ipinfusion™

OcNOS®

Open Compute Network Operating System for Data Centers

Layer 2

Version 7.0.0

March 2026

IP Infusion Inc. Proprietary

©2026 IP Infusion Inc. All Rights Reserved.

This documentation is subject to change without notice. The software described in this document and this documentation are furnished under a license agreement or nondisclosure agreement. The software and documentation may be used or copied only in accordance with the terms of the applicable agreement. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's internal use without the written permission of IP Infusion Inc.

IP Infusion Inc.

3979 Freedom Circle, Suite 900

Santa Clara, CA 95054

+1 408-400-1900

http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:

support@ipinfusion.com

Trademarks:

IP Infusion and are trademarks or registered trademarks of IP Infusion. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Use of certain software included in this equipment is subject to the IP Infusion, Inc. End User License Agreement at http://www.ipinfusion.com/license. By using the equipment, you accept the terms of the End User License Agreement.

CONTENTS

Contents ... **3**

Preface ... **61**
About this Guide ... 61
Audience ... 61
Conventions ... 61
IP Infusion Product Release Version ... 61
Related Documentation ... 62
Feature Availability ... 62
Migration Guide ... 62
IP Maestro Support ... 62
Technical Support ... 62
Technical Sales ... 62
Technical Documentation ... 62
Documentation Disclaimer ... 63
Comments ... 63
Command Line Interface ... 64
Overview ... 64
Chapter Organization ... 64
Command Line Interface Help ... 64
Command Completion ... 65
Command Abbreviations ... 65
Command Line Errors ... 66
Command Negation ... 66
Syntax Conventions ... 66
Variable Placeholders ... 67
Command Description Format ... 68
Keyboard Operations ... 68
Show Command Modifiers ... 69
Begin Modifier ... 69
Include Modifier ... 70
Exclude Modifier ... 70
Redirect Modifier ... 71
Last Modifier ... 71
String Parameters ... 71
Command Modes ... 72
Command Mode Tree ... 73
Transaction-based Command-line Interface ... 73

Layer 2 Configuration Guide ... **75**
802.1X Configuration ... 79
Topology ... 79
Configuration ... 79

© 2026 IP Infusion Inc. Proprietary

Validation ... 80
Disabling Native VLAN Configuration ... 81
Topology ... 81
Configuration of SW1 and SW2 ... 81
SW1 ... 81
SW2 ... 82
Validation ... 82
Configuring acceptable-frame-type vlan-tagged on ingress interface ... 83
SW1 ... 83
Validation ... 83
Disabling Native VLAN Configuration on Trunk mode ... 85
Topology ... 85
Configuration ... 85
SW1 ... 85
SW2 ... 86
Validation ... 86
Configuring Disable-Native-VLAN on Trunk mode ... 87
SW1 ... 87
Validation ... 87
Layer 2 Control Protocols Tunneling ... 89
Overview ... 89
L2CP Tunneling in Provider Bridging ... 89
L2CP Configuration in Provider Bridging ... 89
L2CP Tunneling in VXLAN ... 90
Link Aggregation Configuration ... 92
Topology ... 92
Dynamic LAG Configuration ... 92
SW1 ... 92
SW2 ... 94
Validation ... 95
Static LAG Configuration ... 95
SW1 ... 95
SW2 ... 96
Validation ... 97
Static LAG Minimum Link Configuration ... 98
Topology ... 98
Validation ... 99
Static-LAG Minimum Bandwidth Configuration ... 100
Topology ... 100
Validation ... 101
Dynamic-LAG Minimum Link Configuration ... 103
Topology ... 103
Validation ... 103
Dynamic LAG Minimum Bandwidth Configuration ... 106
Topology ... 106
Validation ... 107
LACP Minimum-Link, Minimum-Bandwidth on Dynamic and Static Channel-Groups with ... 109

MLAG
Overview 109
Minimum Active Members/Bandwidth 109
Topology 110
Configuration 110
Validation 122
LACP Force-Up 124
LACP Force-up with Dynamic LAG 124
LACP Aggregator Force-up 130
Overview 130
Feature Characteristics 130
Benefits 130
LACP Aggregator Force-up for Dynamic LAG Configuration 131
Topology 131
LACP Aggregator Force-up for MLAG Configuration 132
Topology 132
Configuration 133
Implementation Examples 136
CLI Command 136
lacp agg force-up 136
Glossary 137
MLAG Configuration 139
Intra-Domain-Link (IDL) 139
Intra-Domain-Peer (IDP) 139
Options to Configure Intra-Domain 140
With IDL only 140
With IDL and IDP 140
Topology 141
Configuration 141
Validation 146
MLAG Active-Active Dynamic Configuration 150
Topology 150
LEAF 151
LwSW 152
TOR-01 153
TOR-02 156
Validation 158
Static Configuration 160
Topology 161
L2SW 161
TOR1 162
TOR2 163
LEAF 165
Validation 166
ARP ACL Configuration 168
Topology 168
TOR1 168

