 から 0xffffffff の範囲内である必要があります。デフォルトはありません。

コマンド デフォルト

オプションのキーワード/引数の組み合わせを指定しないで **showqbmpool** コマンドを入力した場合は、設定されたすべての QBM プールの情報が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRC	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

設定されたすべての QBM プールまたは指定したプールの情報を表示するには、**showqbmpool** コマンドを使用します。存在しないプール ID を入力すると、エラー メッセージが表示されます。

このコマンドは、QBM 操作をトラブルシューティングする場合に便利です。

例

次に、RSVP 集約が有効になっている場合の **showqbmpool** コマンドの出力例を示します。

```
Router# show qbm pool
Total number of pools allocated:  1
Pool ID 0x00000009
Associated object:  'RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46)'
  Minimum:          300Kbps
  Oper Status:      OPERATIONAL
  Oper Minimum:     300Kbps
Used Bandwidth:  80Kbps
```

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 *246 : show qbm pool* コマンドのフィールドの説明

フィールド	説明
Total number of pools allocated	設定済みの QBM プールの数。
Pool ID	QBM プールの識別子。
Associated object	QBM プールに関連付けられたアプリケーション（またはクライアント）。この文字列はクライアントによって提供され、その結果、クライアントは QBM ではなくその文字列を選択します。たとえば、RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46) は、送信元エンドポイント（アグリゲータ）の IP アドレスが 192.168.40.1 で、宛先エンドポイント（デアグリゲータ）の IP アドレスが 192.168.50.1 で、DiffServ コードポイント（DSCP）が完全優先転送（EF）である RSVP 集約予約に QBM プールが関連付けられることを意味します。
Minimum	プールの最低帯域保証。（単位は異なる場合があります。）
Oper Status	アプリケーションのステータス。値は次のとおりです。 • [OPERATIONAL]：アプリケーションは有効になっています。 • [NON-OPERATIONAL]：アプリケーションは無効になっています。
Oper Minimum	プールが実現できる最低帯域保証を定義します。この値は、動作条件のため、プールの最低帯域保証とは異なることがあります。たとえば、プールがインターフェイスに関連付けられ、そのインターフェイスがダウンして、その [Oper ステータス（Oper Status）] が [NON-OPERATIONAL] である場合、[最小動作（Oper Minimum）] は N/A になります。
使用済み帯域幅（Used Bandwidth）	このプールを使用するアプリケーション/クライアントによって予約された帯域幅。N/A は、プールの [Oper ステータス（Oper Status）] が [NON-OPERATIONAL] である場合に、0 の代わりに表示されます。

次に、プール ID を指定した **showqbmpool** コマンドの出力例を示します。

```
Router# show qbm pool id 0x000000006
Pool ID 0x00000009
Associated object:  'RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46)'
  Minimum:         300Kbps
  Oper Status:     OPERATIONAL
  Oper Minimum:    300Kbps
Used Bandwidth:  80Kbps
```

フィールドの説明については、上記の表を参照してください。

関連コマンド

コマンド	説明
debugqbm	QBMオプションのデバッグ出力を有効にします。
showqbmclient	登録された QBM クライアントを表示します。

show qdm status

ルータに接続されているアクティブな QoS デバイス マネージャ（QDM）クライアントのステータスを表示するには、EXEC モードで **showqdmstatus** コマンドを使用します。

show qdm 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 モード

EXEC

コマンド履歴

リリース	変更箇所
12.1(1)E	このコマンドが導入されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。

使用上のガイドライン

showqdmstatus コマンドは、Cisco 7600 シリーズ ルータで使用できます。

showqdmstatus コマンドの出力には、次の情報が含まれています。

- 接続されている クライアントの数
- クライアント ID
- クライアント ソフトウェアのバージョン
- 接続されているクライアントの IP アドレス
- 接続の継続時間

（注） QDM は、Optical Service Module（OSM）インターフェイスではサポートされていません。

例

次の例は、2 つの QDM クライアントがルータに接続されている場合の **showqdmstatus** の出力を示しています。

```
Router# show qdm status
Number of QDM Clients :2
```

```
QDM Client v1.0(0.13)-System_1 @ 172.16.0.0 (id:30)
     connected since 09:22:36 UTC Wed Mar 15 2000
QDM Client v1.0(0.12)-System_2 @ 172.31.255.255 (id:29)
     connected since 17:10:23 UTC Tue Mar 14 2000
```

関連コマンド

コマンド	説明
disconnectqdm	QDMクライアントを切断します。

show queue

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**showqueue** コマンドは非表示です。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンドシーケンス）を使用する必要があります。詳細（代替コマンドのリストを含む）については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**showqueue** コマンドは、モジュラ QoS CLI（MQC）コマンド（または MQC コマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

特定のインターフェイスまたは仮想回線（VC）のキュー内にあるパケットの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showqueue** コマンドを使用します。

show queue *interface-name interface-number* [**queue-number**][**vc vpi/ vci**]

構文の説明

interface-name	インターフェイスの名前。
interface-number	インターフェイスの番号。
queue-number	（任意）キューの番号。キュー番号は、1 ～ 16 です。
vc	（任意）ATM インターフェイスの場合にのみ、指定された相手先固定接続（PVC）の均等化キューイング設定を表示します。名前には、16 文字まで使用できます。
vpi /	（任意）この PVC の ATM ネットワーク仮想パス識別子（VPI）。「/」と *vpi* 値がない場合、*vpi* 値はデフォルトで 0 になります。 Cisco 7200 および Cisco 7500 シリーズ ルータで、この値範囲は 0 ～ 255 です。 *vpi* および *vci* 引数は両方を 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。 この値を省略すると、指定した ATM インターフェイスまたはサブインターフェイス上にあるすべての VC の情報が表示されます。

vci	（任意）この PVC の ATM ネットワーク仮想チャネル識別子（VCI）。この値は 0 ～ 1 の範囲で、**atmvc-per-vp** コマンドによってこのインターフェイスに対して設定された最大値未満です。一般的に、0 ～ 31 の低いほうの値は、特定のトラフィック（F4 運用管理および保守（OAM）、相手先選択接続（SVC）シグナリング、統合ローカル管理インターフェイス（ILMI）など）のために予約されており、使用できません。 VCI は、ATM セルのヘッダーの 16 ビット フィールドです。VCI 値はローカルにだけ意味があるため、単一リンク上でだけ一意であり、ATM ネットワーク全体では一意ではありません。 *vpi* および *vci* 引数は両方を 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
10.2	このコマンドが導入されました。
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。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されましたが、階層型キューイング フレームワーク（HQF）はサポートされていません。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。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

使用上のガイドライン

このコマンドは、特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。

このコマンドは、VIP 分散重み付きランダム早期検出 WRED（DWRED）をサポートしていません。**vc** キーワードおよび **showqueue** コマンド引数を使用すると、VC 単位キューイングをサポートする拡張 ATM ポート アダプタ（PA-A3）でのみ PVC の出力を表示できます。

このコマンドは HQF をサポートしません。HQF 情報および統計情報を収集するには、**showpolicy-map** および **showpolicy-mapinterface** コマンドを使用します。

例

次の例は、**showqueue** コマンドを入力し、重み付け均等化キューイング（WFQ）、WRED、またはフローベース WRED を設定している場合の出力例を示しています。

WFQ の例

次に、atm2/0.33 ATM サブインターフェイス上の PVC 33 に対する **showqueue** コマンドの出力例を示します。このインターフェイスでは、2 つのメッセージ交換がアクティブです。WFQ により、両方のデータ ストリームがインターフェイス上で等しい帯域幅を受け取り、メッセージをパイプラインに保持するようになります。

```
Router# show queue
 atm2/0.33 vc 33
Interface ATM2/0.33 VC 0/33
  Queueing strategy: weighted fair
  Total output drops per VC: 18149
  Output queue: 57/512/64/18149 (size/max total/threshold/drops)
     Conversations  2/2/256 (active/max active/max total)
     Reserved Conversations 3/3 (allocated/max allocated)
  (depth/weight/discards/tail drops/interleaves) 29/4096/7908/0/0
  Conversation 264, linktype: ip, length: 254
  source: 10.1.1.1, destination: 10.0.2.20, id: 0x0000, ttl: 59,
  TOS: 0 prot: 17, source port 1, destination port 1
  (depth/weight/discards/tail drops/interleaves) 28/4096/10369/0/0
  Conversation 265, linktype: ip, length: 254
  source: 10.1.1.1, destination: 10.0.2.20, id: 0x0000, ttl: 59,
  TOS: 32 prot: 17, source port 1, destination port 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 *247 : WFQ* 用の *show queue* フィールドの説明

フィールド	説明
Queueing strategy	このインターフェイスでアクティブなキューイングの種類。
Total output drops per VC	合計出力パケット ドロップ数。
Output queue	出力キューサイズ（パケット単位）。[最大合計値（max total）] とは、すべての WFQ フローの集約キュー サイズのことです。[しきい値（threshold）] は、各メッセージ交換の個別のキュー サイズです。[ドロップ（drops）] は、WFQ におけるすべてのメッセージ交換からドロップされたパケットです。

フィールド	説明
Conversations	WFQカンバセーションの番号。メッセージ交換は、キューが空になると、非アクティブになるかまたはタイムアウトします。WFQの各トラフィック フローは、キューに基づき、メッセージ交換で表されます。[最大アクティブ（max active）]は、キューイング機能の設定以降に発生したアクティブなメッセージ交換の数です。[最大合計値（max total）]は、同時に許可されたメッセージ交換の数です。
Reserved Conversations	bandwidth コマンドやリソース予約プロトコル（RSVP）フローによって設定されたクラスベース重み付け均等化キューイング（CBWFQ）など、WFQ によってキャプチャされないトラフィック フローには、予約済みのメッセージ交換で表される独立したキューがあります。[割り当て済み（allocated）] は、予約済みメッセージ交換の現在の番号です。[割り当て済み最大数（max allocated）]は、割り当てられた予約済みメッセージ交換のうち、実際に行われたメッセージ交換の最大数です。
depth	メッセージ交換のキューの深さ（パケット単位）。
weight	WFQ に使用されている重み付け値。
discards	メッセージ交換のキューからドロップされたパケットの数。
tail drops	キューがいっぱいになったときに、メッセージ交換からドロップされたパケットの数。
interleaves	インターリーブされたパケットの数。
linktype	プロトコル名です。
length	パケット長。
source	発信元の IP アドレス。
destination	宛先の IP アドレス。
id	パケット ID。
ttl	パケット存続時間（TTL）カウント。
TOS	IP タイプ オブ サービス。
prot	レイヤ 4 プロトコル番号.

フローベース WRED の例

次に、フローベース WRED が設定されているシリアル インターフェイス 1 に対して発行された **showqueue** コマンドの出力例を示します。出力には、キュー内の各パケットの情報が表示されます。このデータにより、番号別パケット、パケットが属するフローベース キュー、使用されたプロトコルなどが明らかになります。

```
Router# show queue Serial1
   Output queue for Serial1 is 2/0

   Packet 1, flow id:160, linktype:ip, length:118, flags:0x88
     source:10.1.3.4, destination:10.1.2.2, id:0x0000, ttl:59,
     TOS:32 prot:17, source port 1, destination port 515
       data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
            0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B

   Packet 2, flow id:161, linktype:ip, length:118, flags:0x88
     source:10.1.3.5, destination:10.1.2.2, id:0x0000, ttl:59,
     TOS:64 prot:17, source port 1, destination port 515
       data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
            0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B
```

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 *248 :* フローベース *WRED* 用の *show queue* フィールドの説明

フィールド	説明
Packet	パケット番号。
flow id	フローベース WRED の番号。
linktype	プロトコル名です。
length	パケット長。
Flags	内部バージョン固有のフラグ。
source	発信元の IP アドレス。
destination	宛先の IP アドレス。
id	パケット ID。
ttl	パケット存続時間（TTL）カウント。
prot	レイヤ 4 プロトコル番号.
data	パケット データ。

WRED の例

次に、WRED が設定されているシリアル インターフェイス 3 に対して発行された **showqueue** コマンドの出力例を示します。24 パケットのうち 2 パケットのみを示すために、出力を省略しました。

```
Router# show queue Serial3
   Output queue for Serial3 is 24/0

   Packet 1, linktype:ip, length:118, flags:0x88
     source:10.1.3.25, destination:10.1.2.2, id:0x0000, ttl:59,
     TOS:192 prot:17, source port 1, destination port 515
       data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
            0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B

   Packet 2, linktype:ip, length:118, flags:0x88
     source:10.1.3.26, destination:10.1.2.2, id:0x0000, ttl:59,
     TOS:224 prot:17, source port 1, destination port 515
       data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
            0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B
```

関連コマンド

Command	Description
atmvc-per-vp	VPI ごとにサポートする VCI の最大数を設定します。
custom-queue-list	カスタム キュー リストをインターフェイスに割り当てます。
fair-queue(class-default)	デフォルト クラス ポリシーの一部として class-default クラスで使用するために予約するダイナミック キューの数を指定します。
fair-queue(WFQ)	インターフェイスに対する WFQ を有効にします。
priority-group	指定した優先リストをインターフェイスに割り当てます。
random-detect(interface)	WRED または DWRED をイネーブルにします。
random-detectflow	フローベース WRED をイネーブルにします。
showframe-relaypvc	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

show queueing

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**showqueueing** コマンドは非表示です。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンドシーケンス）を使用する必要があります。代替コマンドのリストなど詳細については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**showqueueing** コマンドは、モジュラ QoS CLI（MQC）コマンド（または MQC コマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

設定されたキューイング戦略の全部または選択したものだけを一覧表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showqueueing** コマンドを使用します。

show queueing [{**custom**|**fair**|**priority**|**random-detect** [**interface** *atm-subinterface* [**vc** [[*vpi*] *vci*]]]}]

構文の説明

custom	（任意）カスタムのキューイング リスト設定のステータス。
fair	（任意）均等化キューイング設定のステータス。
priority	（任意）プライオリティ キューイング リスト設定のステータス。
random-detect	（任意）フローベース WRED の設定など、重み付けランダム早期検出（WRED）および分散 WRED（DWRED）設定のステータス。
interface *atm-subinterface*	（任意）指定した ATM サブインターフェイスで WRED が有効になっているすべての仮想回線（VC）の WRED パラメータを表示します。
vc	（任意）特定の VC に関連付けられた WRED パラメータを表示します。必要に応じて、仮想パス識別子（VPI）と仮想回線識別子（VCI）の両方の値か、または VCI 値だけを指定できます。

vpi /	（任意）VPI を指定します。*vpi* 引数を省略すると、相手先固定接続（PVC）の位置を特定するための VPI の値として 0 が使用されます。*vpi* 引数を指定する場合は、/ 区切り記号が必要です。
vci	（任意）VCI を指定します。

コマンド デフォルト

オプションのキーワードを入力しない場合には、すべてのインターフェイスの設定が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
10.3	このコマンドが導入されました。
12.0(4)T	このコマンドは、Cisco IOS Release 12.0(4)T に統合されました。**red** キーワードは、**random-detect** に変更されました。
12.1(2)T	このコマンドが変更されました。このコマンドは、フレーム リレー PVC インターフェイス プライオリティ キューイング（FR PIPQ）機能に関する情報が含まれるように変更されました。
12.2(2)T	このコマンドが Cisco IOS Release 12.2(2)T に統合されました。
12.0(24)S	このコマンドが、Cisco IOS Release 12.0(24)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(18)SXF2	このコマンドが、Cisco IOS Release 12.2(18)SXF2 に統合されました。
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。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

使用上のガイドライン

このコマンドは HQF をサポートしません。HQF 情報および統計情報を収集するには、**showpolicy-map** および **showpolicy-mapinterface** コマンドを使用します。

例

このセクションでは、**showqueueing** コマンドの出力例を示します。使用されているインターフェイスまたはプラットフォーム、および、イネーブルにされているオプションによって、表示される出力は次に示すものと若干異なります。

FR PIPQ：例

次の出力例は、FR PIPQ（「DLCI プライオリティ キュー」と呼ばれます）がシリアル インターフェイス 0 に設定されていることを示しています。出力には、4 つのデータ リンク接続識別子（DLCI）プライオリティ キューのサイズも表示されます。

```
Router# show queueing
Current fair queue configuration:
  Interface           Discard     Dynamic      Reserved
                      threshold   queue count  queue count
  Serial3/1           64          256          0
  Serial3/3           64          256          0
Current DLCI priority queue configuration:
  Interface           High    Medium  Normal  Low
                      limit   limit   limit   limit
  Serial0             20      40      60      80
Current priority queue configuration:
List   Queue  Args
1      low    protocol ipx
1      normal protocol vines
1      normal protocol appletalk
1      normal protocol ip
1      normal protocol decnet
1      normal protocol decnet_node
1      normal protocol decnet_rout
1      normal protocol decnet_rout
1      medium protocol xns
1      high   protocol clns
1      normal protocol bridge
1      normal protocol arp
Current custom queue configuration:
Current random-detect configuration:
```

重み付け均等化キューイング：例

次は、**showqueueing** コマンドの出力例です。シリアル インターフェイス 0 には、アクティブなメッセージ交換が 2 つあります。重み付け均等化キューイング（WFQ）により、これらの IP データ ストリームの両方（どちらも TCP を使用）がインターフェイスで等しい帯域幅を受け取り、メッセージをパイプラインに保持するようになります。これは、キュー内にリモート プロシージャ コール（RCP）データよりも多くの FTP データがある場合でも同じです。

```
Router# show queueing
Current fair queue configuration:
Interface           Discard     Dynamic      Reserved
                    threshold   queue count  queue count
  Serial0             64          256          0
  Serial1             64          256          0
  Serial2             64          256          0
```

```
  Serial3             64          256          0
Current priority queue configuration:
List   Queue  Args
1      high   protocol cdp
2      medium interface Ethernet1
Current custom queue configuration:
Current random-detect configuration:
  Serial5
    Queueing strategy:random early detection (WRED)
    Exp-weight-constant:9 (1/512)
    Mean queue depth:40
    Class   Random       Tail    Minimum    Maximum     Mark
              drop       drop  threshold  threshold  probability
      0       1401       9066         20         40      1/10
      1          0          0         22         40      1/10
      2          0          0         24         40      1/10
      3          0          0         26         40      1/10
      4          0          0         28         40      1/10
      5          0          0         31         40      1/10
      6          0          0         33         40      1/10
      7          0          0         35         40      1/10
      rsvp       0          0         37         40      1/10
```

カスタムのキューイング：例

次に、**showqueueingcustom** コマンドの出力例を示します。

```
Router# show queueing custom
Current custom queue configuration:
List   Queue  Args
3      10     default
3      3      interface Tunnel3
3      3      protocol ip
3      3      byte-count 444 limit 3
```

フローベース WRED：例

次に、**showqueueingrandom-detect** コマンドの出力例を示します。出力は、フローベース WRED によりフロー間でパケット ドロップが均等化されるようにインターフェイスが設定されていることを示しています。**random-detectflowaverage-depth-factor** コマンドは、このインターフェイスにスケール係数として 8 を設定するために使用していました。スケール係数は、キューでパケットドロップが起きやすくなる前に、フローごとに使用可能なバッファ数を調整し、アクティブな各フローの出力キューで許可するパケット数を決定するために使用します。このインターフェイスの最大フロー カウントは、**random-detectflowcount** コマンドによって 16 に設定されました。

```
Router# show queueing random-detect
    Current random-detect configuration:
      Serial1
        Queueing strategy:random early detection (WRED)
        Exp-weight-constant:9 (1/512)
        Mean queue depth:29
        Max flow count:16       Average depth factor:8
        Flows (active/max active/max):39/40/16
```

```
        Class   Random       Tail    Minimum    Maximum     Mark
                  drop       drop  threshold  threshold  probability
          0         31          0         20         40     1/10
          1         33          0         22         40     1/10
          2         18          0         24         40     1/10
          3         14          0         26         40     1/10
          4         10          0         28         40     1/10
          5          0          0         31         40     1/10
          6          0          0         33         40     1/10
          7          0          0         35         40     1/10
       rsvp          0          0         37         40     1/10
```

DWRED：例

次に、DWRED に対する **showqueueingrandom-detect** コマンドの出力例を示します。

```
    Current random-detect configuration:
      Serial1
        Queueing strategy:random early detection (WRED)
        Exp-weight-constant:9 (1/512)
        Mean queue depth:29
        Max flow count:16       Average depth factor:8
        Flows (active/max active/max):39/40/16

        Class   Random       Tail    Minimum    Maximum     Mark
                  drop       drop  threshold  threshold  probability
          0         31          0         20         40     1/10
          1         33          0         22         40     1/10
          2         18          0         24         40     1/10
          3         14          0         26         40     1/10
          4         10          0         28         40     1/10
          5          0          0         31         40     1/10
          6          0          0         33         40     1/10
          7          0          0         35         40     1/10
       rsvp          0          0         37         40     1/10
Current random-detect configuration:
  FastEthernet2/0/0
    Queueing strategy:fifo
    Packet drop strategy:VIP-based random early detection (DWRED)
    Exp-weight-constant:9 (1/512)
    Mean queue depth:0
    Queue size:0       Maximum available buffers:6308
    Output packets:5  WRED drops:0  No buffer:0
    Class   Random       Tail    Minimum    Maximum     Mark       Output
              drop       drop  threshold  threshold  probability  Packets
      0          0          0       109        218      1/10            5
      1          0          0       122        218      1/10            0
      2          0          0       135        218      1/10            0
      3          0          0       148        218      1/10            0
      4          0          0       161        218      1/10            0
      5          0          0       174        218      1/10            0
      6          0          0       187        218      1/10            0
      7          0          0       200        218      1/10            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 *249 : show queueing* フィールドの説明

フィールド	説明
Discard threshold	各キューで許可されるメッセージ数。
Dynamic queue count	ベストエフォート型のメッセージ交換に使用されるダイナミック キューの数。
Reserved queue count	予約されたメッセージ交換に使用される予約可能なキューの数。
High limit	上限の DLCI プライオリティ キュー サイズ（パケット最大数）。
Medium limit	中程度の DLCI プライオリティ キュー サイズ（パケット最大数）。
Normal limit	通常の DLCI プライオリティ キュー サイズ（パケット最大数）。
Low limit	下限の DLCI プライオリティ キュー サイズ（パケット最大数）。
List	カスタム キューイング：キュー リストの数。 プライオリティ キューイング：プライオリティ リストの数。
Queue	カスタム キューイング：キューの数。 プライオリティ キューイング：プライオリティ キューのレベル（**high**、**medium**、**normal**、または **low** キーワード）。
Args	そのキューのパケット一致基準。
Exp-weight-constant	指数加重係数。
Mean queue depth	キューの深さの平均。これは、インターフェイスの実際のキューの深さおよび指数重み付け定数に基づいて算出されます。これは移動平均です。最小しきい値および最大しきい値と、この値とを比較してドロップの是非を決定します。
Class	IP プレシデンス値です。
Random drop	キューの深さの平均が、指定された IP プレシデンス値の最小しきい値と最大しきい値の間である場合に、ランダムにドロップされたパケット数。
Tail drop	キューの深さの平均が、指定された IP プレシデンス値の最大しきい値を上回る場合に、ランダムにドロップされたパケット数（バイト単位でも表示）。
Minimum threshold	WRED 最小しきい値（パケット数単位）。
Maximum threshold	WRED 最大しきい値（パケット数単位）。

フィールド	説明
Mark probability	平均キューの深さが最大しきい値の場合にドロップされたパケットの割合。

関連コマンド

Command	Description
custom-queue-list	カスタムキューリストをインターフェイスに割り当てます。
exponential-weighting-constant	WRED パラメータ グループの平均キュー サイズ計算のための指数加重係数を設定します。
fair-queue(WFQ)	インターフェイスに対する WFQ を有効にします。
frame-relayinterface-queuepriority	FR PIPQ 機能を有効にします。
precedence(WREDgroup)	特定の IP Precedence に対して WRED グループを設定します。
priority-group	指定した優先リストをインターフェイスに割り当てます。
priority-listinterface	特定のインターフェイスから着信するパケットのキューイング プライオリティを確立します。
priority-listqueue-limit	各プライオリティ キューで待機可能なパケットの最大数を指定します。
queue-listinterface	インターフェイスに着信するパケットのキューイング プライオリティを確立します。
queue-listqueuebyte-count	特定のサイクル中に特定のキューからシステムが配信できるバイト数を指定します。
random-detect(interface)	WRED または DWRED をイネーブルにします。
random-detectflowaverage-depth-factor	乗数を、フローベース WRED が有効な場合にフローの平均深度係数の決定に使用するために設定します。
random-detectflowcount	フローベース WRED のフローカウントを設定します。
showinterfaces	シリアルインターフェイスに固有の統計情報を表示します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。

Command	Description
showqueueinginterface	インターフェイスまたは VC のキューイングの統計情報を表示します。

show queueing interface

インターフェイスのキューイング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 **showqueueinginterface** コマンドを使用します。

show queueing interface *type number* [**vc** [[*vpi*/] *vci*]]

Catalyst 6500 シリーズ スイッチ
show queueing interface {*type number*|**null 0**|**vlan** *vlan-id*} **[detailed]**

Cisco 7600 シリーズ ルータ
show queueing interface {*type number*|**null 0**|**vlan** *vlan-id*}

構文の説明

type number	インターフェイス タイプとインターフェイス番号 Cisco 7600 シリーズ ルータの場合、有効なインターフェイス タイプは **ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**、**pos**、**atm**、および **ge-wan** です。 Cisco 7600 シリーズ ルータの場合、インターフェイス番号はモジュールおよびポート番号です。詳細については、「使用上のガイドライン」を参照してください。
vc	（任意）特定の仮想回線（VC）に関連付けられた重み付け均等化キューイング（WFQ）および重み付けランダム早期検出（WRED）パラメータを表示します。必要に応じて、仮想パス識別子（VPI）と仮想チャネル識別子（VCI）の両方の値か、または VCI 値だけを指定できます。
vpi /	（任意）VPI。*vpi* 引数を省略すると、相手先固定接続（PVC）の位置を特定するための VPI の値として 0 が使用されます。*vpi* 引数を指定する場合は、/ 区切り記号が必要です。
vci	（任意）VCI。
null0	null インターフェイス番号を指定します。唯一有効な値は 0 です。
vlan *vlan-id*	VLAN 識別番号を指定します。有効な値は 1 ～ 4094 です。
detailed	（任意）ポリシー クラス単位で詳細な統計情報を表示します。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

Cisco 7600 シリーズ ルータ

ユーザ EXEC (>)

コマンド履歴

リリース	変更箇所
11.1(22)CC	このコマンドが導入されました。
12.2(14)SX	このコマンドがスーパーバイザ エンジン 720 に実装されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
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。
12.2(33)SXI	**detailed** キーワードが追加されました。

使用上のガイドライン

Cisco 7600 シリーズ ルータ

pos、atm、および ge-wan インターフェイスは、スーパバイザ エンジン 2 が搭載された Cisco 7600 シリーズ ルータでのみサポートされています。

typenumber 引数を **interface** キーワードとともに使用すると、モジュール番号とポート番号を指定できます。有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。たとえば、ギガビット イーサネット インターフェイスを指定し、13 スロット シャーシに設置された 48 ポート 10/100BASE-T イーサネット モジュールを使用する場合、モジュール番号の有効値の範囲は 1 ～ 13 であり、ポート番号の有効値の範囲は 1 ～ 48 です。

showqueueinginterface コマンドは、ハードウェアにプログラミングされた絶対値を表示しません。ハードウェアにプログラミングされた値を検証するには、**showqm-spport-data** コマンドを使用します。

Catalyst 6500 シリーズ スイッチ

Cisco IOS リリース 12.2(33)SXI 以降のリリースでは、オプションの **detailed** キーワードを使用できます。**showqueueinginterfacedetailed** コマンドの出力には、次の情報が含まれています。

- 過去 30 秒のカウンタの表示。
- 過去 5 分にわたるピーク 30 秒のカウンタの表示。
- 5 分平均およびピークの pps レートの表示。
- ピーク レートは、10 秒の解像度でモニタされます。Cisco IOS リリース 12.2(33)SXI より前のリリースは、30 秒の解像度でモニタされていました。

例

次に、**showqueueinginterface** コマンドの出力例を示します。この例では、WRED が使用中のキューイング戦略です。出力は、使用中のキューイング戦略によって異なります。

```
Router# show queueing interface atm 2/0
  Interface ATM2/0 VC 201/201
  Queueing strategy:random early detection (WRED)
    Exp-weight-constant:9 (1/512)
```

```
Mean queue depth:49
Total output drops per VC:759
Class    Random       Tail    Minimum    Maximum     Mark
           drop       drop  threshold  threshold  probability
  0         165         26         30         50     1/10
  1         167         12         32         50     1/10
  2         173         14         34         50     1/10
  3         177         25         36         50     1/10
  4           0          0         38         50     1/10
  5           0          0         40         50     1/10
  6           0          0         42         50     1/10
  7           0          0         44         50     1/10
 rsvp         0          0         46         50     1/10
```

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 *250 : show queueing interface* フィールドの説明

フィールド	説明
Queueing strategy	使用中のキューイング戦略の名前（たとえば、WRED）。
Exp-weight-constant	指数加重定数。WRED パラメータ グループのために平均キュー サイズの計算に使用される指数。
Mean queue depth	インターフェイスの実際のキューの深さおよび指数重み付け定数に基づいたキューの深さの平均。これは、変動する平均です。最小しきい値および最大しきい値と、この値とを比較してドロップの是非を決定します。
Class	IP precedence レベル。
Random drop	キューの深さの平均が、指定された IP precedence レベルの最小しきい値と最大しきい値の間である場合に、ランダムにドロップされたパケット数。
Tail drop	キューの深さの平均が、指定された IP precedence レベルの最大しきい値を上回る場合に、ランダムにドロップされたパケット数（バイト単位でも表示）。
Minimum threshold	WRED 最小しきい値（パケット単位）。
Maximum threshold	WRED 最大しきい値（パケット単位）。
Mark probability	平均キューの深さが最大しきい値の場合にドロップされたパケットの割合。

次に、Cisco IOS リリース 12.2(33)SXI 以降のリリースで **showqueueinginterface** コマンドを実行した場合の出力例を示します。

```
Router# show queueing interface gigabitethernet 3/27 detailed

.
.
.
  Packets dropped on Transmit:
```

```
   BPDU packets:  0
   queue  Total pkts   30-s pkts / peak   5 min average/peak pps   [cos-map]
-------------------------------------------------------------------------------
   1      443340       55523 / 66671      3334 / 44455             [0 1 ]
   1      7778888      555555 / 666666    233333 / 340000          [2 3 ]
   2      0            0 / 0              0 / 0                    [4 5 ]
   2      0            0 / 0              0 / 0                    [6 7 ]
.
.
.
```

次の表では、**detailed** キーワードを入力すると追加される重要なフィールドについて説明します。

表 *251 : show queueing interface detailed* フィールドの説明

フィールド	説明
Packets dropped on Transmit	送信中にドロップされたパケットに関する情報を表示します。
BPDU packets	ブリッジプロトコルデータユニット（BPDU）パケットの数。
queue	キュー番号。
Total pkts	過去 30 秒のカウンタの表示。
30-s pkts / peak	過去 5 分にわたるピーク 30 秒のカウンタの表示。
5 min average/peak pps	5 分平均およびピーク レートのパケット/秒（pps）の表示。
cos-map	サービス クラス（CoS）マッピング。

関連コマンド

custom-queue-list	カスタム キュー リストをインターフェイスに割り当てます。
fair-queue(class-default)	デフォルト クラス ポリシーの一部として class-default クラスで使用するために予約するダイナミック キューの数を指定します。
fair-queue(WFQ)	インターフェイスに対する WFQ を有効にします。
priority-group	指定した優先リストをインターフェイスに割り当てます。
random-detectflow	フローベース WRED をイネーブルにします。
random-detect(interface)	WRED または DWRED をイネーブルにします。
random-detect(perVC)	per-VC WRED または per-VC DWRED をイネーブルにします。
showframe-relaypvc	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。

showpolicy-mapinterface	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービス ポリシーのクラスを表示します。
showqm-spport-data	QoS Manager スイッチ プロセッサに関する情報を表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

show random-detect-group

（注） Cisco IOS リリース 15.0(1)S および Cisco IOS リリース 15.1(3)T では、**showrandom-detect-group** コマンドは非表示になります。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンドシーケンス）を使用する必要があります。詳細については（後継のコマンドのリストを含む）、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能のドキュメント、または『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能のドキュメントを参照してください。

重み付けランダム早期検出（WRED）または分散 WRED（DWRED）パラメータ グループを表示するには、特権 EXEC モードで **showrandom-detect-group** コマンドを使用します。

show random-detect-group [*group-name*]

構文の説明

group-name	（任意）WRED または DWRED パラメータ グループの名前。

コマンド デフォルト

WRED や DWRED パラメータ グループは表示されません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(22)T	このコマンドは、Cisco IOS Release 12.4(22)T よりも前のリリースに導入されました。
12.2(33)SRC	このコマンドは、Cisco IOS Release 12.2(33)SRC よりも前のリリースに統合されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI. よりも前のリリースに統合されました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。

使用上のガイドライン

WRED は輻輳回避メカニズムで、輻輳の発生時にランダムにパケットをドロップすることでトラフィックを低下させます。DWRED は WRED に類似していますが、Route Switch Processor（RSP）の代わりに Versatile Interface Processor（VIP）が使用されます。WRED と DWRED は、

転送速度を下げることによってドロップされるパケットに応答する、TCPのようなプロトコルをトラフィックが使用する際に最も効果的です。

例

次の例では、group-name という DWRED グループの現在の設定を表示しています。

```
Router# show random-detect-group group-name
exponential weight 9
class    min-threshold    max-threshold    mark-probablity
------------------------------------------------------------
0          -                -                1/10
1           1               2000             1/30
2           1               3000             1/40
3           1               4000             1/50
4           1               3000             1/60
5           1               3000             1/60
6           1               4000             1/60
7           1               4000             1/60
rsvp        1                1               1/10
```

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 *252 : show random-detect group* フィールドの説明

フィールド	説明
exponential weight	WRED パラメータ グループの平均キュー サイズ計算のための指数加重係数。
class	ポリシー マップ クラス名。
min-threshold	パケット数での最小しきい値。この引数に指定できる値の範囲は、1～4096です。平均キューの長さが最小しきい値に達すると、WRED では、指定された IP プレシデンスで一部のパケットがランダムにドロップされます。
max-threshold	パケット数での最大しきい値。この引数の値の範囲は、*min-threshold* 引数の最小値から4096までです。キューの平均の長さが最大しきい値を超えると、WRED は指定された IP プレシデンス値のすべてのパケットをドロップします。
mark-probability	平均キューの深さが最小しきい値の場合にドロップされたパケットの割合の分母。たとえば、分母が512の場合、平均キューが最小しきい値のときに、512パケットごとに1パケットがドロップされます。値の範囲は、1～65536です。デフォルトは10です。つまり、最小しきい値に達したときに、10パケットにつき 1 つのパケットがドロップされます。
rsvp	リソース予約プロトコル（RSVP）トラフィックを示します。

関連コマンド

Command	Description
dscp	DSCP 値の最小および最大パケットしきい値を変更します。

Command	Description
exponential-weighting-constant	WRED パラメータ グループの平均キュー サイズ計算のための指数加重係数を設定します。
precedence(WREDgroup)	特定の IP Precedence に対して WRED グループを設定します。
random-detect-group	WRED または DWRED パラメータ グループを定義します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。
showqueueinginterface	インターフェイスまたは VC のキューイングの統計情報を表示します。

show running-config service-group

1 つまたはすべてのサービス グループの実行コンフィギュレーションを表示するには、特権 EXEC モードで **showrunning-configservice-group** コマンドを使用します。

show running-config service-group [*service-group-identifier*]

構文の説明

service-group-identifier	（任意）サービス グループ番号。サービス グループ番号を入力します。

コマンド デフォルト

サービス グループ番号を指定しないと、すべてのサービス グループの情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRE	このコマンドが導入されました。

例

次に、実行中のすべてのサービス グループに関する情報を表示する例を示します。

```
Router# show running-config service-group
Building configuration...
Current configuration:
service-group 1
service-group 2
service-group 3
 service-policy output test
service-group 4
service-group 5
 service-policy output test
end
```

次に、実行中の特定のサービス グループに関する情報を表示する例を示します。次の例では、サービス グループ 700 を指定しています。

```
Router# show running-config service-group 700
Building configuration...
Current configuration:
service-group 700
 service-policy output test
end
```

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 *253 : show running-config service-group* フィールドの説明

フィールド	説明
service-group	サービス グループ番号を示します。

フィールド	説明
service-policyoutput	サービス グループにアタッチされている出力ポリシーを示します。

show sdm prefer current

システムに設定されたテンプレートを検証するには、プラットフォームの **show sdm prefer current** コマンド使用します。

show sdm prefer current

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

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
XE 3.18.1 SP	このコマンドのサポートが ASR 900 シリーズ ルータに追加されました。

例

次の例は、ポート チャネル アクティブ/アクティブ モードを有効にした後の設定の検証を示しています。

```
#show sdm prefer current
The current sdm template is "default"
The current portchannel template is "enable_portchannel_qos_multiple_active"
```