TOR2 170
SW1 172
LEAF 173
Validation 174
MSTP Configuration 175
Configuration 175
Topology 175
Validation 183
Port Security Configuration 190
Secured MACs Learned Dynamically 190
SW1 190
Validation 191
Secured MAC Addresses Learned Statically 192
Validation 192
Static Mode 193
Validation 193
Disable Spanning Tree Configuration 195
Disabling MSTP Configuration 195
MSTP Validation 196
Verify MSTP details with the show spanning-tree mst detail command. 196
STP Configuration 200
STP Validation 200
RSTP Configuration 202
RSTP Validation 203
Link Layer Discovery Protocol Configuration 206
Topology 206
LLDPv2 (Interface Mode TLV) 207
Default Agent 207
Customer Bridge 209
Non-Tpmr-Bridge 211
Global Mode TLV 214
Topology 214
SW1 214
SW2 214
LLDP-MED 217
LLDP-MED Network Connectivity Device 217
LLDP-MED Generic Endpoint (Class I) 217
LLDP-MED Generic Endpoint (Class 2) 217
LLDP-MED Generic Endpoint (Class 3) 218
Provider Bridging Configuration 222
Overview 222
Single Provider Bridge Configuration 222
Topology 222
Configuration 222
Validation 224
Two Provider Bridge Configuration 225
Topology 225

© 2026 IP Infusion Inc. Proprietary

Configuration 225
Validation 228
Layer 2 Protocol Tunneling (L2PT/L2CP Tunneling) 229
Topology 229
Configuring the L2PT Protocol on the Interface 229
Validation 230
Provider Bridging with VLAN Translation 230
Topology 231
PEB1 231
PEB2 233
Translation Cases 234
Provider Bridging QoS Configuration 242
Scenario: 1 Traffic flow from CEP to PNP 242
Validation for Scenario 1 244
Scenario: 2 Traffic flow from PNP to CEP 246
Validation for Scenario 2 248
Provider Bridging Untagged-pep Configuration 249
Topology 249
Configuration 250
Validation 252
Provider Bridging Configuration (SVLAN) 253
Customer-Network Port (CNP) 253
STAG-based Interface 253
Port-based Interface 253
Topology 254
Configuration 254
SW1 (PEB) 254
SW2 (PB) 255
SW3 (PEB) 255
Validation 256
Traffic Mirroring Configuration 257
SPAN Overview 257
Port Mirroring 257
VLAN Mirroring 257
Rule Based Mirroring 257
Topology 258
Port Mirroring Configuration 258
Validation 259
Validation 260
VLAN and Rule Based Mirroring 261
Validation 262
RSPAN Overview 262
Topology 263
Port Mirroring Configuration 263
Validation 264
VLAN and Rule Based Mirroring Configuration 264
Validation 265

© 2026 IP Infusion Inc. Proprietary

VLAN Mirroring Using VLAN Ranges Configuration 266
Feature Characteristics 266
Benefits 266
Configuration 266
Topology 267
VTEP1 267
VTEP2 272
Validation 278
Validation for Port Mirroring 281
Revised CLI Commands 281
Abbreviations 282
Traffic Mirroring using ERSPAN 283
Overview 283
Feature Characteristics 283
Supported Hardware 283
Prerequisites 284
Configuration 284
Topology 284
Configure ERSPAN destination 285
Configure ERSPAN sender session 286
CLI Commands 287
destination erspn 287
origin-ip 287
destination-ip 288
vrf 289
ttl 289
dscp 290
enable-truncate 291
erspan-type 291
erspn-id 292
hardware-id 293
switch-id 293
Revised Command 294
Glossary 294
Private VLAN Configuration 296
Topology 296
Configure PVLAN Trunk and Promiscuous Trunk Port 296
SW1 296
SW2 298
Validation 299
Configure PVLAN Trunk and Promiscuous Access Port 299
SW1 299
SW2 301
Validation 302
Spanning Tree Protocol Configuration 304
Configurations 304
Topology 304