関連コマンド

コマンド	説明
show sdm prefer current	ポートチャネルアクティブ/アクティブモードを有効にした後で設定を検証します。
show etherchannel summary	ポートチャネル概要の詳細を検証します。
show policy-map interface brief	ポートチャネルインターフェイスでアタッチしたポリシーマップを検証します。

show service-group

特定のサービス グループまたはすべてのサービス グループのサービス グループ情報を表示するには、特権 EXEC モードで **showservice-group** コマンドを使用します。

show service-group {*service-group-identifier*|**all**} **[detail]**

構文の説明

service-group-identifier	サービス グループ番号。表示するサービス グループの番号を入力します。
all	すべてのサービス グループの情報を表示します。
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	変更箇所
12.2(33)SRE	このコマンドが導入されました。

使用上のガイドライン

メンバーシップやインターフェイスに関する統計情報や、ポリシーマップやメンバー識別番号に関する情報などを表示するには、**showservice-group** コマンドを使用します。

例

次に、**showservice-group** コマンドの出力例を示します。この例は、サービス グループ 1 の統計情報を表示しています。

```
Router# show service-group 1

Service Group 1:
  Number of members:                    2
  State:                                Up
  Interface:                            GigabitEthernet2/0/0
    Number of members:                  2
```

次に、**detail** キーワードを指定した **showservice-group** コマンドの出力例を示します。この例は、サービス グループ 1 の詳細な統計情報を表示しています。

```
Router# show service-group 1 detail
Service Group 1:
  Description: Test service group.
  Number of members:                    2
      Service Instance                  2
  State:                                Up
  Features configured:                  QoS
  Input service policy:                 in1
  Output service policy:                out1
  Number of Interfaces:                 1
  Interface:                            GigabitEthernet2/0/0
    Number of members:                  2
```

```
Service Instance ID:
    1
    3
```

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 *254 : show service-group* フィールドの説明

フィールド	説明
Service Group 1	サービス グループ番号。
Number of members	サービス グループ内のメンバー数。サービス インスタンス番号も含まれています。
State	サービス グループの管理状態を示します。 （注） Cisco IOS リリース 12.2(33)SRE では、管理状態は常に「Up」であり、変更することはできません。
Interface	サービス グループが適宜メンバーの番号とともにアタッチされるインターフェイス。

次の表では、**detail** キーワードを指定した場合に、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 *255 : show service-group detail* フィールドの説明

フィールド	説明
Service Group	サービス グループ番号。
Description	サービス グループの説明。
Number of members	サービス グループ内のメンバー数。サービス インスタンス番号も含まれています。
State	サービス グループの管理状態を示します。 （注） Cisco IOS リリース 12.2(33)SRE では、管理状態は常に「Up」であり、変更することはできません。
Features configured	サービス グループに設定されている機能。 （注） Cisco IOS リリース 12.2(33)SRE の場合、Cisco 7600 シリーズ ルータでサポートされている機能は Quality of Service（QoS）のみです。
Input service policy	入力サービス ポリシーの名前。

フィールド	説明
Output service policy	出力サービス ポリシーの名前。
Number of Interfaces	インターフェイスの数。
Interface	インターフェイスの名前、サービス グループ内のメンバーの数、およびサービス インスタンス番号（ある場合）。

show service-group interface

インターフェイス別にサービス グループ メンバーシップ情報を表示するには、特権EXECモードで **showservice-groupinterface** コマンドを使用します。

show service-group interface *type number* [**group** *service-group-identifier*] **[detail]**

構文の説明

type	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	インターフェイス番号。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。
group	（任意）サービス グループ情報を表示します。
service-group-identifier	（任意）サービス グループ番号。表示するサービス グループの番号を入力します。
detail	（任意）すべてのグループの詳細な統計情報を表示します。

コマンド デフォルト

インターフェイスを指定しないと、すべてのインターフェイスについてサービス グループ情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRE	このコマンドが導入されました。

例

次に、ギガビット イーサネット インターフェイス 3/1 のサービス グループ メンバーシップ情報を表示する例を示します。

```
Router# show service-group interface gigabitethernet 3/1
Interface GigabitEthernet3/1:
  Number of groups:                     3
  Group
      1
      2
      3
This example shows how to display service-group detailed membership information for
Gigabit Ethernet interface 3/1:
Router# show service-group interface gigabitethernet 3/1 detail
Interface GigabitEthernet3/1:
  Number of groups:                     3
Service Group 1:
  Number of members:                    3000
    Service Instance ID:
```

```
          1
          2
          3
          4
          5
          6
          7
          8
          9
         10
        . . .
This example shows how to display detailed membership information for Gigabit Ethernet
interface 3/1 service group 10:
Router# show service-group interface gigabitethernet 3/1 group 10 detail
Service Group 10:
 Number of members:                     3
  Service Instance ID:
   100
   101
   102
```

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 *256 : show service-group interface service group* 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タイプと番号
Number of groups	グループの数
Service Group	サービス グループ番号。
Number of members	サービス グループ内のメンバー数。
Service Instance ID	サービス インスタンス識別子。

show service-group state

1 つまたはすべてのサービス グループの状態情報を表示するには、特権 EXEC モードで **showservice-groupstate** コマンドを使用します。

show service-group state [**group** *service-group-identifier*]

構文の説明

group	（任意）サービス グループ状態統計情報を表示します。
service-group-identifier	（任意）サービス グループ番号。表示するサービス グループの番号を入力します。

コマンド デフォルト

サービス グループ番号を指定しないと、すべてのサービス グループの情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRE	このコマンドが導入されました。

例

次は、**showservice-groupstate** コマンドの出力例です。この例では、すべてのサービス グループの状態情報が表示されます。フィールドの説明は自明です。

（注） Cisco IOS リリース 12.2(33)SRE では、状態は常に「Up」であり、変更することはできません。

```
Router# show service-group state
    Group      State
      1         Up
      2         Up
      3         Up
     10         Up
     20         Up
```

show service-group stats

サービス グループ統計情報を表示するには、特権 EXEC モードで **showservice-groupstats** コマンドを使用します。

show service-group stats [{**errors**|**group** *service-group-identifier*|**interface** *type number*|**module** *slot*}]

構文の説明

errors	（任意）サービス グループ エラーを表示します。
group	（任意）サービス グループ統計情報を表示します。
service-group-identifier	（任意）サービス グループ番号。表示するサービス グループの番号を入力します。
interface	（任意）指定されたインターフェイスの統計情報を表示します。
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）インターフェイス番号。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。
module	（任意）設定されたモジュールの統計情報を表示します。
slot	（任意）モジュール スロット。有効なエントリの範囲は、インターフェイスによって異なります。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。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRE	このコマンドが導入されました。

例

次のセクションには、さまざまなキーワードおよび引数を指定したこのコマンドの出力例が含まれています。出力にはフィールドの説明も表示されます。

次に、すべてのサービス グループ統計情報を表示する例を示します。

```
Router# show service-group stats
Service Group global statistics:
  Number of groups:                     5
  Number of members:                    8005
Service Group 1 statistics:
```

```
  Number of Interfaces:                   1
  Number of members:                      3000
    Service Instance                      3000
  Members joined:                         13000
  Members left:                           10000
Service Group 2 statistics:
  Number of Interfaces:                   1
  Number of members:                      2000
    Service Instance                      2000
  Members joined:                         10000
  Members left:                           8000
Service Group 3 statistics:
  Number of Interfaces:                   1
  Number of members:                      3000
    Service Instance                      3000
  Members joined:                         9000
  Members left:                           6000
Service Group 10 statistics:
  Number of Interfaces:                   1
  Number of members:                      3
    Service Instance                      3
  Members joined:                         8003
  Members left:                           8000
Service Group 20 statistics:
  Number of Interfaces:                   1
  Number of members:                      2
    Service Instance                      2
  Members joined:                         8002
  Members left:                           8000
This example shows how to display all error statistics for all service groups:
Router# show service-group stats errors
Service Group 1 errors:
  Members rejected to join:
    Capability limitation:                0
    Rejected by other software modules:   0
    Failed to install service policy:     0
    Database error:                       0
    Feature encountered error:            0
    Invalid member type:                  0
    Invalid member id:                    0
Service Group 2 errors:
  Members rejected to join:
    Capability limitation:                0
    Rejected by other software modules:   0
    Failed to install service policy:     0
    Database error:                       0
    Feature encountered error:            0
    Invalid member type:                  0
    Invalid member id:                    0
Service Group 3 errors:
  Members rejected to join:
    Capability limitation:                0
    Rejected by other software modules:   0
    Failed to install service policy:     0
    Database error:                       0
    Feature encountered error:            0
    Invalid member type:                  0
    Invalid member id:                    0
This example shows how to display statistics for service group 20:
Router# show service-group stats group 20
Service Group 20 statistics:
  Number of Interfaces:                   1
  Number of members:                      2
    Service Instance:                     2
```

```
  Members joined:                         8002
  Members left:                           8000
This example shows how to display statistics for the service-groups on a specific
interface:
Router# show service-group stats interface gigabitethernet2/0/0

Interface GigabitEthernet2/0/0:
  Number of groups:                       1
  Number of members:                      2
  Group  Members  Service Instances
      1        2                 2
This example shows how to display statistics for the service-groups on module 3:
Router# show service-group stats module 3
Module 3:
  Number of groups:                       3
  Number of members:                      8000
  Group               Interface  Members  Service Instances
      1       GigabitEthernet3/1     3000               3000
      2       GigabitEthernet3/1     2000               2000
      3       GigabitEthernet3/1     3000               3000
```

show service-group traffic-stats

サービス グループ トラフィック統計情報を表示するには、特権 EXEC モードで **showservice-grouptraffic-stats** コマンドを使用します。

show service-group traffic-stats [**group** *service-group-identifier*]

構文の説明

group	（任意）サービス グループ統計情報を表示します。
service-group-identifier	（任意）サービス グループ識別子。既存のサービス グループの番号を入力します。

コマンド デフォルト

サービス グループ番号を指定しないと、すべてのサービス グループの情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRE	このコマンドが導入されました。

使用上のガイドライン

showservice-grouptraffic-stats コマンドは、サービス グループの全メンバーのトラフィック統計情報をまとめた合計をレポートします。

トラフィック統計情報の収集方法

サービス グループの各メンバーのトラフィック統計情報が蓄積されて、定期的に加算されます。メンバーの統計情報が加算されるたびに、グループ統計情報も同じ量だけ加算されます。次の点に注意してください。

- メンバーがサービス グループに加わると、サービス グループ トラフィック統計情報は全メンバーのトラフィック統計情報の総計となります。グループに加わる前に収集されたトラフィック統計情報は含まれません。このため、任意の時点で、メンバーのトラフィック統計情報の合計がグループのトラフィック統計情報よりも大きくなる場合があります。
- メンバーのトラフィック統計情報は、**clearethernetserviceinstance** コマンドを使用してクリアできます。メンバーのトラフィック統計情報をクリアしても、グループの統計情報には影響しません。
- グループのトラフィック統計情報をクリアしても、グループ メンバーのトラフィック統計情報はクリアされません。

例

次のセクションでは、**showservice-grouptraffic-stats** コマンドの出力例を示します。出力にはフィールドの説明も表示されます。

次に、すべてのサービス グループのトラフィック統計情報を表示する例を示します。

```
Router# show service-group traffic-stats
Traffic Statistics of service groups:
  Group     Pks In   Bytes In   Pkts Out  Bytes Out
      1          0          0          0          0
      2          0          0          0          0
      3          0          0          0          0
     10          0          0          0          0
     20          0          0          0          0
This example shows how to display traffic statistics for service group 10:
Router# show service-group traffic-stats group 10
Traffic Statistics of service groups:
  Group     Pks In   Bytes In   Pkts Out  Bytes Out
     10          0          0          0          0
```

関連コマンド

コマンド	説明
clearethernetserviceinstance	MAC アドレスなどのイーサネット サービス インスタンス属性と統計をクリアし、イーサネットサービスインスタンスのエラーを消去します。

show subscriber policy ppm-shim-db

ルータ上で動的に作成されたテンプレート サービス ポリシー マップおよびNet Effect ポリシー マップの合計数を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showsubscriberpolicyppm-shim-db** コマンドを使用します。

show subscriber policy ppm-shim-db

構文の説明

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	変更箇所
Cisco IOS Release XE 3.2S	このコマンドは、ASR 1000 シリーズのアグリゲーション サービス ルータに導入されました。

例

次は、**showsubscriberpolicyppm-shim-db** コマンドの出力例です。

```
Router# show subscriber policy ppm-shim-db
Total number of dynamically created policy = 10
The output fields are self-explanatory.
```

show table-map

指定されたテーブルマップまたはすべてのテーブルマップの設定を表示するには、EXECモードで **showtable-map** コマンドを使用します。

show table-map *table-map-name*

構文の説明

table-map-name	パケットマーキング値同士をマップするために使用されるテーブル マップの名前。この名前には最大 64 文字までの英数字を指定できます。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。

例

showtable-map コマンドの出力例では、「map 1」というテーブルマップの内容を表示しています。「map1」では、「to-from」の関係が確立され、デフォルト値が定義されています。さらに「to-from」のマッピングを確立するためのフィールドが、テーブルマップの設定先となるポリシーマップによって定義されます。（ポリシーマップの設定は、テーブル マップの作成後に続く次の論理的な手順です。）

たとえば、値 0 の優先順位や DiffServ コード ポイント（DSCP）を値 1 のサービス クラス（CoS）にマップしたり、その逆方向にマップしたりでき、これは値をテーブルマップにどのように定義するかによって異なります。「to-from」の関係に明示的に定義されていない値は、デフォルト値に設定されます。

showtable-map コマンドの次の出力例では、「map1」というテーブル マップの内容を表示しています。このテーブル マップでは、パケットマーキング値 0 がパケットマーキング値 1 にマップされています。他のすべてのパケットマーキング値は、デフォルト値 3 にマップされています。

```
Router# show table-map map1
 Table Map map1
 from 0 to 1
 default 3
```

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。

表 *257 : show table-map* フィールドの説明

フィールド	説明
Table Map	表示されているテーブル マップの名前。

フィールド	説明
from, to	**table-map**（値マッピング）コマンドによって確立され、さらにテーブルマップの設定先となるポリシー マップによって定義される「to-from」の関係の値。
default	**table-map**（値マッピング）コマンドによって「to-from」の関係に明示的に定義されていない値に使用されるデフォルトのアクション。デフォルトのアクションを table-map（値マッピング）コマンドに指定しない場合、デフォルトのアクションは「コピー」になります。

関連コマンド

コマンド	説明
policy-map	1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapclass	指定されたポリシー マップの指定されたクラスの設定を表示します。
table-map(valuemapping)	1 つの packet-marking 値を別の値にマッピングおよび変換するための、マッピング テーブルを作成します。

show tech-support nbar platform

Network-Based Application Recognition（NBAR）に関する一般的な情報を表示するには、特権 EXEC モードで show tech-support nbar platform コマンドを使用します。

show tech-support nbar platform

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE Release XE 3.10S	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 tech-support nbar platform コマンドは、次のコマンド出力を表示します：**show ip nbar protocol activated**， **show ip nbar attribute-map**， **show ip nbar parameter extraction activated**， **show ip nbar parameter subclassification activated**， **show ip nbar protocol-attribute**， **show ip nbar protocol-discovery**， **show ip nbar protocol-pack active**， **show ip nbar resources**， **show ip nbar resources flow**， **show ip nbar statistics**， **show ip nbar version**， **show platform hardware qfp active feature nbar profiling**， **show platform software nbar statistics**， and **show policy-map interface**。また、次の関数の出力も表示します：st_sui_fia_show、st_sui_fia_ut_mean_func_show、st_sui_fe_show、st_sui_fv_stats_show、st_sui_mpe_chunk_utl_show、st_sui_mpe_dp_utl_show、st_sui_mtp_dp_dump_external_flags、st_sui_mtp_dp_show_cfg、st_sui_mtp_dp_show_prs_graph、st_sui_mtp_stats_general、st_sui_stile_is_ready、st_sui_stile_show_cls_err_cnt、st_sui_stile_show_msc。これらの関数は **show platform hardware qfp active feature nbar function** コマンドとともに使用され、たとえば、**show platform hardware qfp active feature nbar function** *st_sui_fe_show* というようになります。