Validation 307
MLAG with Provider Bridging Configuration 313
Configuration 313
Topology 313
Validation 320
RPVST+ Configuration 326
Topology 326
Configuration 326
Switch 2 326
Switch 1 327
Switch 3 327
Validation 328
Switch2 328
RSTP Configuration 331
Configuration 331
Topology 331
Validation 333
VLAN Configuration 340
Configuration 340
Topology 340
Validation 344
ErrDisable for Link-Flapping Configuration 347
Topology 347
Automatic Recovery 347
RTR1 347
Log Message 348
Manual Recovery 349
RTR1 349
ErrDisable at the Interface Level 350
ErrDisable for Storm-Control Configuration 351
Topology 351
Automatic Recovery 351
RTR1 351
Validation 352
Log Message 352
Manual Recovery 353
RTR1 353
Validation 353
Errdisable at the Interface Level 354
Validation 354
Sample show running-configuration output 355
Support IGMP Snooping for Provider Bridge 358
Overview 358
Feature Characteristics 358
Benefits 358
Prerequisites 358
Configuration 359

Topology 359
R1 359
PE1 360
PE 361
PE2 362
Validation 363
Abbreviations 365
Unidirectional Link Detection Configuration 366
Topology 366
Configuration 366
S1 366
S2 367
Validation 367
Enable UDLD under bridge-group 368
S1 368
S2 368
Validation 369
MAC Authentication Bypass 370
Topology 370
Configuration 370
Switch Configuration for MAC Authentication Bypass (MAB) 370
Validation 371
Configuration 371
MAC Authentication Configuration 371
Validation 372
Traffic Segmentation-Protected Port 373
Topology 373
Isolated-Promiscuous Configuration 373
RTR1 373
Isolated-Isolated Configuration 376
RTR1 376
Mirror Filtered Packets to CPU 380
Feature Characteristics 380
Benefits 380
Limitations 380
Supported Hardware 381
Configuration 381
Topology 381
Validation 383
CLI Commands 384
monitor destination sniff truncate 384

Layer 2 Command Reference 386

Link Layer Discovery Protocol v2 Commands 395
clear lldp counters 396
Command Syntax 396
Parameters 396

Command Mode 396
Applicability 396
Examples 396
clear lldp neighbors 397
Command Syntax 397
Parameters 397
Command Mode 397
Applicability 397
Examples 397
lldp-agent 398
Command Syntax 398
Parameters 398
Default 398
Command Mode 398
Applicability 398
Examples 398
debug lldp 399
Command Syntax 399
Parameters 399
Command Mode 399
Applicability 399
Examples 399
lldp run 400
Command Syntax 400
Parameters 400
Command Mode 400
Applicability 400
Example 400
lldp tlv-select 401
Command Syntax 401
Parameters 401
Default 401
Command Mode 401
Applicability 401
Examples 401
lldp tlv-select med 402
Command Syntax 402
Parameters 402
Default 402
Command Mode 402
Applicability 402
Examples 402
lldp tlv-select basic-mgmt 403
Command Syntax 403
Parameters 403
Default Value 403
Command Mode 403

Applicability 403
Examples 403
lldp tlv-select ieee-8021-org-specific 404
Command Syntax 404
Parameters 404
Default Value 404
Command Mode 404
Applicability 404
Examples 404
lldp tlv-select ieee-8023-org-specific 405
Command Syntax 405
Parameters 405
Default Value 405
Command Mode 405
Applicability 405
Examples 405
set lldp agt-circuit-id 406
Command Syntax 406
Parameters 406
Command Mode 406
Applicability 406
Examples 406
set lldp chassis-id-tlv 407
Command Syntax 407
Parameters 407
Command Mode 407
Applicability 407
Examples 407
set lldp chassis locally-assigned 408
Command Syntax 408
Parameters 408
Command Mode 408
Applicability 408
Examples 408
set lldp disable 409
Command Syntax 409
Parameters 409
Command Mode 409
Applicability 409
Examples 409
set lldp enable 410
Command Syntax 410
Parameters 410
Default 410
Command Mode 410
Applicability 410
Examples 410