例

次の例は、NBAR 情報を表示する **show tech-support nbar platform** コマンドの出力からの抜粋です。

```
Device# show tech-support nbar platform

------------------ show running-config ------------------


Building configuration...

Current configuration : 1600 bytes
!
! Last configuration change at 04:16:19 PST Thu Jul 25 2013
!
version 15.3
service timestamps debug uptime
service timestamps log uptime
!
hostname R1
!
boot-start-marker
boot-end-marker
```

```
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
!
!
!
!
!


!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Tunnel21
 no ip address
 ip nbar protocol-discovery
!
interface Ethernet0/0
 no ip address
 shutdown
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 no ip address
 shutdown
!
interface Ethernet1/1
```

```
 no ip address
 ip nbar protocol-discovery
 shutdown
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
!
!
no ip http server
!
!
!
!
control-plane
!
!
line con 0
```

```
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
!
end


------------------ show ip nbar statistics ------------------



Compiler statistics
Malloc failure = 0
Control-plane statistics
Malloc failure = 0
Invalid iterators = 0
Data-plane statistics
Malloc failure = 0
FO create failure = 0
CFT Age set failure = 0
L3 Classification Error = 0

------------------ show ip nbar resources ------------------

NBAR memory usage for tracking Stateful sessions
   System link age      : 30 secs
   Initial memory       : 4160 KBytes
   Max initial memory   : 13868 KBytes
   Memory expansion     : 128 KBytes
   Max memory expansion : 128 KBytes
   Memory in use        : 4160 KBytes
   Max memory allowed   : 27736 KBytes
   Active links         : 0
   Total links          : 32504
   Flow Object in Use   : 0


------------------ show ip nbar protocol activated ------------------



Following Protocol(s) is(are) enabled
 Feature:PD
       Hwidb:Tunnel21 MI:1 SI:0 FR:0 PVC:0
       Hwidb:Ethernet1/1 MI:1 SI:0 FR:0 PVC:0
All iana protocols



------------------ show ip nbar version ------------------




NBAR software version:  16
NBAR minimum backward compatible version:  13

1   base                              Mv: 6
2   ftp                               Mv: 7
      Iv:                              smtp - 2
      Iv:                            gridftp - 1
```

```
      Iv:                          ftp-data - 1
3   ftp-data                          Mv: 1
      Iv:                               ftp - 7
      Iv:                              smtp - 2
      Iv:                            gridftp - 1
4   http                              Mv: 20
      Iv:                           youtube - 6
      Iv:                     msn-messenger - 3
      Iv:                    yahoo-messenger - 3
      Iv:                        flash-video - 2
      Iv:                         flashyahoo - 2
      Iv:                       flashmyspace - 2
      Iv:                     audio-over-http - 2
      Iv:                    binary-over-http - 2
      Iv:                     video-over-http - 2
      Iv:                                 irc - 2
      Iv:                           babelgum - 1
      Iv:                             itunes - 1
      Iv:                              sling - 1
      Iv:                         google-earth - 1
      Iv:                          baidu-movie - 1
      Iv:                                pando - 1
      Iv:                             napster - 1
      Iv:                            songsari - 1
      Iv:                           webthunder - 1
      Iv:                              sopcast - 3
      Iv:                           tunnel-http - 1
      Iv:                              soribada - 2
      Iv:                                   icq - 1
      Iv:                                skype - 5
      Iv:                              edonkey - 7
      Iv:                         directconnect - 5
      Iv:                              gnutella - 7
      Iv:                            ms-update - 1
      Iv:                                 rtsp - 9
      Iv:                              netflix - 1
      Iv:                            megavideo - 1
      Iv:                           bittorrent - 5
      Iv:                                  tor - 1
      Iv:                                gmail - 1
      Iv:                                gtalk - 1
      Iv:                            gtalk-voip - 1
      Iv:                           gtalk-video - 1
      Iv:                            activesync - 1
      Iv:                              rhapsody - 1
      Iv:                                 fring - 1
      Iv:                                 rtmpt - 1
      Iv:                           livestation - 1
      Iv:                            secondlife - 1
      Iv:                              vnc-http - 1
      Iv:                           share-point - 1
      Iv:                         ms-office-365 - 1
      Iv:                                ms-sms - 1
      Iv:                             ghostsurf - 1
      Iv:                              gotomypc - 1
      Iv:                         adobe-connect - 1
      Iv:                             realmedia - 1
      Iv:                         windows-azure - 1
      Iv:                       ms-live-accounts - 1
      Iv:                          aol-messenger - 2
      Iv:                    aol-messenger-video - 1
      Iv:                                mikogo - 1
      Iv:                                pandora - 1
      Iv:               oracle-ebsuite-unsecured - 1
```

```
      Iv:                          hotmail - 1
      Iv:                         facebook - 1
      Iv:                          twitter - 1
      Iv:                             hulu - 1
      Iv:                          blogger - 1
      Iv:                       yahoo-mail - 1
      Iv:                         linkedin - 1
      Iv:                          logmein - 1
      Iv:                          gbridge - 1
      Iv:                           citrix - 12
      Iv:                              ssl - 1
      Iv:                         showmypc - 1
      Iv:                   yahoo-accounts - 1
      Iv:                         exchange - 4
      Iv:                       salesforce - 1
      Iv:                         ppstream - 1
      Iv:                          ms-lync - 1
      Iv:                           qqlive - 1
      Iv:                             pptv - 1
      Iv:                           xunlei - 1
      Iv:           bittorrent-networking - 1
      Iv:                       shoutcast - 1
      Iv:                     xunlei-kankan - 1
5   static                            Mv: 6
6   socks                             Mv: 3
7   nntp                              Mv: 2
      Iv:                 yahoo-messenger - 3
8   tftp                              Mv: 2
9   ms-rpc                            Mv: 2
      Iv:                         exchange - 4
      Iv:                      ms-netlogon - 1
      Iv:                       ms-win-dns - 1
      Iv:                           ms-iis - 1
      Iv:                 active-directory - 1
10  exchange                          Mv: 4
      Iv:                            ms-rpc - 2
      Iv:                              http - 20
11  vdolive                           Mv: 1
12  sqlnet                            Mv: 2
13  oracle-sqlnet                     Mv: 2
14  netshow                           Mv: 3
15  sunrpc                            Mv: 3
      Iv:                              nfs - 1
      Iv:                         clearcase - 1
16  nfs                               Mv: 1
17  streamwork                        Mv: 2
18  citrix                            Mv: 12
      Iv:                              http - 20
19  fasttrack                         Mv: 3
20  gnutella                          Mv: 7
      Iv:                              http - 20
21  kazaa2                            Mv: 11
22  dhcp                              Mv: 1
23  rtsp                              Mv: 9
      Iv:                           youtube - 6
      Iv:                              http - 20
24  webex-meeting                     Mv: 1
      Iv:                              ssl - 1
      Iv:                             spdy - 1
      Iv:                             http - 20
25  rtp                               Mv: 8
      Iv:                          stun-nat - 1
      Iv:                        gtalk-voip - 1
      Iv:                       gtalk-video - 1
```

```
      Iv:                     ms-lync-media - 1
26  mgcp                              Mv: 2
27  skinny                            Mv: 3
      Iv:                       cisco-phone - 4
28  sip                               Mv: 5
      Iv:                       cisco-phone - 4
      Iv:             telepresence-control - 4
      Iv:              yahoo-voip-over-sip - 1
      Iv:                        secondlife - 1
      Iv:                          stun-nat - 1
      Iv:                          facetime - 1
29  rtcp                              Mv: 5
      Iv:             telepresence-control - 4
      Iv:                          stun-nat - 1
30  edonkey                           Mv: 7
      Iv:                           http - 20
31  winmx                             Mv: 5
32  bittorrent                        Mv: 5
      Iv:                         blizwow - 2
      Iv:                           socks - 3
      Iv:                            http - 20
      Iv:                             dht - 1
      Iv:            bittorrent-networking - 1
33  directconnect                     Mv: 5
      Iv:                            http - 20
34  hl7                               Mv: 3
35  fix                               Mv: 3
      Iv:                             ssl - 1
      Iv:                            spdy - 1
36  msn-messenger                     Mv: 3
      Iv:                            http - 20
      Iv:                           ms-wbt - 1
      Iv:                           socks - 3
      Iv:                 msn-messenger-ft - 1
      Iv:                             ssl - 1
37  ms-live-accounts                  Mv: 1
      Iv:                            http - 20
      Iv:                             ssl - 1
38  windows-azure                     Mv: 1
      Iv:                            http - 20
      Iv:                             ssl - 1
39  pandora                           Mv: 1
      Iv:                            http - 20
      Iv:                             ssl - 1
40  oracle-ebsuite-unsecured          Mv: 1
      Iv:                            http - 20
41  hotmail                           Mv: 1
      Iv:                            http - 20
      Iv:                             ssl - 1
42  dicom                             Mv: 4
43  yahoo-messenger                   Mv: 3
      Iv:                            http - 20
      Iv:                            nntp - 2
      Iv:                           socks - 3
      Iv:                             ssl - 1
      Iv:                            spdy - 1
44  bgp                               Mv: 1
45  l2tp                              Mv: 1
46  mapi                              Mv: 3
47  cifs                              Mv: 2
48  cisco-phone                       Mv: 4
      Iv:                             sip - 5
      Iv:                          skinny - 3
      Iv:             telepresence-control - 4
```

```
49  youtube                          Mv: 6
      Iv:                             http - 20
      Iv:                             rtsp - 9
      Iv:                              ssl - 1
50  realmedia                        Mv: 1
      Iv:                             http - 20
      Iv:                             rtsp - 9
      Iv:                              ssl - 1
51  imap                             Mv: 1
52  pop3                             Mv: 1
53  irc                              Mv: 2
      Iv:                             http - 20
54  skype                            Mv: 5
      Iv:                             http - 20
      Iv:                              dns - 1
55  blizwow                          Mv: 2
      Iv:                          bittorrent - 5
56  telepresence-media               Mv: 3
57  telepresence-control             Mv: 4
      Iv:                              rtcp - 5
      Iv:                         cisco-phone - 4
      Iv:                              sip - 5
58  zattoo                           Mv: 3
59  sopcast                          Mv: 3
      Iv:                             http - 20
60  flash-video                      Mv: 2
      Iv:                             http - 20
61  flashyahoo                       Mv: 2
      Iv:                             http - 20
62  flashmyspace                     Mv: 2
      Iv:                             http - 20
63  audio-over-http                  Mv: 2
      Iv:                             http - 20
64  binary-over-http                 Mv: 2
      Iv:                             http - 20
65  video-over-http                  Mv: 2
      Iv:                             http - 20
66  my-jabber-ft                     Mv: 1
67  ayiya-ipv6-tunneled              Mv: 1
68  filetopia                        Mv: 1
69  guruguru                         Mv: 1
70  manolito                         Mv: 1
71  radius                           Mv: 1
72  teamspeak                        Mv: 1
73  soribada                         Mv: 2
      Iv:                             http - 20
74  dht                              Mv: 1
75  pptp                             Mv: 2
76  ntp                              Mv: 1
77  poco                             Mv: 2
78  ventrilo                         Mv: 1
79  tomatopang                       Mv: 1
80  maplestory                       Mv: 1
81  itunes                           Mv: 1
      Iv:                             http - 20
82  napster                          Mv: 1
      Iv:                             http - 20
83  sling                            Mv: 1
      Iv:                             http - 20
84  google-earth                     Mv: 1
      Iv:                             http - 20
85  baidu-movie                      Mv: 1
      Iv:                             http - 20
86  pando                            Mv: 1
```

```
      Iv:                                http - 20
87  webthunder                          Mv: 1
      Iv:                                http - 20
      Iv:                               xunlei - 1
88  babelgum                            Mv: 1
      Iv:                                http - 20
89  songsari                            Mv: 1
      Iv:                                http - 20
90  tunnel-http                         Mv: 1
      Iv:                                http - 20
91  teredo-ipv6-tunneled                Mv: 1
92  sixtofour-ipv6-tunneled             Mv: 1
      Iv:               isatap-ipv6-tunneled - 1
93  isatap-ipv6-tunneled                Mv: 1
      Iv:          sixtofour-ipv6-tunneled - 1
94  fring                               Mv: 1
      Iv:                                http - 20
95  fring-voip                          Mv: 1
      Iv:                         fring-video - 1
96  fring-video                         Mv: 1
      Iv:                          fring-voip - 1
97  waste                               Mv: 1
98  kuro                                Mv: 1
99  smtp                                Mv: 2
      Iv:                                 ftp - 7
100  icq                                Mv: 1
      Iv:                                http - 20
101  soulseek                           Mv: 1
102  yahoo-voip-messenger               Mv: 2
      Iv:                                 rtp - 8
103  yahoo-voip-over-sip                Mv: 1
      Iv:                                 sip - 5
104  aol-protocol                       Mv: 1
      Iv:                       aol-messenger - 2
105  ipsec                              Mv: 1
106  isakmp                             Mv: 1
107  ppstream                           Mv: 1
      Iv:                                http - 20
108  rtmp                               Mv: 1
109  rtmpe                              Mv: 1
110  rtmpt                              Mv: 1
      Iv:                                http - 20
111  dns                                Mv: 1
      Iv:                           tcpoverdns - 1
      Iv:                                skype - 5
112  windows-update                     Mv: 1
113  encrypted-emule                    Mv: 1
114  networking-gnutella                Mv: 1
115  encrypted-bittorrent               Mv: 1
116  ms-wbt                             Mv: 1
      Iv:                       msn-messenger - 3
117  gmail                              Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
118  openvpn                            Mv: 1
      Iv:                                 ssl - 1
      Iv:                               spdy - 1
119  ssl                                Mv: 1
      Iv:                                 fix - 3
      Iv:                       webex-meeting - 1
      Iv:                             netflix - 1
      Iv:                               gmail - 1
      Iv:                         livemeeting - 1
      Iv:                         livestation - 1
```

```
      Iv:                              dmp - 1
      Iv:                          rhapsody - 1
      Iv:                        secondlife - 1
      Iv:                  ms-live-accounts - 1
      Iv:                   google-accounts - 1
      Iv:                  active-directory - 1
      Iv:                           sip-tls - 1
      Iv:                     ms-office-365 - 1
      Iv:                             pcoip - 1
      Iv:                       vmware-view - 1
      Iv:                           openvpn - 1
      Iv:                         ms-update - 1
      Iv:                             mysql - 1
      Iv:                          gotomypc - 1
      Iv:                         ghostsurf - 1
      Iv:                     adobe-connect - 1
      Iv:                     aol-messenger - 2
      Iv:                       share-point - 1
      Iv:                         realmedia - 1
      Iv:           ms-dynamics-crm-online - 1
      Iv:                   windows-azure - 1
      Iv:                           twitter - 1
      Iv:                              hulu - 1
      Iv:                            logmein - 1
      Iv:                             mikogo - 1
      Iv:                            pandora - 1
      Iv:                            hotmail - 1
      Iv:                           facebook - 1
      Iv:                    google-services - 1
      Iv:                        google-plus - 1
      Iv:                        google-docs - 1
      Iv:                             picasa - 1
      Iv:                         yahoo-mail - 1
      Iv:                            youtube - 6
      Iv:                          linkedin - 1
      Iv:                             gtalk - 1
      Iv:                              http - 20
      Iv:                          facetime - 1
      Iv:                          showmypc - 1
      Iv:                    yahoo-accounts - 1
      Iv:                   msn-messenger-ft - 1
      Iv:                      msn-messenger - 3
      Iv:                 msn-messenger-video - 1
      Iv:                             ms-lync - 1
      Iv:                                spdy - 1
120   aol-messenger                     Mv: 2
      Iv:                              socks - 3
      Iv:                                ssl - 1
      Iv:                               http - 20
      Iv:                               spdy - 1
121   ghostsurf                         Mv: 1
      Iv:                               http - 20
122   netflix                           Mv: 1
      Iv:                               http - 20
      Iv:                                ssl - 1
123   megavideo                         Mv: 1
      Iv:                               http - 20
124   stun-nat                          Mv: 1
      Iv:                                ssl - 1
      Iv:                               spdy - 1
      Iv:                         ms-lync-media - 1
125   viber                             Mv: 1
126   cisco-ip-camera                   Mv: 1
      Iv:                               rtsp - 9
```

```
127  livestation                      Mv: 1
      Iv:                             http - 20
      Iv:                             rtmp - 1
      Iv:                              ssl - 1
128  gridftp                          Mv: 1
      Iv:                              ftp - 7
129  winny                            Mv: 1
130  livemeeting                      Mv: 1
      Iv:                              ssl - 1
      Iv:                         stun-nat - 1
      Iv:                             spdy - 1
131  tor                              Mv: 1
      Iv:                             http - 20
      Iv:                              ssl - 1
132  xmpp-client                      Mv: 1
133  gtalk-chat                       Mv: 1
      Iv:                        xmpp-client - 1
134  gtalk                            Mv: 1
      Iv:                             http - 20
      Iv:                        stun-nat - 1
      Iv:                       gtalk-video - 1
      Iv:                        gtalk-voip - 1
      Iv:                          gtalk-ft - 1
      Iv:                               ssl - 1
135  gtalk-voip                       Mv: 1
      Iv:                             http - 20
      Iv:                         stun-nat - 1
      Iv:                            gtalk - 1
      Iv:                              rtp - 8
136  gtalk-ft                         Mv: 1
      Iv:                         stun-nat - 1
      Iv:                            gtalk - 1
137  gtalk-video                      Mv: 1
      Iv:                             http - 20
      Iv:                         stun-nat - 1
      Iv:                            gtalk - 1
138  steam                            Mv: 1
139  ping                             Mv: 1
140  exec                             Mv: 1
141  login                            Mv: 1
142  shell                            Mv: 1
143  netapp-snapmirror                Mv: 1
144  ms-iis                           Mv: 1
      Iv:                           ms-rpc - 2
145  ms-win-dns                         Mv: 1
      Iv:                           ms-rpc - 2
146  ms-netlogon                        Mv: 1
      Iv:                           ms-rpc - 2
147  ms-sms                             Mv: 1
      Iv:                             http - 20
      Iv:                         ms-update - 1
148  perforce                         Mv: 1
149  vnc                              Mv: 1
      Iv:              apple-remote-desktop - 1
150  vnc-http                         Mv: 1
      Iv:                             http - 20
151  secondlife                       Mv: 1
      Iv:                              ssl - 1
      Iv:                             http - 20
      Iv:                              sip - 5
      Iv:                             spdy - 1
152  msn-messenger-ft                 Mv: 1
      Iv:                     msn-messenger - 3
      Iv:                              ssl - 1
```

```
      Iv:                              socks - 3
      Iv:                               spdy - 1
153   icq-filetransfer                 Mv: 1
154   tcpoverdns                       Mv: 1
      Iv:                               dns - 1
155   msn-messenger-video              Mv: 1
      Iv:                          stun-nat - 1
      Iv:                               rtp - 8
      Iv:                     msn-messenger - 3
      Iv:                             socks - 3
      Iv:                               ssl - 1
156   share-point                      Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
157   sip-tls                          Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
158   activesync                       Mv: 1
      Iv:                              http - 20
159   rhapsody                         Mv: 1
      Iv:                              http - 20
      Iv:                              rtmp - 1
      Iv:                               ssl - 1
160   ip-messenger                     Mv: 1
161   capwap-control                   Mv: 1
      Iv:                       capwap-data - 1
162   capwap-data                      Mv: 1
      Iv:                    capwap-control - 1
163   dmp                              Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
164   netbios-ns                       Mv: 1
165   ldap                             Mv: 1
166   active-directory                 Mv: 1
      Iv:                             ms-rpc - 2
      Iv:                               cifs - 2
      Iv:                               ldap - 1
      Iv:                               ssl - 1
167   google-accounts                  Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
168   ms-office-365                    Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
169   teamviewer                       Mv: 1
170   pcanywhere                       Mv: 1
171   snmp                             Mv: 1
172   vmware-vmotion                   Mv: 1
173   pcoip                            Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
174   vmware-view                      Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
175   gotomypc                         Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
176   ms-dynamics-crm-online           Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
177   kerberos                         Mv: 1
178   clearcase                        Mv: 1
179   ms-update                        Mv: 1
      Iv:                               ssl - 1
```

```
      Iv:                                http - 20
      Iv:                              ms-sms - 1
      Iv:                                spdy - 1
180   mysql                              Mv: 1
      Iv:                                 ssl - 1
181   google-services                    Mv: 1
      Iv:                                 ssl - 1
      Iv:                                spdy - 1
182   google-plus                        Mv: 1
      Iv:                                 ssl - 1
      Iv:                                spdy - 1
183   google-docs                        Mv: 1
      Iv:                                 ssl - 1
      Iv:                                spdy - 1
184   picasa                             Mv: 1
      Iv:                                 ssl - 1
      Iv:                                spdy - 1
185   blogger                            Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
      Iv:                              gmail - 1
      Iv:                     google-services - 1
      Iv:                                spdy - 1
186   sqlserver                          Mv: 1
      Iv:                                cifs - 2
187   adobe-connect                      Mv: 1
      Iv:                                rtmp - 1
      Iv:                                 ssl - 1
      Iv:                                http - 20
      Iv:                                spdy - 1
188   aol-messenger-audio                Mv: 1
      Iv:                                 rtp - 8
189   aol-messenger-video                Mv: 1
      Iv:                 aol-messenger-audio - 1
      Iv:                                 rtp - 8
      Iv:                                http - 20
      Iv:                              stun-nat - 1
      Iv:                                rtmp - 1
190   aol-messenger-ft                   Mv: 1
      Iv:                 aol-messenger-audio - 1
191   facebook                           Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
192   xunlei                             Mv: 1
      Iv:                                http - 20
      Iv:                       xunlei-kankan - 1
      Iv:                          webthunder - 1
193   xunlei-kankan                      Mv: 1
      Iv:                                http - 20
      Iv:                              xunlei - 1
194   ms-sql-m                           Mv: 1
195   ssh                                Mv: 1
196   hopopt                             Mv: 1
197   mikogo                             Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
198   ipv6-frag                          Mv: 1
199   ipv6-nonxt                         Mv: 1
200   ipv6-opts                          Mv: 1
201   ipv6-route                         Mv: 1
202   salesforce                         Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
203   twitter                            Mv: 1
```

```
      Iv:                                http - 20
      Iv:                                 ssl - 1
204   hulu                               Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
205   oscar-filetransfer                 Mv: 1
      Iv:                aol-messenger-audio - 1
206   logmein                            Mv: 1
      Iv:                                 ssl - 1
      Iv:                                http - 20
      Iv:                                spdy - 1
207   iscsi                              Mv: 1
208   yahoo-mail                         Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
      Iv:                                spdy - 1
209   linkedin                           Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
210   showmypc                           Mv: 1
      Iv:                                 ssl - 1
      Iv:                                http - 20
      Iv:                                rtmp - 1
      Iv:                                spdy - 1
211   gbridge                            Mv: 1
      Iv:                                http - 20
212   ms-lync                            Mv: 1
      Iv:                              stun-nat - 1
      Iv:                                  http - 20
      Iv:                                   ssl - 1
213   ms-lync-media                      Mv: 1
      Iv:                              stun-nat - 1
      Iv:                                   rtp - 8
      Iv:                                   ssl - 1
214   spdy                               Mv: 1
      Iv:                                   ssl - 1
215   facetime                           Mv: 1
      Iv:                              stun-nat - 1
      Iv:                                   sip - 5
      Iv:                                   ssl - 1
216   yahoo-accounts                     Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
217   pptv                               Mv: 1
      Iv:                                http - 20
218   net-assistant                      Mv: 1
219   apple-remote-desktop               Mv: 1
      Iv:                                 vnc - 1
220   lotus-notes                        Mv: 1
221   webex-media                        Mv: 1
      Iv:                                http - 20
222   webex-app-sharing                  Mv: 1
      Iv:                                http - 20
223   notes                              Mv: 1
224   qqlive                             Mv: 1
      Iv:                                http - 20
225   bittorrent-networking              Mv: 1
      Iv:                            bittorrent - 5
      Iv:                                http - 20
      Iv:                                 dht - 1
226   shoutcast                          Mv: 1
      Iv:                                http - 20
227   dameware-mrc                       Mv: 1
228   iana                               Mv: 1
```

```
229  custom-protocols                Mv: 1
230  attribute                       Mv: 1


{<No.>}<PDLM name> Mv: <PDLM Version>, {Nv: <NBAR Software Version>; <File name>}
            {Iv: <PDLM Interdependency Name>   - <PDLM Interdependency Version>}


------------------ show ip nbar protocol-pack active ------------------



Active Protocol Pack:

Name:                           Advanced Protocol Pack
Version:                        4.10001
Publisher:                      Cisco Systems Inc.
NBAR Engine Version:            16
State:                          Active


------------------ show ip nbar resources flow ------------------


------------------ show ip nbar attribute-map ------------------


% NBAR Error: No attribute-map configured


------------------ show ip nbar parameter extraction       activated ------------------



 Protocol        Parameter            ID
 --------        ---------            --

------------------ show ip nbar parameter subclassification        activated
------------------


 Protocol        Parameter          Parameter value        ID
 --------        ---------          ---------------        --

------------------ show ip nbar protocol-discovery ------------------


 Ethernet1/1

 Last clearing of "show ip nbar protocol-discovery" counters 00:28:02

                            Input                    Output
                            -----                    ------
   Protocol                 Packet Count             Packet Count
                            Byte Count               Byte Count
                            5min Bit Rate (bps)      5min Bit Rate (bps)
                            5min Max Bit Rate (bps)  5min Max Bit Rate (bps)
```

```
  ------------------------ ------------------------ ------------------------
  Total                    0                        0
                           0                        0
                           0                        0
                           0                        0

Tunnel21

Last clearing of "show ip nbar protocol-discovery" counters 00:23:09


                           Input                    Output
                           -----                    ------
  Protocol                 Packet Count             Packet Count
                           Byte Count               Byte Count
                           5min Bit Rate (bps)      5min Bit Rate (bps)
                           5min Max Bit Rate (bps)  5min Max Bit Rate (bps)
  ------------------------ ------------------------ ------------------------
  Total                    0                        0
                           0                        0
                           0                        0
                           0                        0

------------------ show policy-map interface ------------------
```