set lldp locally-assigned 411
Command Syntax 411
Parameters 411
Command Mode 411
Applicability 411
Examples 411
set lldp management-address-tlv 412
Command Syntax 412
Parameters 412
Command Mode 412
Applicability 412
Examples 412
set lldp med-devtype 413
Command Syntax 413
Parameters 413
Default 413
Command Mode 413
Applicability 413
Examples 413
set lldp msg-tx-hold 414
Command Syntax 414
Parameters 414
Default 414
Command Mode 414
Applicability 414
Examples 414
set lldp port-id-tlv 415
Command Syntax 415
Parameters 415
Command Mode 415
Applicability 415
Examples 415
set lldp system-description 416
Command Syntax 416
Parameters 416
Command Mode 416
Applicability 416
Example 416
set lldp system-name 417
Command Syntax 417
Parameters 417
Command Mode 417
Applicability 417
Example 417
set lldp timer 418
Command Syntax 418
Parameters 418

© 2026 IP Infusion Inc. Proprietary

Default ... 418
Command Mode ... 418
Applicability ... 418
Examples ... 418
set lldp too-many-neighbors ... 420
Command Syntax ... 420
Parameters ... 420
Default ... 420
Command Mode ... 420
Applicability ... 420
Examples ... 421
set lldp tx-fast-init ... 422
Command Syntax ... 422
Parameters ... 422
Default ... 422
Command Mode ... 422
Applicability ... 422
Examples ... 422
set lldp tx-max-credit ... 423
Command Syntax ... 423
Parameters ... 423
Default ... 423
Command Mode ... 423
Applicability ... 423
Examples ... 423
show debugging lldp ... 424
Command Syntax ... 424
Parameters ... 424
Command Mode ... 424
Applicability ... 424
Example ... 424
show lldp neighbors ... 425
Command Syntax ... 425
Parameters ... 425
Command Mode ... 425
Applicability ... 425
Example ... 425
show lldp interface ... 428
Command Syntax ... 428
Parameters ... 428
Command Mode ... 428
Applicability ... 428
Example ... 428
snmp restart lldp ... 430
Port Based xConnect Commands ... 431
backup ... 432
Command Syntax ... 432

Parameters 432
Default 432
Command Mode 432
Applicability 432
Example 432
cross-connect 433
Command Syntax 433
Parameters 433
Default 433
Command Mode 433
Applicability 433
Example 433
cross-connect-switchover-type-revertive 434
Command Syntax 434
Parameters 434
Default 434
Command Mode 434
Applicability 434
Example 434
disable 435
Command Syntax 435
Parameters 435
Default 435
Command Mode 435
Applicability 435
Example 435
ep1ep2 436
Command Syntax 436
Parameters 436
Default 436
Command Mode 436
Applicability 436
Example 436
link-fault-pass-through enable 437
Command Syntax 437
Parameters 437
Default 437
Command Mode 437
Applicability 437
Example 437
show cross-connect 438
Command Syntax 438
Parameters 438
Default 438
Command Mode 438
Applicability 438
Example 438

Fundamental Layer 2 Commands 440
errdisable cause 441
Command Syntax 441
Parameters 441
Default 441
Command Mode 441
Applicability 441
Examples 441
errdisable link-flap-setting 442
Command Syntax 442
Parameters 442
Default 442
Command Mode 442
Applicability 442
Examples 442
errdisable storm-control 443
Command Syntax 443
Parameters 443
Default 443
Command Mode 443
Applicability 443
Examples 444
errdisable timeout 445
Command Syntax 445
Parameters 445
Default 445
Command Mode 445
Applicability 445
Examples 445
l2protocol all learn-disable 446
Command Syntax 446
Parameters 446
Default 446
Command Mode 446
Applicability 446
Examples 446
show errdisable details 447
Command Syntax 447
Parameters 447
Default 447
Command Mode 447
Applicability 447
Examples 447
show interface errdisable status 448
Command Syntax 448
Parameters 448
Default 448

© 2026 IP Infusion Inc. Proprietary

Command Mode 448
Applicability 448
Examples 448
show running-config switch 449
Command Syntax 449
Parameters 449
Default 450
Command Mode 450
Applicability 450
Examples 450
show tcp 451
Command Syntax 451
Parameters 451
Command Mode 451
Applicability 451
Examples 451
watch static-mac-movement 453
Command Syntax 453
Parameters 453
Default 453
Command Mode 453
Applicability 453
Examples 453
Bridge Commands 454
bridge acquire 455
Command Syntax 455
Parameter 455
Default 455
Command Mode 455
Applicability 455
Example 455
bridge address 456
Command Syntax 456
Parameters 456
Default 456
Command Mode 456
Applicability 456
Example 457
bridge ageing 458
Command Syntax 458
Parameters 458
Default 458
Command Mode 458
Applicability 458
Example 458
bridge forward-time 459
Command Syntax 459