show tech-support rsvp

リソース予約プロトコル（RSVP）に関連するすべての情報のレポートを生成するには、特権 EXEC モードで **showtech-supportrsvp** コマンドを使用します。

show tech-support rsvp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
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。

使用上のガイドライン

オペレーティング システムの通常の使用に、このコマンドは不要です。このコマンドは、RSVP に関する問題についてテクニカル サポート担当者に問い合わせるときに便利です。**showtech-supportrsvp** コマンドは、テクニカル サポート担当者が問題を解決するのに役立つ一連のレポートを生成します。

showtech-support コマンドに当てはまる問題点や注意点は、このコマンドにも当てはまります。たとえば、イネーブル パスワード（設定した場合）は、**showrunning-config** コマンドの出力に表示されません。

例

showtech-supportrsvp コマンドは、次のコマンドを発行するのに相当します。

- **showiprsvpinstalled**
- **showiprsvpinterface**
- **showiprsvpneighbor**
- **showiprsvppolicycops**
- **showiprsvpreservation**
- **showiprsvpsender**
- **showrunning-config**
- **showversion**

詳細については、個別のコマンドの表示および説明で具体的な例を参照してください。

show traffic-shape

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**showtraffic-shape** コマンドは非表示です。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンドシーケンス）を使用する必要があります。代替コマンドのリストなど詳細については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**showtraffic-shape** コマンドは、モジュラ QoS CLI（MQC）コマンド（または MQC コマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

現在のトラフィック シェーピング設定を表示するには、EXEC モードで **showtraffic-shape** コマンドを使用します。

show traffic-shape [*interface-type interface-number*]

構文の説明

interface-type	（任意）インターフェイスのタイプ。インターフェイスを指定しないと、設定されたすべてのインターフェイスのトラフィック シェーピングの詳細が表示されます。
interface-number	（任意）インターフェイスの番号。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
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。

リリース	変更箇所
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。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQCコマンド（またはMQCコマンドのシーケンス）に置き換えられました。

使用上のガイドライン

traffic-shaperate、**traffic-shapegroup**、または**frame-relaytraffic-shaping** コマンドを使用してトラフィック シェーピング情報を表示するには、まずトラフィック シェーピングを有効にしておく必要があります。

例

次は、**showtraffic-shape** コマンドの出力例です。

```
Router# show traffic-shape
Interface   Fa0/0
       Access Target    Byte   Sustain   Excess    Interval  Increment Adapt
VC     List   Rate      Limit  bits/int  bits/int  (ms)      (bytes)   Active
-             1000000   6250   25000     25000     25        3125      -
```

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 *258 : show traffic-shape* 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タイプと番号
VC	仮想回線。 （注） インターフェイス レベルではなくVCレベルでトラフィック シェーピングを設定すると、このフィールドに数値が表示されます。
Access List	アクセス リストの番号（設定されている場合）。
Target Rate	トラフィックがシェーピングされるレート（1秒あたりのビット数）。
Byte Limit	内部間隔単位で送信される最大バイト数。

フィールド	説明
Sustain bits/int	間隔あたりの設定済み持続ビット。
Excess bits/int	最初の間隔における設定済み超過ビット。
Interval (ms)	内部で使用されている間隔（ミリ秒単位）。これは、短い間隔を設定した方がトラフィック フローの安定度が増すとルータが判断した場合には、設定情報レートで除算された認定バーストよりも小さくなる場合があります。
Increment (bytes)	内部間隔単位で持続されるバイトの数。
Adapt Active	フレーム リレーに逆方向明示的輻輳通知（BECN）アダプテーションが設定されている場合には、「BECN」が含まれます。

関連コマンド

Command	Description
frame-relaycir	フレーム リレー仮想回線の着信または発信の設定情報レート（CIR）を指定します。
frame-relaytraffic-rate	仮想回線（VC）のすべてのトラフィック シェーピング特性を単一のコマンドに設定します。
frame-relaytraffic-shaping	フレーム リレー インターフェイス上のすべての PVC および SVC に対してトラフィック シェーピングと VC 単位キューイングの両方を有効にします。
showtraffic-shapequeue	インターフェイス レベルまたは DLCI レベルで、トラフィック シェーピングによってキューに入れられた要素に関する情報を表示します。
showtraffic-shapestatisitcs	現在のトラフィック シェーピング統計情報を表示します。
traffic-shapeadaptive	BECN 信号の受信時に使用可能な帯域幅を推定するように、フレーム リレー サブインターフェイスを設定します。
traffic-shapefecn-adap	FECN ビット（BECN ビットを設定した TEST RESPONSE メッセージで設定）が設定されたメッセージに返信します。
traffic-shapegroup	インターフェイス上でアウトバウンド トラフィック専用のアクセス リストに基づくトラフィック シェーピングをイネーブルにします。
traffic-shaperate	インターフェイスの発信トラフィックにトラフィック シェーピングを有効にします。

show traffic-shape queue

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**showtraffic-shapequeue** コマンドは非表示です。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンド シーケンス）を使用する必要があります。代替コマンドのリストなど詳細については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**showtraffic-shapequeue** コマンドは、モジュラ QoS CLI（MQC）コマンド（または MQC コマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

インターフェイス レベルまたはデータリンク接続識別子（DLCI）レベルでトラフィック シェーピングによってキューイングされた要素に関する情報を表示するには、特権 EXEC モードで **showtraffic-shapequeue** コマンドを使用します。

show traffic-shape queue [*interface-number* [**dlci** *dlci-number*]]

構文の説明

interface-number	（任意）インターフェイスの番号。
dlci	（任意）キューイングされた要素に関する情報を表示する特定の DLCI。
dlci-number	（任意）DLCI の番号。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
12.0(3)XG	このコマンドが、Cisco IOS Release 12.0(3)XG に組み込まれました。*dlci* 引数が追加されました。

リリース	変更箇所
12.0(4)T	このコマンドは、Cisco IOS Release 12.0(4)T に統合されました。*dlci* 引数が追加されました。
12.0(5)T	このコマンドは、**frame-relayvoicebandwidth** コマンドの **queue** キーワードを使用して作成される特別な音声キューに関する情報を含めるように変更されました。
12.2(28)SB	このコマンドは、フレーム リレー（FR）インターフェイスまたは相手先固定接続（PVC）で階層型キューイング フレームワーク（HQF）をサポートするように変更されました。
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。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

使用上のガイドライン

このコマンドにパラメータを指定しないと、キューイングされた要素が含まれているすべてのインターフェイスおよびDLCIの情報が出力に表示されます。特定のインターフェイスおよびDLCIを指定すると、そのDLCIについてのみ、キューイングされた要素の情報が表示されます。

HQF でこのコマンドを使用した場合、出力は表示されません。

例

次に、DLCI 16 に関連付けられたマップ クラスに重み付け均等化キューイングが設定されている場合の **showtraffic-shapequeue** コマンドの出力例を示します。

```
Router# show traffic-shape queue Serial1/1 dlci 16
Traffic queued in shaping queue on Serial1.1 dlci 16
  Queueing strategy: weighted fair
  Queueing Stats: 1/600/64/0 (size/max total/threshold/drops)
     Conversations  0/16 (active/max total)
     Reserved Conversations 0/2 (active/allocated)
  (depth/weight/discards) 1/4096/0
  Conversation 5, linktype: ip, length: 608
```

```
source: 172.21.59.21, destination: 255.255.255.255, id: 0x0006, ttl: 255,
  TOS: 0 prot: 17, source port 68, destination port 67
```

次に、DLCI 16 に関連付けられたマップ クラスにプライオリティ キューイングが設定されている場合の **showtraffic-shapequeue** コマンドの出力例を示します。

```
Router# show traffic-shape queue Serial1/1 dlci 16
Traffic queued in shaping queue on Serial1.1 dlci 16
  Queueing strategy: priority-group 4
  Queueing Stats: low/1/80/0 (queue/size/max total/drops)
Packet 1, linktype: cdp, length: 334, flags: 0x10000008
```

次に、DLCI 16 に関連付けられたマップ クラスに先着順キューイングが設定されている場合の **showtraffic-shapequeue** コマンドの出力例を示します。

```
Router# show traffic-shape queue Serial1/1 dlci 16
Traffic queued in shaping queue on Serial1.1 dlci 16
  Queueing strategy: fcfs
  Queueing Stats: 1/60/0 (size/max total/drops)
Packet 1, linktype: cdp, length: 334, flags: 0x10000008
```

次に、**frame-relayvoicebandwidth** コマンドを入力すると自動的に作成される音声トラフィック用の特別なキューの統計情報を表示する **showtraffic-shapequeue** コマンドの出力例を示します。

```
Router# show traffic-shape queue Serial1/1 dlci 45

 Voice queue attached to traffic shaping queue on Serial1 dlci 45
 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    Voice Queueing Stats: 0/100/0 (size/max/dropped)
    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
 Traffic queued in shaping queue on Serial1 dlci 45
   Queueing strategy: weighted fair
   Queueing Stats: 0/600/64/0 (size/max total/threshold/drops)
      Conversations  0/16 (active/max total)
      Reserved Conversations 0/2 (active/allocated)
```

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 *259 : show traffic-shape queue* フィールドの説明

フィールド	説明
Queueing strategy	フレーム リレー トラフィック シェーピング（FRTS）が設定されている場合、キューイング タイプは、この DLCI のフレーム リレー マップ クラスに何を設定するかによって、重み付け均等化、カスタム キュー、プライオリティ グループ、fcfs（先着順）のいずれかにすることができます。FRTS の場合、デフォルトは fcfs です。汎用トラフィック シェーピングが設定されている場合、使用できるキューイング タイプは重み付け均等化キューイング（WFQ）だけです。

フィールド	説明
Queueing Stats	設定されたキューイング戦略の統計情報。具体的な情報は次のとおりです。 • [サイズ（size）]：キューの現在のサイズ。 • [最大合計値（max total）]：すべてのキューにキューイングできるあらゆるタイプのパケットの最大数。 • [しきい値（threshold）]：WFQ の場合、キュー内のパケット数がこの値を超えると、高帯域幅メッセージ交換の新規パケットがドロップされるようになります。 • [ドロップ（drops）]：この間隔中に破棄されたパケットの数。
Conversations active	現在アクティブなメッセージ交換の番号。
Conversations max total	同時メッセージ交換の最大許可数。
Reserved Conversations active	音声用に予約されている現在アクティブなメッセージ交換の番号。
Reserved Conversations allocated	予約済みメッセージ交換の最大設定数。
depth	現在キューイングされているパケットの数。
weight	パケットの分類および優先順位付けに使用された数値。
discards	キューから破棄されたパケットの数。
Packet	キューイングされたパケットの数。
linktype	キューイングされたパケットのプロトコル タイプ。(cdp = Cisco Discovery Protocol)
length	キューイングされたパケット内のバイトの数。
Flags	キューイングされたパケット内のフラグ文字の数。
source	発信元の IP アドレス。
destination	宛先の IP アドレス。
id	Packet ID.
ttl	パケット存続時間（TTL）カウント。
TOS	IP タイプ オブ サービス。

フィールド	説明
prot	レイヤ 4 プロトコル番号.プロトコル番号のリストについては、RFC 943 を参照してください。（17 = User Datagram Protocol（UDP））
source port	送信元ポートのポート番号。
destination port	宛先ポートのポート番号。

関連コマンド

Command	Description
showframe-relayfragment	フレーム リレー フラグメンテーションの詳細を表示します。
showframe-relaypvc	フレームリレー インターフェイス対応 PVC に関する統計情報を表示します。
showframe-relayvofr	VoFR DLCI で使用中の FRF.11 サブチャネルに関する詳細を表示します。
showtraffic-shape	現在のトラフィック シェーピング設定を表示します。
showtraffic-shapestatistics	現在のトラフィック シェーピング統計情報を表示します。

show traffic-shape statistics

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**showtraffic-shapestatistics** コマンドは非表示です。このコマンドはCisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンドシーケンス）を使用する必要があります。代替コマンドのリストなど詳細については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**showtraffic-shapestatistics** コマンドは、モジュラ QoS CLI（MQC）コマンド（またはMQCコマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

現在のトラフィック シェーピング統計情報を表示するには、EXEC モードで **showtraffic-shapestatistics** コマンドを使用します。

show traffic-shape statistics [*interface-type interface-number*]

構文の説明

interface-type	（任意）インターフェイスのタイプ。インターフェイスを指定しないと、設定されたすべてのインターフェイスのトラフィック シェーピング統計情報が表示されます。
interface-number	（任意）インターフェイスの番号。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
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。

リリース	変更箇所
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。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQCコマンド（またはMQCコマンドのシーケンス）に置き換えられました。

使用上のガイドライン

traffic-shaperate、**traffic-shapegroup**、または**frame-relaytraffic-shaping** コマンドを使用してトラフィック シェーピング情報を表示するには、まずトラフィック シェーピングを有効にしておく必要があります。

例

次に、**showtraffic-shapestatistics** コマンドの出力例を示します。

```
Router# show traffic-shape statistics
          Access Queue     Packets   Bytes     Packets   Bytes     Shaping
I/F       List   Depth                        Delayed   Delayed   Active
Et0       101    0         2         180       0         0         no
Et1              0         0         0         0         0         no
```

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 *260 : show traffic-shape statistics* フィールドの説明

フィールド	説明
I/F	インターフェイス。
Access List	アクセス リストの番号。
Queue Depth	キュー内のメッセージ数。
Packets	インターフェイスを介して送信されたパケットの数。
Bytes	インターフェイスを介して送信されたバイトの数。
Packets Delayed	インターフェイスを介して送信されたパケットのうち、トラフィック シェーピング キュー内で遅延したパケットの数。

フィールド	説明
Bytes Delayed	インターフェイスを介して送信されたバイトのうち、トラフィック シェーピング キュー内で遅延したバイトの数。
Shaping Active	タイマーがトラフィック シェーピングの発生を示す場合には「yes」、トラフィック シェーピングの発生なしを示す場合には「no」が含まれます。

関連コマンド

Command	Description
frame-relaytraffic-shaping	フレーム リレー インターフェイス上のすべての PVC および SVC に対してトラフィック シェーピングと VC 単位キューイングの両方を有効にします。
showinterfaces	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。
showiprsvpneighbor	RSVP 関連のインターフェイス情報を表示します。
traffic-shapeadaptive	BECN 信号の受信時に使用可能な帯域幅を推定するように、フレーム リレー サブインターフェイスを設定します。
traffic-shapegroup	インターフェイス上でアウトバウンド トラフィック専用のアクセス リストに基づくトラフィック シェーピングをイネーブルにします。
traffic-shaperate	インターフェイスの発信トラフィックにトラフィック シェーピングを有効にします。

show vrf

定義済みのバーチャル 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）インスタンスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showvrf** コマンドを使用します。

show vrf [{**ipv4**|**ipv6**}] [{**interface**|**brief**|**detail**|**id**|**select**|**lock**}] [*vrf-name*]

構文の説明

ipv4	（任意）IPv4 アドレス ファミリタイプの VRF インスタンスを表示します。
ipv6	（任意）IPv6 アドレス ファミリタイプの VRF インスタンスを表示します。
interface	（任意）指定した VRF インスタンスに関連付けられたインターフェイスを表示します。
brief	（任意）指定した VRF インスタンスに関する要約情報を表示します。
detail	（任意）指定した VRF インスタンスに関する詳細情報を表示します。
id	（任意）指定した VRF インスタンスの VPN ID 情報を表示します。
select	（任意）指定した VRF インスタンスの選択情報を表示します。
lock	（任意）指定した VRF インスタンスの VPN ロック情報を表示します。
vrf-name	（任意）VRF に割り当てられた名前。

コマンド デフォルト

引数やキーワードを指定しないと、設定されたすべての VRF に関する簡潔な情報が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SB に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
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。

リリース	変更箇所
12.2(33)SRE	このコマンドが変更されました。プレフィックス独立コンバージェンス機能または Best External 機能を介してバックアップ パスが作成された場合、**showvrfdetail** コマンドの出力には次の行が表示されます。 追加のパスが有効になっているプレフィックス保護（Prefix protection with additional path enabled）
15.0(1)S	このコマンドが、Cisco IOS Release 15.0(1)S に統合されました。

使用上のガイドライン

指定した VRF インスタンスまたはすべての VRF インスタンスに関する情報を表示するには、**showvrf** コマンドを使用します。引数やキーワードを指定しないと、すべての VRF インスタンスに関する情報が表示されます。

例

showvrf コマンドの次の出力例は、設定されたすべての VRF インスタンスに関する要約情報を表示しています。

```
Router# show vrf
  Name                              Default RD          Protocols   Interfaces
  N1                                100:0               ipv4,ipv6
  V1                                1:1                 ipv4        Lo1
  V2                                2:2                 ipv4,ipv6   Et0/1.1
                                                                    Et0/1.2
                                                                    Et0/1.3
  V3                                3:3                 ipv4        Lo3
                                                                    Et0/1.4
```

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 *261 : show vrf* フィールドの説明

フィールド	説明
Name	VRF インスタンスの名前。
Default RD	指定した VRF インスタンスのデフォルトのルート識別子（RD）。
Protocols	指定した VRF インスタンスのアドレス ファミリ プロトコル タイプ。
Interfaces	VRF インスタンスに関連付けられたネットワーク インターフェイス。

detail キーワードを指定した **showvrf** コマンドの次の出力例は、cisco という名前の VRF の情報を表示しています。

```
Router# show vrf detail
VRF cisco1; default RD 100:1; default VPNID <not set>
  Interfaces:
    Ethernet0/0                 Loopback10
Address family ipv4 (Table ID = 0x1):
```

```
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
Address family ipv6 (Table ID = 0xE000001):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
```

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 *262 : show vrf detail* フィールドの説明

フィールド	説明
default RD 100:1	この VRF に付与された RD。
Interfaces:	VRF がアタッチされるインターフェイス。
Export VPN route-target communities RT:100:1	エクスポートするルート ターゲット VPN 拡張コミュニティ。
Import VPN route-target communities RT:100:1	インポートするルートターゲットVPN拡張コミュニティ。

次の例は、バックアップ パスがプレフィックス独立コンバージェンス機能または Best External 機能を介して作成された場合の **showvrfdetail** コマンドの出力を示しています。**showvrfdetail** コマンドの出力には、次の行が表示されます。

Prefix protection with additional path enabled

```
Router# show vrf detail
VRF vpn1 (VRF Id = 1); default RD 1:1; default VPNID <not set>
  Interfaces:
    Et1/1
Address family ipv4 (Table ID = 1 (0x1)):
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix

Prefix protection with additional path enabled
Address family ipv6 not active.
```

showvrflock コマンドの次の出力例では、VPN ロック情報を表示しています。

```
Router# show vrf lock
VRF Name: Mgmt-intf; VRF id = 4085 (0xFF5)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :108
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
VRF Name: vpn1; VRF id = 1 (0x1)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :100
         Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
```

関連コマンド

コマンド	説明
vrfdefinition	VRF ルーティング テーブル インスタンスを設定し、VRF コンフィギュレーション モードを開始します。
vrfforwarding	VRF インスタンス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。

show wrr-queue

Weighted Round Robin（WRR; 加重ラウンドロビン）スケジューリングごとに提供されるキュー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 **showwrr-queue** コマンドを使用します。

show wrr-queue {**bandwidth**|**cos-map**}

構文の説明

bandwidth	帯域幅情報を表示します。
cos-map	サービス クラス（CoS）マップ情報を表示します。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(24)T	このコマンドは、Cisco IOS Release 12.4(24)T よりも前のリリースに導入されました。

使用上のガイドライン

WRR 単位で提供するようにスケジュールされているキュー情報を表示するには、このコマンドを使用します。WRR はスケジュールのタイプで、ハイ プライオリティ トラフィックの時間帯にロープライオリティ キューが完全に無視されるのを防ぐことができます。WRR スケジューラは、代わりに各キューから一部のパケットを送信します。スケジューラが送信するパケットの数は、キューの相対的な重要度に対応します。

例

次に、**showwrr-queue** コマンドの出力例を示します。フィールドの説明は自明です。

```
Router# show wrr-queue bandwidth
wrr-queue bandwidth for Etherswitch HWIC is:
WRR Queue  :   1   2   3   4
Bandwidth  :   1   2   4   8


Router# show wrr-queue cos-map
wrr-queue cos_map for Etherswitch HWIC is:
CoS Value      :  0  1  2  3  4  5  6  7
Priority Queue :  1  1  2  2  3  3  4  4
```

subscriber accounting accuracy

アカウンティング停止レコード内の入力/出力パケット/バイト統計情報を 1 秒以内の精度になるようにするには、特権 EXEC モードで **subscriberaccountingaccuracy** コマンドを使用します。この統計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。

subscriber accounting accuracy *value*
no subscriber accounting accuracy

構文の説明

value	加入者アカウンティング精度機能の値（ミリ秒単位）。指定できる範囲は 1,000 ～ 10,000 です。

コマンド デフォルト

デフォルト値は、1000 ミリ秒です。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS Release XE 3.2S	このコマンドが、ASR 1000 シリーズ ルータに追加されました。

例

このセクションでは、**subscriberaccountingaccuracy** コマンドをデフォルト値に設定する例を示します。

```
Router# subscriber accounting accuracy 1000
```

svc-bundle

相手先選択接続（SVC）バンドルのメンバーを作成または変更するには、SVC バンドル コンフィギュレーション モードで **svc-bundle** コマンドを使用します。バンドルから SVC バンドル 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。

svc-bundle *svc-handle*
no svc-bundle *svc-handle*

構文の説明

svc-handle	ルータにおける SVC の一意の名前。

コマンド デフォルト

SVC には SVC バンドルのメンバーはありません。

コマンド モード

SVC バンドル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(4)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

このコマンドを使用すると、システムは SVC バンドル メンバー コンフィギュレーション モードになります。このモードでは、メンバーの特性を設定できます。優先順位、可変ビット レート（VBR）トラフィック シェーピング、未指定ビット レート（UBR）トラフィック シェーピング、UBR+ トラフィック シェーピング、アイドル タイムアウト、バンピング条件などです。

例

次の例では、SVC バンドルのメンバーを「five」という名前で作成しています。

```
svc-bundle five
```

table-map（値マッピング）

パケットマーキング値間でマッピングおよび変換を行うためのマッピングテーブルを作成および設定するには、グローバルコンフィギュレーションモードで **table-map**（値マッピング）コマンドを使用します。このテーブル マップの使用を無効にするには、このコマンドの **no** 形式を使用します。

table-map *table-map-name* **map from** *from-value* **to** *to-value* [**default** *default-value-or-action*]
no table-map *table-map-name* **map from** *from-value* **to** *to-value* [**default** *default-value-or-action*]

構文の説明

table-map-name	作成するテーブル マップの名前。この名前には最大 64 文字までの英数字を指定できます。
mapfrom	[マップ元（map from）] の値が使用されることを示します。
from-value	パケットマーキング カテゴリの [マップ元（map from）] の値。値の範囲は、マップおよび変換の元となるパケットマーキングカテゴリによって異なります。詳細については、次の「使用上のガイドライン」を参照してください。
to	[マップ先（map to）] の値が使用されることを示します。
to-value	パケットマーキング カテゴリの [宛先の値（to-value）] の値。値の範囲は、マップおよび変換先のパケットマーキングカテゴリによって異なります。詳細については、次の「使用上のガイドライン」を参照してください。
default	（任意）デフォルトの値またはアクションが使用されることを示します。
default-value-or-action	（任意）「to-from」の関係が明示的に設定されていない場合に使用されるデフォルトの値またはアクション。デフォルトのアクションは「無視」および「コピー」です。どちらのアクションも指定していない場合は、「コピー」が使用されます。

コマンド デフォルト

default キーワードと *default-value-or-action* 引数に、値が明示的に指定されなかった場合に使用するデフォルト値（アクション）を設定します。

テーブル マップは設定したものの、**default** キーワードの *default-value-or-action* 引数を指定しなかった場合、デフォルトのアクションは「コピー」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	変更箇所
12.2(13)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

このコマンドでは、マッピング テーブルを作成できます。マッピング テーブル（変換チャートのタイプ）は、パケットマーキング タイプまたはカテゴリ間の「to-from」の関係を確立するために使用します。たとえば、マッピングテーブルを使用すると、次のパケットマーキング カテゴリ間の「to-from」の関係を確立できます。

- サービス クラス（CoS）
- Precedence
- Diffserv コード ポイント（DSCP）
- Quality of Service（QoS）グループ
- マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）インポジション
- MPLS EXP topmost

テーブル マップを設定するときは、変換で使用されるパケット マーキング値を指定する必要があります。入力できる値は、パケットマーキング カテゴリによって異なります。

次の表は、パケットマーキング カテゴリごとに入力できる有効な値の範囲を示しています。

表 *263 :* 有効な値の範囲

パケットマーキング カテゴリ	値の範囲
CoS	0 ～ 7 の範囲における特定の IEEE 802.1Q 番号。
Precedence	番号の範囲は 0 ～ 7 です。
DSCP	番号の範囲は 0 ～ 63 です。
QoS グループ	番号の範囲は 0 ～ 99 です。
MPLS EXP インポジション	番号の範囲は 0 ～ 7 です。
MPLS EXP topmost	番号の範囲は 0 ～ 7 です。

例

次の例では、**table-map**（値マッピング）コマンドは「map1」というテーブル マップを作成するように設定されています。「map1」では、2 つの「to-from」の関係が確立され、デフォルト値が定義されています。さらに「to-from」のマッピングを確立するためのフィールドが、テーブルマップの設定先となるポリシーマップによって定義されます。（ポリシーマップの設定は、テーブルマップの作成後に続く次の論理的な手順です。）

たとえば、値 0 の優先順位や DSCP を値 0 の CoS にマップしたり、その逆方向にマップしたりでき、これはテーブル マップをどのように設定するかによって異なります。「to-from」の関係に明示的に定義されていない値は、デフォルト値に設定されます。

```
Router(config)# table-map map1
Router(config-tablemap)# map from 0 to 0
Router(config-tablemap)# map from 2 to 1
Router(config-tablemap)# default 3
Router(config-tablemap)# end
```

関連コマンド

コマンド	説明
policy-map	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapclass	指定されたポリシーマップの指定されたクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。
showtable-map	指定されたテーブル マップまたはすべてのテーブル マップの設定を表示します。

tcp

IP ヘッダー圧縮（IPHC）プロファイル内で Transmission Control Protocol（TCP）ヘッダー圧縮を有効にするには、IPHC プロファイル コンフィギュレーション モードで **tcp** コマンドを使用します。TCP ヘッダー圧縮を無効にするには、このコマンドの **no** 形式を使用します。

tcp
no tcp

構文の説明

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

TCP ヘッダー圧縮は有効です。

コマンド モード

IPHC 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	変更箇所
12.4(9)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

IPHC プロファイルでの使用目的

tcp コマンドは、IPHC プロファイルの一部として使用することを目的としています。IPHC プロファイルは、ネットワークでのヘッダー圧縮を有効および設定するために使用されます。IPHC プロファイルを使用してヘッダー圧縮を設定する詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、リリース 12.4T の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

例

次は、profile1 という IPHC プロファイルの例を示しています。この例では、TCP ヘッダー圧縮が有効になっています。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile1 van-jacobson
Router(config-iphcp)# tcp
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
iphc-profile	IPHCプロファイルを作成します。

tcp contexts

Transmission Control Protocol（TCP）ヘッダー圧縮に使用できるコンテキストの数を設定するには、IPHCプロファイルコンフィギュレーションモードで**tcpcontexts**コマンドを使用します。以前に設定したコンテキストの数を削除するには、このコマンドの **no** 形式を使用します。

tcp contexts {**absolute** *number-of-contexts*|**kbps-per-context** *kbps*}
no tcp contexts

構文の説明

absolute	圧縮した TCP コンテキストの最大数が固定（絶対）数に基づくことを示します。
number-of-contexts	TCP コンテキストの数。範囲は 1 ～ 256 です。
kbps-per-context	圧縮した TCP コンテキストの最大数が使用可能な帯域幅に基づくことを示します。
kbps	各コンテキストに許可する kbps 数です。範囲は 1 ～ 100 です。

コマンド デフォルト

tcpcontexts コマンドは、帯域幅に基づいてコンテキストの数を計算し、コンテキストごとに 4 kbps を割り当てます。

コマンド モード

IPHC 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	変更箇所
12.4(9)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

TCPヘッダー圧縮に使用可能なコンテキストの数を設定するには、**tcpcontexts**コマンドを使用します。コンテキストとは、コンプレッサがヘッダーの圧縮に使用し、デコンプレッサがヘッダーの圧縮解除に使用する状態です。コンテキストは、送信された最終ヘッダーの非圧縮バージョンであり、パケットの圧縮と圧縮解除に使用する情報が含まれます。

IPHC プロファイルでの使用目的

tcpcontexts コマンドは、IPHC プロファイルの一部として使用することを目的としています。IPHC プロファイルは、ネットワークでのヘッダー圧縮を有効および設定するために使用されます。IPHC プロファイルを使用してヘッダー圧縮を設定する詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、リリース 12.4T の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

絶対数としてのコンテキストの数の設定

tcpcontexts コマンドにより、コンテキストの数を絶対数として設定できます。コンテキストの数を絶対数として設定するには、1 ～ 256 の数を入力します。

帯域幅に基づくコンテキストの数の計算

tcpcontexts コマンドにより、IPHC プロファイルが適用されるネットワーク リンクで使用できる帯域幅に基づいて、コンテキストの数を計算できます。

使用可能な帯域幅に基づいてコンテキストの数を計算するには、**kbps-per-context** キーワードを入力し、その後に *kbps* 引数の値を続けます。コマンドは、指定された kbps で使用可能な帯域幅を分割します。たとえば、ネットワーク リンクの帯域幅が 2000 kbps で、*kbps* 引数に 10 を入力すると、このコマンドは 200 のコンテキストを算出します。

例

profile2 という IPHC プロファイルの例を、次に示します。この例では、TCP コンテキストの数を 75 に設定しています。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 van-jacobson
Router(config-iphcp)# tcp contexts absolute 75
Router(config-iphcp)# end
```

関連コマンド

コマンド	説明
iphc-profile	IPHCプロファイルを作成します。

traffic-shape adaptive

逆方向明示的輻輳通知（BECN）信号の受信時に使用可能な帯域幅を推定するようにフレームリレーサブインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **traffic-shapeadaptive** インターフェイス コンフィギュレーション コマンドを使用します。BECN 信号を無視し、使用可能な帯域幅を推定しないようにするには、このコマンドの **no** 形式を使用します。

traffic-shape adaptive *bit-Rate*
no traffic-shape adaptive

構文の説明

bit-Rate	トラフィックがシェーピングされる最低ビット レート（1 秒あたりのビット数）。デフォルトの *bitrate* 値は 0 です。

コマンド デフォルト

BECN 信号の受信時に、帯域幅は推定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
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。

使用上のガイドライン

このコマンドは、BECN 信号の受信時にトラフィックがシェーピングされる境界を指定します。**traffic-shapeadaptive** コマンドを使用するには、**traffic-shaperate** コマンドまたは **traffic-shapegroup** コマンドを使用してインターフェイスでトラフィック シェーピングを有効にしておく必要があります。

traffic-shaperate コマンドに指定するビット レートはインターフェイスでの BECN 信号の受信時にトラフィックがシェーピングされる上限値で、**traffic-shapeadaptive** コマンドに指定するビット レートはその下限値です。実際にシェーピングされるレートは、この 2 つのビット レートの範囲内になります。

トラフィックが主に一方向に流れているときでも、接続で適応型トラフィック シェーピングを実現するため、このコマンドおよび **traffic-shapefecn-adapt** コマンドを接続の両端に設定する必要があります。**traffic-shapefecn-adapt** コマンドは、順方向明示的輻輳通知（FECN）信号を BECN 信号として反射するようにルータを設定します。

例

次の例では、上限を 128 kbps、下限を 64 kbps にして、シリアル インターフェイス 0.1 でトラフィック シェーピングを設定しています。この設定により、リンクは輻輳レベルに応じて 64 ～ 128 kbps で動作できます。

```
interface serial 0
 encapsulation-frame-relay
interface serial 0.1
 traffic-shape rate 128000
 traffic-shape adaptive 64000
 traffic-shape fecn-adapt
```

関連コマンド

Command	Description
showtraffic-shape	現在のトラフィック シェーピング設定を表示します。
showtraffic-shapestatistics	現在のトラフィック シェーピング統計情報を表示します。
traffic-shapefecn-adapt	FECN ビット（BECN ビットを設定した TEST RESPONSE メッセージで設定）が設定されたメッセージに返信します。
traffic-shapegroup	インターフェイス上でアウトバウンド トラフィック専用のアクセス リストに基づくトラフィック シェーピングをイネーブルにします。
traffic-shaperate	インターフェイスの発信トラフィックにトラフィック シェーピングを有効にします。

traffic-shape fecn-adapt

順方向明示的輻輳通知（FECN）ビットがあるメッセージ（BECN ビットが設定された TEST RESPONSE メッセージとともに送信される）に応答するには、インターフェイス コンフィギュレーション モードで **traffic-shapefecn-adapt** コマンドを使用します。逆方向明示的輻輳通知（BECN）シグナルの生成を停止するには、このコマンドの **no** 形式を使用します。

traffic-shape fecn-adapt
no traffic-shape fecn-adapt

構文の説明

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

トラフィック シェーピ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（config-if）

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
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。

使用上のガイドライン

インターフェイスでトラフィック シェーピングを有効にするには、**traffic-shaperate** コマンドまたは **traffic-shapegroup** コマンドを使用します。FECN は、トラフィック シェーピングが設定されている場合にのみ使用可能になります。

FECN ビットを BECN ビットとして反映するには、このコマンドを使用します。FECN ビットを BECN ビットとして反映すると、送信レートが速すぎて DTE では処理できないとの通知が送信側の DTE に送られます。BECN 信号の受信時に転送速度を調整するようにルータを設定するには、**traffic-shapeadaptive** コマンドを使用します。

トラフィックが主に一方向に流れているときでも、接続で適応型トラフィック シェーピングを実現するため、このコマンドおよび **traffic-shapeadaptive** コマンドを接続の両端に設定する必要があります。

例

次の例では、上限を 128 kbps、下限を 64 kbps にして、シリアル インターフェイス 0.1 でトラフィック シェーピングを設定しています。この設定により、リンクは輻輳レベルに応じて 64 ～ 128 kbps で動作できます。ルータは、FECN 信号を BECN 信号として反映します。

```
interface serial 0
```

```
 encapsulation-frame-relay
interface serial 0.1
 traffic-shape rate 128000
 traffic-shape adaptive 64000
 traffic-shape fecn-adapt
```

関連コマンド

Command	Description
showtraffic-shape	現在のトラフィック シェーピング設定を表示します。
showtraffic-shapestatistics	現在のトラフィック シェーピング統計情報を表示します。
traffic-shapeadaptive	BECN 信号の受信時に使用可能な帯域幅を推定するように、フレーム リレー サブインターフェイスを設定します。
traffic-shapegroup	インターフェイス上でアウトバウンドトラフィック専用のアクセスリストに基づくトラフィック シェーピングをイネーブルにします。
traffic-shaperate	インターフェイスの発信トラフィックにトラフィック シェーピングを有効にします。

traffic-shape group

インターフェイスで発信トラフィックの特定のアクセス リストに基づいてトラフィック シェーピ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**traffic-shapegroup** コマンドを使用します。アクセス リストのインターフェイスでトラフィック シェーピ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。

traffic-shape group *access-list bit-rate* [*burst-size* [*excess-burst-size*]]
no traffic-shape group *access-list*

構文の説明

access-list	インターフェイスでトラフィック シェーピングの適用対象となるパケットを制御するアクセス リストの番号。アクセス リスト番号の範囲は、1 ～ 2699 です。
bit-Rate	トラフィックがシェーピングされるビット レート（1秒あたりのビット数）。これは、サービス プロバイダーと契約したアクセス ビット レート、または維持するサービス レベルです。ビット レートの範囲は、8000 ～ 100000000 bps です。
burst-size	（任意）間隔あたりの送信持続ビット数。フレーム リレー インターフェイスでは、これはサービス プロバイダーと契約した認定バースト サイズです。有効なエントリの範囲は、0 ～ 100000000 です。
excess-burst-size	（任意）輻輳イベントの最初の間隔でバースト サイズを超過できる最大ビット数。フレーム リレー インターフェイスでは、これはサービス プロバイダーと契約した超過バースト サイズです。有効なエントリの範囲は、0 ～ 100000000 です。デフォルトは、*burst-size* 引数に等しくなります。

コマンド デフォルト

無効

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
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。

使用上のガイドライン

汎用トラフィック シェーピングは、ISDN およびダイヤルアップ インターフェイスではサポートされていません。また、非汎用ルーティング カプセル化トンネル インターフェイスでもサ

ポートされていません。トラフィック シェーピングは、フロースイッチングと一緒にはサポートされません。

トラフィック シェーピングは、キューを使用して、ネットワークの輻輳を招くサージを制限します。トラフィックが特定の接続で約束されたトラフィック エンベロープ内に収まるよう、データはバッファされ、制限された量だけネットワークに送信されます。

traffic-shapegroup コマンドでは、以前に定義した 1 つ以上のアクセス リストを指定して、インターフェイス上のトラフィックをシェーピングできます。インターフェイス上のアクセス リストごとに **traffic-shapegroup** コマンドを 1 つ指定する必要があります。

traffic-shapegroup コマンドは、標準と拡張の両方のアクセス リストをサポートしています。

トラフィック シェーピングは、あるネットワークでアクセス レートがさまざまに異なる場合や、サブレート サービスを提供している場合に使用します。サービス プロバイダーとの契約または維持するサービス レベルに従って値を設定できます。

間隔は、次のように計算されます。

- *burst-size* がゼロでない場合、間隔は *burst-size* を *bit-rate* で除算した値になります。
- *burst-size* がゼロの場合、間隔は *excess-burst-size* を *bit-rate* で除算した値になります。

トラフィック シェーピングは、ルータ上のすべてのメディア タイプおよびカプセル化タイプでサポートされています。フレーム リレー仮想回線でトラフィック シェーピングを実行するには、**frame-relaytraffic-shaping** コマンドを使用することもできます。フレーム リレー トラフィック シェーピングの詳細については、『*Cisco IOS Wide-Area Networking Configuration Guide*』の「Configuring Frame Relay」の章を参照してください。

traffic-shaperate コマンドを使用してトラフィック シェーピングをフレーム リレー ネットワークで実行する場合は、**traffic-shapeadaptive** コマンドを使用して、トラフィックをシェーピングする最小ビット レートを指定することもできます。

例

次の例では、アクセス リスト 101 に一致するトラフィックを特定のレートにシェーピングし、アクセス リスト 102 に一致するトラフィックをインターフェイス上の別のレートにシェーピングしています。

```
interface serial 1
 traffic-shape group 101 128000 16000 8000
 traffic-shape group 102 130000 10000 1000
```

関連コマンド

Command	Description
access-list(IPStandard)	標準 IP アクセス リストを定義します。
showtraffic-shape	現在のトラフィック シェーピング設定を表示します。
showtraffic-shapestatistics	現在のトラフィック シェーピング統計情報を表示します。
traffic-shapeadaptive	BECN 信号の受信時に使用可能な帯域幅を推定するように、フレーム リレー サブインターフェイスを設定します。

Command	Description
traffic-shapefecn-adapt	FECN ビット（BECN ビットを設定した TEST RESPONSE メッセージで設定）が設定されたメッセージに返信します。
traffic-shaperate	インターフェイスの発信トラフィックにトラフィック シェーピングを有効にします。

traffic-shape rate

インターフェイスで発信トラフィックのトラフィック シェーピ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 **traffic-shaperate** コマンドを使用します。インターフェイスでトラフィック シェーピ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。

traffic-shape rate *bit-Rate* [*burst-size* [*excess-burst-size*]] [*buffer-limit*]
no traffic-shape rate

構文の説明

bit-Rate	トラフィックがシェーピングされるビット レート（1秒あたりのビット数）。これは、サービス プロバイダーと契約したアクセス ビット レート、または維持するサービス レベルです。ビット レートの範囲は、8000 ～ 100000000 bps です。
burst-size	（任意）間隔あたりの送信持続ビット数。フレーム リレー インターフェイスでは、これはサービス プロバイダーと契約した認定バースト サイズです。有効なエントリの範囲は、0 ～ 100000000 です。
excess-burst-size	（任意）輻輳イベントの最初の間隔でバースト サイズを超過できる最大ビット数。フレーム リレー インターフェイスでは、これはサービス プロバイダーと契約した超過バースト サイズです。有効なエントリの範囲は、0～100000000 です。デフォルトは、*burst-size* 引数に等しくなります。
buffer-limit	（任意）最大バッファ制限（bps）。有効なエントリの範囲は、0 ～ 4096 です。

コマンド デフォルト

発信トラフィックに対するトラフィック シェーピングは有効になりません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。
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。
12.4(18e)	このコマンドは、同じインターフェイスにレガシー トラフィック シェーピングと MQC シェーピングを同時に設定できないように変更されました。

使用上のガイドライン

汎用トラフィック シェーピングは、ISDNおよびダイヤルアップ インターフェイスではサポートされていません。また、非汎用ルーティング カプセル化トンネル インターフェイスでもサポートされていません。トラフィック シェーピングは、フロー スイッチングと一緒にはサポートされません。

トラフィック シェーピングは、キューを使用して、ネットワークの輻輳を招くサージを制限します。トラフィックが特定の接続で約束されたトラフィック エンベロープ内に収まるよう、データはバッファされ、制限された量だけネットワークに送信されます。

トラフィック シェーピングは、あるネットワークでアクセス レートがさまざまに異なる場合や、サブレート サービスを提供している場合に使用します。サービス プロバイダーとの契約または維持するサービス レベルに従って値を設定できます。

間隔は、次のように計算されます。

- *burst-size* がゼロでない場合、間隔は *burst-size* を *bit-rate* で除算した値になります。
- *burst-size* がゼロの場合、間隔は *excess-burst-size* を *bit-rate* で除算した値になります。

トラフィック シェーピングは、ルータ上のすべてのメディア タイプおよびカプセル化タイプでサポートされています。フレーム リレー仮想回線でトラフィック シェーピングを実行するには、**frame-relaytraffic-shaping** コマンドを使用することもできます。フレーム リレー トラフィック シェーピングの詳細については、『*Cisco IOS Wide-Area Networking Configuration Guide*』の「Configuring Frame Relay」の章を参照してください。

traffic-shaperate コマンドを使用してトラフィック シェーピングをフレーム リレー ネットワークで実行する場合は、**traffic-shapeadaptive** コマンドを使用して、トラフィックをシェーピングする最小ビット レートを指定することもできます。

（注） Cisco IOS Release 12.4(18e) 以降は、トラフィック シェープ レートおよびMQC シェーピングを同時に同じインターフェイスに設定することはできません。サービス ポリシーを適用する前に、インターフェイスに設定されたトラフィック シェープ レートを削除する必要があります。たとえば、**traffic-shaperate** コマンドがすでに有効になっている場合に **service-policy** {**input** | **output**} *policy-map-name* コマンドを入力しようとすると、「サービスポリシーをアタッチする前に、インターフェイスに設定された traffic-shape rate を削除してください。（Remove traffic-shape rate configured on the interface before attaching the service-policy.）」というメッセージが表示されます。先に MQC シェーパーをアタッチしてから、同じインターフェイスに従来の **traffic-shaperate** コマンドを入力した場合、このコマンドは拒否され、エラー メッセージが表示されます。

例

次の例では、サービス プロバイダーが必要とする帯域幅を使用して、シリアル インターフェイス 0 でトラフィック シェーピングを有効にしています。

```
interface serial 0
 traffic-shape rate 128000 16000 8000
```

関連コマンド

Command	Description
showtraffic-shape	現在のトラフィック シェーピング設定を表示します。
showtraffic-shapestatistics	現在のトラフィック シェーピング統計情報を表示します。
traffic-shapeadaptive	BECN 信号の受信時に使用可能な帯域幅を推定するように、フレーム リレー サブインターフェイスを設定します。
traffic-shapefecn-adapt	FECN ビット（BECN ビットを設定した TEST RESPONSE メッセージで設定）が設定されたメッセージに返信します。
traffic-shapegroup	インターフェイス上でアウトバウンドトラフィック専用のアクセスリストに基づくトラフィック シェーピングをイネーブルにします。

trust

class ポリシーマップ コンフィギュレーション コマンドで分類されるトラフィックの信頼状態を定義するには、ポリシーマップ クラス コンフィギュレーション モードで **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。

trust [{**cos**|**dscp**|**precedence**}]
no trust [{**cos**|**dscp**|**precedence**}]

構文の説明

cos	（任意）パケットの Class of Service（CoS）値を使用して、入力パケットを分類します。タグのない IP パケットの場合、ポートのデフォルトの CoS 値が使用されます。
dscp	（任意）パケットの DiffServ コードポイント（DSCP）値（8 ビット サービスタイプ フィールドの上位 6 ビット）を使用して、入力パケットを分類します。パケットがタグ付きの場合、非 IP パケットにはパケットの CoS 値が使用されます。パケットがタグなしの場合、CoS の DSCP マッピングにデフォルト ポートの CoS 値が使用されます。
precedence	（任意）入力パケットの優先順位を分類します。

コマンド デフォルト

アクションは信頼されていません。

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（config-pmap-c）

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドが Catalyst 6500 シリーズに追加されました。
12.2(33)SRA	このコマンドが Catalyst 7600 シリーズに実装されました。

使用上のガイドライン

特定のトラフィックの Quality of Service（QoS）の信頼動作を他のトラフィックと区別するために、このコマンドを使用します。たとえば、ある DSCP 値を持った着信トラフィックが信頼されます。着信トラフィック内の DSCP 値と一致し、信頼するようにクラス マップを設定できます。

このコマンドで設定された信頼性の値は、**qostrust** インターフェイス コンフィギュレーション コマンドで設定された信頼性の値に優先します。

trustcos コマンドを指定した場合、QoS は受信した CoS 値、またはデフォルト ポートの CoS 値および CoS/DSCP マップを使用して、パケットの DSCP 値を生成します。

trustdscp コマンドを指定した場合、QoS は入力パケットから DSCP 値を使用します。タグ付きの非 IP パケットに対しては、QoS は受信した CoS 値を、タグなしの非 IP パケットに対して

は、デフォルト ポートの CoS 値を使用します。どちらの場合も、パケットの DSCP 値は CoS/DSCP マップから抽出されます。

例

次の例では、「class1」で分類されたトラフィックの着信DSCP値を信頼するために、ポート信頼状態を定義する方法を示します。

```
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# trust dscp
Router(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
Router#
```

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

関連コマンド

コマンド	説明
class	トラフィック ポリシーを作成または変更するクラスの名前を指定します。
police	トラフィック ポリシング機能を設定します。
policy-map	複数ポートに適用可能なポリシーマップを作成し、サービスポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
set	パケットに CoS、DSCP または IP プレシデンスを設定して、IP トラフィックをマークします。
showpolicy-map	ポリシー マップ情報を表示します。

tx-ring-limit

デジタル加入者線（DSL）WAN インターフェイス カード（WIC）またはインターフェイスの伝送リングで使用できるパケットの数を制限するには、ATM VC コンフィギュレーション モードで **tx-ring-limit** コマンドを使用します。DSL WIC またはインターフェイスの伝送リングで使用できるパケットの数を制限しないようにするには、このコマンドの **no** 形式を使用します。

tx-ring-limit *ring-limit*
no tx-ring-limit *ring-limit*

構文の説明

ring-limit	伝送リングに配置できるパケットの最大数を指定します。有効なエントリの範囲は 1 ～ 32767 です。デフォルト値は 60 です。Cisco 1700 シリーズ ルータの場合、使用できる値は 2 ～ 60 です。Cisco 2600 および 3600 シリーズ ルータの場合、使用できる値は 3 ～ 60 です。

コマンド デフォルト

ring-limit 引数のデフォルト値は 60 です。

コマンド モード

ATM VC 設定

コマンド履歴

リリース	変更箇所
12.0(7)XE1	このコマンドが導入されました。
12.0(9)S	このコマンドが Cisco IOS Release 12.0(9)XS に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.2(2)XK	非対称デジタル加入者線（ADSL）のサポートが追加され、Cisco 2600 および Cisco 3600 ルータで遅延が重視される ADSL トラフィック用に伝送（tx）リング設定 3 が追加されました。
12.2(4)XL	G.SHDSL のサポートが追加されました。
12.2(8)YN	Cisco 1720、Cisco 1750、Cisco 1751、Cisco 1760、Cisco 2610XM-2651XM、Cisco 3640、Cisco 3640A、および Cisco 3660 用に拡張 Quality of Service（QoS）機能が追加されました。
12.3(2)T	1721、2610-2651、Cisco 2610XM – Cisco 2651XM、Cisco 2691、Cisco 3620、Cisco、および Cisco 3660 のプラットフォームのサポートが追加されました。
12.3(3a)	Cisco 7200 シリーズ ルータで Packet over SONET（POS）インターフェイスのサポートが追加されました。
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。

リリース	変更箇所
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。

例

次の例では、ATM 相手先固定接続（PVC）サブインターフェイスで伝送リング制限を 3 パケットに設定しています。

```
Router(config)# interface atm1/0.1 point-to-point
Router(config-subif)#

pvc 2/200
Router(config-if-atm-vc)#

tx-ring-limit 3
```

関連コマンド

コマンド	説明
showatmvc	すべての ATM PVC およびトラフィック情報を表示します。

vbr-nrt

ATM 相手先固定チャネル（PVC）、PVC 範囲、相手先選択接続（SVC）、VC クラス、または VC バンドル メンバーの可変ビット レート非リアルタイム（VBR-NRT）Quality of Service（QoS）を設定し、出力ピーク セル レート（PCR）、出力平均セル レート（SCR）、および出力最大バースト セル サイズを指定するには、該当するコマンド モードで **vbr-nrt** コマンドを使用します。VBR-NRT 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。

vbr-nrt *output-pcr output-scr output-maxburstsize* [*input-pcr*] [*input-scr*] [*input-maxburstsize*]
no vbr-nrt *output-pcr output-scr output-maxburstsize* [*input-pcr*] [*input-scr*] [*input-maxburstsize*]

Cisco 10000 シリーズ ルータ
vbr-nrt *output-pcr output-scr output-maxburstsize*
no vbr-nrt *output-pcr output-scr output-maxburstsize*

構文の説明

output-pcr	出力 PCR（単位：KB/秒（kbps））。
output-scr	kbps 単位の出力 SCR
output-maxburstsize	出力最大バースト セル サイズ（セルの数で示される）。
input-pcr	（SVC の場合だけの任意）kbps 単位の入力 PCR。
input-scr	（SVC の場合だけの任意）kbps 単位の入力 SCR。
input-maxburstsize	（SVC の場合だけの任意）入力最大バースト セル サイズ（セルの数で示される）。

コマンド デフォルト

物理インターフェイスの最大ライン レートでの未指定ビット レート（UBR）QoS がデフォルトです。

コマンド モード

ATM PVC-in-range コンフィギュレーション（PVC 範囲内の個々の PVC の場合）
ATM PVC 範囲コンフィギュレーション（ATM PVC 範囲の場合）
ATM PVP コンフィギュレーション
Bundle-vc コンフィギュレーション（ATM VC バンドル メンバーの場合）
interface-ATM-VC コンフィギュレーション（ATM PVC または SVC の場合）
VC-class コンフィギュレーション（VC クラスの場合）

コマンド履歴

リリース	変更箇所
11.3T	このコマンドが導入されました。

リリース	変更箇所
12.0(3)T	このコマンドは、ATMバンドルメンバーおよびVCバンドルメンバーに対する、BR-NRT QoS の設定、および、出力 PCR、出力 SCR、および、出力最大バーストセルサイズの指定をサポートするために拡張されました。
12.0(25)SX	このコマンドが Cisco IOS Release 12.0(25)SX に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.1(5)T	このコマンドが、PVC 範囲コンフィギュレーション モードおよび PVC-in-range コンフィギュレーション モードで使用できるようになりました。
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。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 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。
Cisco IOS XE リリース 2.3	このコマンドが、ATM PVP コンフィギュレーション モードで使用できるようになりました。

使用上のガイドライン

QoS パラメータを設定するには、**ubr**、**ubr+**、**vbr-nrt** のいずれかのコマンドを使用します。最後に入力したコマンドが、該当する PVC または SVC に適用されます。

ATM PVC または SVC 上で、**vbr-nrt** コマンドが明示的に設定されない場合、VC は次のデフォルト設定を継承します（優先順位の順にリストされています）。

- PVC または SVC 自身に割り当てられた VC クラスの任意の QoS コマンド（**ubr**、**ubr+**、または **vbr-nrt**）の設定。
- PVC または SVC の ATM サブインターフェイスに割り当てられた VC クラスの任意の QoS コマンド（**ubr**、**ubr+**、または **vbr-nrt**）の設定。
- PVC または SVC の ATM メイン インターフェイスに割り当てられた VC クラスの任意の QoS コマンド（**ubr**、**ubr+**、または **vbr-nrt**）の設定。
- グローバル デフォルト：PVC または SVC の最大ライン レートの UBR QoS

このコマンドを VC-class コンフィギュレーション モードで使用するには、**vbr-nrt** コマンドを入力する前に **vc-classatm** 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。コマンドを含む VC クラスがスタンドアロン VC（バンドル メンバーではない VC）に付加されている場合、このコマンドは効果がありません。

このコマンドを bundle-VC コンフィギュレーション モードで使用するには、**pvc-bundle** コンフィギュレーション コマンドを入力し、VC をバンドル メンバーとして追加します。

VCバンドルのVCは、次の設定継承規則に従います（優先順位の順にリストされています）。

- bundle-VC モードの VC 設定
- バンドルモードのバンドル設定（および、割り当てられたVC-classコンフィギュレーションの影響）
- サブインターフェイス モードのサブインターフェイス設定

Cisco 10000 シリーズ ルータ

入力 PCR、入力 SCR、および入力最大バースト サイズ（MBS）はサポートされていません。

Cisco IOS Release 12.2(31)SB2 以降のリリースの場合、出力 PCR と SCR を同じ値に設定すると、Cisco IOS ソフトウェアでは最大バースト セル サイズを 1 にすることができます。次に例を示します。

Cisco IOS Release 12.2(31)SB2 より前

```
interface ATM2/0/0.81801 point-to-point
 bandwidth 11760
 pvc 81/801
  vbr-nrt 11760 11760 32
  encapsulation aal5snap
  protocol pppoe
```

Cisco IOS Release 12.2(31)SB2 以降のリリース

```
interface ATM2/0/0.81801 point-to-point
 bandwidth 11760
 pvc 81/801
  vbr-nrt 11760 11760 1
  encapsulation aal5snap
  protocol pppoe
```

例

次の例では、ATM PVC の出力 PCR に 100,000 kbps を、出力 SCR に 50,000 kbps を、出力 MBS に 64 を指定しています。

```
pvc 1/32
 vbr-nrt 100000 50000 64
```

次の例では、ATM SVC の VBR-NRT 出力パラメータ、および入力パラメータを指定しています。

```
svc atm-svc1 nsap 47.0091.81.000000.0040.0B0A.2501.ABC1.3333.3333.05
 vbr-nrt 10000 5000 32 20000 10000 64
```

関連コマンド

コマンド	説明
abr	ABR QoS を選択し、ATM PVC または仮想回線クラスの出力ピーク セル レートおよび出力最小保証セル レートを設定します。

コマンド	説明
broadcast	ブロードキャスト パケットの複製と、ATM VC クラス、PVC、SVC、または VC バンドルへの送信を設定します。
bump	仮想回線バンドルに割り当てることができる仮想回線クラスのバンピング ルールを設定します。
bundle	バンドルを作成するか、または既存のバンドルを修正してバンドル コンフィギュレーション モードを開始します。
class-int	VC クラスを ATM メイン インターフェイスまたはサブインターフェイスに割り当てます。
class-vc	VC クラスを ATM PVC、SVC、または VC バンドル メンバーに割り当てます。
encapsulation	インターフェイスで使用するカプセル化方式を設定します。
inarp	ATM PVC、VC クラス、または VC バンドルの Inverse ARP の時間を設定します。
oam-bundle	仮想回線バンドルに適用できる仮想回線クラスに対して、エンドツーエンド F5 OAM ループバック セル生成および OAM 管理を有効にします。
oamretry	ATM PVC、SVC、VC クラス、または、VC バンドルの OAM 管理に関連するパラメータを設定します。
precedence	仮想回線バンドルに割り当てることができ、したがって、そのバンドルのすべての仮想回線メンバーに適用される、仮想回線クラスの優先レベルを設定します。
protect	保護されたグループまたは保護された仮想回線ステータスが仮想回線バンドル メンバーに適用されるように、仮想回線クラスを設定します。
protocol(ATM)	ATM PVC、SVC、VC クラス、または VC バンドルのスタティック マップを設定します。次に、直接 PVC 上、VC バンドル上、または VC クラス内で Inverse ARP を設定することによって、ATM PVC の Inverse ARP または Inverse ARP ブロードキャストをイネーブルにします（IP および IPX プロトコルだけに適用）。
pvc-bundle	バンドルに対してバンドルのメンバーとして PVC を追加し、PVC バンドル メンバーを設定するために bundle-vc コンフィギュレーション モードに入ります。
ubr	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レートを指定します。
ubr+	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レートと出力最小保証セル レートを指定します。

コマンド	説明
vc-classatm	ATM PVC、SVC、または ATM インターフェイス用に VC クラスを作成し、VC-class コンフィギュレーション モードを開始します。

vc-hold-queue

ATM アダプタで仮想回線（VC）単位ホールド キューを設定するには、インターフェイス コンフィギュレーション モードで**vc-hold-queue** コマンドを使用します。VC 単位ホールド キューのデフォルト値に戻るには、このコマンドの **no** 形式を使用します。

vc-hold-queue *number-of-packets*
no vc-hold-queue *number-of-packets*

構文の説明

number-of-packets	VC 単位ホールド キューに設定できるパケット数を指定します。パケット数は、最小で 5、最大で 1024 です。

コマンド デフォルト

ホールド キューのデフォルト値は、使用中のキューイング メカニズムによって設定されます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(5)T	このコマンドが導入されました。
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。

使用上のガイドライン

このコマンドは、VC 単位キューイングをサポートする Cisco 7200 シリーズ ルータ、Cisco 2600 アダプタ、および Cisco 3600 アダプタ上でのみ使用できます。

このコマンドは、VC レベルでのみ設定できます。

例

次に、VC 単位ホールド キューを 55 に設定する例を示します。

```
interface atm2/0.1
 pvc 1/101
  vc-hold-queue 55
```

関連コマンド

コマンド	説明
hold-queue	インターフェイスのホールドキュー制限を指定します。
showinterfaces	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。
showqueueinginterface	インターフェイスまたはVCのキューイングの統計情報を表示します。

wrr-queue bandwidth

標準の送信キュー間で帯域幅を割り当てるには、インターフェイス コンフィギュレーション モードで **wrr-queuebandwidth** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

wrr-queue bandwidth *weight-1 . . . weight-n*
no wrr-queue bandwidth

構文の説明

weight-1 ...weight-n	WRR 重みを指定します。有効値は 1 ～ 255 です。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- QoS が有効な場合 - 4：255
- QoS が無効な場合 - 255：1

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17a)SX	このコマンドは、7 個のキューの重みをサポートするように変更されました。
12.2(17d)SXB	Supervisor Engine 2 でのこのコマンドのサポートが Release 12.2(17d)SXB に拡張されました。
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。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

Supervisor Engine 720 で設定されている Cisco 7600 シリーズ ルータでは、最大 7 個のキューの重みを設定できます。

Supervisor Engine 2 で設定されている Cisco 7600 シリーズ ルータでは、最大 3 個のキューの重みを設定できます。

WRR を使用すると、出力ポートで帯域幅を共有できます。このコマンドは、スケジューリング重みによって、出力 WRR の帯域幅を定義します。出力完全優先キューを有効にしている場合を除き、4 個のキューが WRR に参加します。完全優先キューは空になるまで使用される絶対優先キューで、空になると WRR キューのいずれかが使用されます。

wrr-queuebandwidth コマンドに順序の依存関係はありません。出力優先順位を有効にすると、最初の 2 つと最後のパラメータで重み比率が計算されます。それ以外の場合は、4 つすべてのパラメータが使用されます。

WRR 重みは、すべてのキューが空でない場合に、キュー間で帯域幅を分割するために使用されます。たとえば、重み 1:3 を入力すると、両方のキューにデータが存在する限り、1 つのキューが 25 % の帯域幅を取得し、もう 1 つのキューが 75 % の帯域幅を取得することになります。

例

次に、3 対 1 の帯域幅比率を割り当てる例を示します。

```
Router(config-if)# wrr-queue bandwidth 3 1
```

関連コマンド

コマンド	説明
showqueueinginterface	キューイング情報を表示します。
wrr-queuequeue-limit	インターフェイス上の送信キューサイズ比を設定します。

wrr-queue cos-map

キューの廃棄しきい値に CoS 値をマップするには、インターフェイス コンフィギュレーション モードで **wrr-queuecos-map** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

wrr-queue cos-map *queue-id threshold-id cos-1 ... cos-n*
no wrr-queue cos-map

構文の説明

queue-id	キュー番号。有効値は 1 ～ 2 です。
threshold-id	しきい値 ID。有効値は 1 ～ 2 です。
cos-1 *...cos-n*	CoS 値。有効値は 0 ～ 7 です。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- 受信キュー 1/廃棄しきい値 1 および送信キュー 1/廃棄しきい値 1： CoS 0 および 1。
- 受信キュー 1/廃棄しきい値 2 および送信キュー 1/廃棄しきい値 2： CoS 2 および 3。
- 受信キュー 2/廃棄しきい値 3 および送信キュー 2/廃棄しきい値 1： CoS 4 および 6。
- 受信キュー 2/廃棄しきい値 4 および送信キュー 2/廃棄しきい値 2： CoS 7。
- 1p1q4t、1p2q2t、および 1p3q1t インターフェイスでは、CoS 5 が完全プライオリティ キューにマッピングされます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	スーパーバイザ エンジン 2 上のこのコマンドのサポートが Release 12.2(17d)SXB に拡張されました。
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。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

しきい値にマッピングする CoS 値を、最大 8 つ入力します。

1p3q1t のしきい値は常に 1 です。

例

次に、標準送信キュー 1/しきい値 1 に CoS 値 0 および 1 をマッピングする例を示します。

```
Router(config-if)# wrr-queue cos-map 1 1 0 1
```

awrr-queue dscp-map

キューの廃棄しきい値にハードウェア DiffServ コードポイント（DSCP）値をマップするには、インターフェイス コンフィギュレーション モードで **wrr-queuedscp-map** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

wrr-queue dscp-map *queue-id threshold-id dscp-1 ... dscp-n*
no wrr-queue dscp-map *queue-id*

構文の説明

queue-id	キュー番号。有効値は 1 ～ 8 です。
threshold-id	しきい値 ID。有効値は 1 ～ 4 です。
dscp-1 ...dscp-n	DSCP 値。有効値は、0 ～ 7 です。

コマンド デフォルト

インターフェイスはサービス クラス（CoS）モードになっています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(18)SXF5	このコマンドが導入されました。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

（注） **wrr-queuedscp-map** コマンドを入力するには、インターフェイスが DSCP キューイング モードである必要があります。モードを DSCP に設定するには、**mlsqosqueue-modemode-dscp** コマンドを使用します。

このコマンドは、10 ギガビット イーサネット ポートだけでサポートされます。

DSCP 値をマッピングする場合、次の注意事項に従ってください。

- キューとしきい値にマッピングする DSCP 値を、最大 8 つ入力できます。

- 複数のコマンドを入力して、追加のDSCP値をキューおよびしきい値にマッピングできます。
- キューおよびしきい値ごとに個別のコマンドを入力する必要があります。

例

次に、ハードウェアDSCP値をキューの廃棄しきい値にマッピングする例を示します。

```
wrr-queue dscp-map 8 1 0 1 2 3
```

関連コマンド

showqueueinginterface	キューイング情報を表示します。

wrr-queue queue-limit

インターフェイスで送信キュー サイズ比率を設定するには、インターフェイス コンフィギュレーション モードで **wrr-queuequeue-limit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

wrr-queue queue-limit *queue1-weight* [*queue2-weight*] *queue3-weight*
no wrr-queue queue-limit

構文の説明

queue1-weight	ロー プライオリティ キューの重み比を指定します。有効値は 1 ～ 100% です。
queue2-weight	（任意）ミディアム プライオリティ キューの重み比を指定します。有効値は 1 ～ 100% です。
queue3-weight	ハイ プライオリティ キューの重み比を指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- ロー プライオリティでは 90%
- ハイ プライオリティでは 10%

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	スーパーバイザ エンジン 2 上のこのコマンドのサポートが Release 12.2(17d)SXB に拡張されました。
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。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

有効なハイ プライオリティ重み値は 1 ～ 100% です。ただし、1p2q1t 出力 LAN ポートでは例外的に、ハイ プライオリティ キューの有効値は 5 ～ 100% です。

1p2q2t インターフェイスでは、QoS はハイ プライオリティ キュー サイズに等しい絶対優先キュー サイズを設定します。

ネットワークにおけるロー プライオリティ トラフィックとハイ プライオリティ トラフィックの比率を概算してください（例：ロー プライオリティ トラフィック 80%、ハイ プライオリティ トラフィック 20%など）。概算したパーセント値を、各キューの重みとして使用します。

ハードウェアのプログラミング精度により、ハードウェアに設定される値は、指定された値の近似値となります。たとえば、0% を指定した場合、実際にプログラムされる値は必ずしも 0 ではありません。

例

次に、送信キュー サイズ比を設定する例を示します。

```
Router(config-if)# wrr-queue queue-limit 75 25
```

関連コマンド

コマンド	説明
showqueueinginterface	キューイング情報を表示します。
wrr-queuebandwidth	標準送信キュー間の帯域幅を割り当てます。

wrr-queue random-detect

1p2q2t および 1p3q1t インターフェイスの指定したキューに対して、WRED を有効にしたり、最小および最大 WRED しきい値を指定したりするには、インターフェイス コンフィギュレーション モードで **wrr-queuerandom-detect** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

wrr-queue random-detect *queue-id*
wrr-queue random-detect {**max-threshold**|**min-threshold**} *queue-id threshold-percent-1 ... threshold-percent-n*
no wrr-queue random-detect *queue-id*
no wrr-queue random-detect {**max-threshold**|**min-threshold**} *queue-id*

構文の説明

queue-id	キュー番号。有効値は1、2、または3です。
max-threshold	最大 WRED 廃棄しきい値を指定します。
min-threshold	最小 WRED 廃棄しきい値を指定します。
threshold-percent-1 threshold-percent-n	しきい値の重み。有効値は 1 ～ 100% です。

コマンド デフォルト

デフォルトでは、WRED はディセーブルです。WRED をイネーブルにした場合、デフォルトは次のとおりです。

- 最大しきい値は 40%（低）および 100%（高）です。
- 最小しきい値は、両方ともゼロに設定されます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	スーパーバイザ エンジン 2 上のこのコマンドのサポートが Release 12.2(17d)SXB に拡張されました。
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。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

1p2q1t および 1p3q1t インターフェイスの場合、標準送信キューに WRED 廃棄しきい値があります。1p3q1t送信キューは、WRED廃棄しきい値またはテール廃棄しきい値を使用するように設定できます。

1p2p1t インターフェイスの WRED 廃棄しきい値を有効にするには、**wrr-queuerandom-detect***queue-id* コマンドを使用します。WRED を無効にするには、このコマンドの **no** 形式を使用します。

1p3q1t インターフェイスの WRED 廃棄しきい値を有効にするには、**wrr-queuerandom-detect***queue-id* コマンドを使用します。テール ドロップしきい値に戻すには、**nowrr-queuerandom-detect***queue-id* コマンドを使用します。

queue-id 引数は、標準ロープライオリティ キューの場合は1、標準ハイ プライオリティ キューの場合は 2、絶対優先キューの場合は 3 です。

完全プライオリティ キューのしきい値は設定できません。

1p2q2t インターフェイスの各キューには 2 つのしきい値、1p3q1t インターフェイスには 1 つのしきい値があります。

しきい値には、それぞれロー WRED 値およびハイ WRED 値があります。

WRED 値はキュー容量のパーセントです。

WRED しきい値の設定の詳細については、『*Cisco 7600 Series Router Cisco IOS Software Configuration Guide*』の QoS の章を参照してください。

例

次に、ロー プライオリティ送信キューのハイ WRED 廃棄しきい値を設定する例を示します。

```
Router(config-if)# wrr-queue random-detect max-threshold 1 60 100
```

関連コマンド

コマンド	説明
showqueueinginterface	キューイング情報を表示します。
wrr-queuequeue-limit	インターフェイス上の送信キューサイズ比を設定します。

wrr-queue threshold

1q4tおよび2q2tインターフェイスの標準受信キューおよび標準送信キューの廃棄しきい値パーセントを設定するには、インターフェイス コンフィギュレーション モードで**wrr-queuethreshold** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

wrr-queue threshold *queue-id threshold-percent-1 ... threshold-percent-n*
no wrr-queue threshold *queue-id*

構文の説明

queue-id	キュー番号。有効値は 1 ～ 2 です。
threshold-percent-1 threshold-percent-n	キュー 1 および 2 の重み値。有効値は 1 ～ 100% です。

コマンド デフォルト

QoS をイネーブルにした場合、デフォルト値は次のとおりです。

- **100** %：しきい値 1
- **60** %：しきい値 2

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	スーパーバイザ エンジン 2 上のこのコマンドのサポートが Release 12.2(17d)SXB に拡張されました。
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。
12.2(50)SY	このコマンドがサポートされるようになりました。

使用上のガイドライン

（注） Cisco IOS Release 12.2(50)SY 以降では、**platform qos queueing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

送信キュー番号としきい値番号を使用する必要があります。

queue-id 引数は、標準ロープライオリティ キューの場合は 1、標準ハイ プライオリティ キューの場合は 2 です。

しきい値は常に 2 ～ 100% の範囲で設定してください。

受信キューの廃棄しきい値は、trust CoS に設定されたギガビット イーサネット インターフェイスに限りサポートされます。

例

受信キュー 1/しきい値 1 および送信キュー 1/しきい値 1 を設定する例を示します。

```
Router(config-if)# wrr-queue threshold 1 60 100
```

関連コマンド

コマンド	説明
showqueueinginterface	キューイング情報を表示します。
wrr-queuequeue-limit	インターフェイス上の送信キューサイズ比を設定します。