Parameters 459
Default 459
Command Mode 459
Applicability 459
Example 459
bridge-group 460
Command Syntax 460
Parameters 460
Default 460
Command Mode 460
Applicability 460
Examples 460
bridge hello-time 461
Command Syntax 461
Parameters 461
Default 461
Command Mode 461
Applicability 461
Examples 461
bridge mac-priority-override 462
Command Syntax 462
Parameters 462
Default 462
Command Mode 462
Applicability 462
Example 462
bridge max-age 464
Command Syntax 464
Parameters 464
Default 464
Command Mode 464
Applicability 464
Examples 464
bridge max-hops 465
Command Syntax 465
Parameters 465
Default 465
Command Mode 465
Applicability 465
Examples 465
bridge priority 466
Command Syntax 466
Parameters 466
Default 466
Command Mode 466
Applicability 466
Examples 466

bridge shutdown 467
Command Syntax 467
Parameters 467
Default 467
Command Mode 467
Applicability 467
Example 467
bridge transmit-holdcount 468
Command Syntax 468
Parameters 468
Default 468
Command Mode 468
Applicability 468
Examples 468
bridge-group path-cost 469
Command Syntax 469
Parameters 469
Default 469
Command Mode 469
Applicability 469
Example 469
bridge-group priority 470
Command Syntax 470
Parameters 470
Default 470
Command Mode 470
Applicability 470
Example 470
clear allowed-ethertype 471
Command Syntax 471
Parameters 471
Command Mode 471
Applicability 471
Example 471
clear mac address-table 472
Command Syntax 472
Parameters 472
Command Mode 472
Applicability 473
Examples 473
dot1ad ethertype 474
Command Syntax 474
Parameters 474
Default 474
Command Mode 474
Applicability 474
Examples 474

l2protocol all learn-disable 475
Command Syntax 475
Parameters 475
Default 475
Command Mode 475
Applicability 475
Examples 475
bridge forward-time 476
Command Syntax 476
Parameters 476
Default 476
Command Mode 476
Applicability 476
Example 476
show allowed-ethertype 477
Command Syntax 477
Parameters 477
Command Mode 477
Applicability 477
Examples 477
show bridge 478
Command Syntax 478
Parameters 478
Command Mode 478
Applicability 478
Example 478
show interface switchport 479
Command Syntax 479
Parameter 479
Command Mode 479
Applicability 479
Example 479
show mac address-table count bridge 481
Command Syntax 481
Parameter 481
Command Mode 481
Applicability 481
Example 481
show mac address-table bridge 483
Command Syntax 483
Parameter 483
Command Mode 483
Applicability 483
Example 483
show mac-address-table bridge 1 learning 485
Command Syntax 485
Parameter 485

© 2026 IP Infusion Inc. Proprietary

Command Mode 485
Applicability 485
Example 485
switchport 486
Command Syntax 486
Parameters 486
Default 486
Command Mode 486
Applicability 486
Examples 486
switchport allowed ethertype 487
Command Syntax 487
Parameters 487
Default 487
Command Mode 487
Applicability 487
Examples 487
Link Aggregation Commands 488
channel-group mode 489
Command Syntax 489
Parameters 489
Command Mode 489
Applicability 489
Examples 489
clear lacp 491
Command Syntax 491
Parameters 491
Command Mode 491
Applicability 491
Example 491
debug lacp 492
Command Syntax 492
Parameters 492
Command Mode 492
Applicability 492
Example 492
interface po 493
Command Syntax 493
Parameters 493
Default 493
Command Mode 493
Applicability 493
Example 493
interface sa 494
Command Syntax 494
Parameters 494
Default 494

Command Mode 494
Applicability 494
Example 494
lacp destination-mac 495
Command Syntax 495
Parameters 495
Default 495
Command Mode 495
Applicability 495
Example 495
lacp force-up 496
Command Syntax: 496
Parameters 496
Default 496
Command Mode 496
Applicability 496
Example 496
lacp port-priority 497
Command Syntax 497
Parameters 497
Default 497
Command Mode 497
Applicability 497
Example 497
lacp system-priority 498
Command Syntax 498
Parameters 498
Default 498
Command Mode 498
Applicability 498
Example 498
lacp timeout 499
Command Syntax 499
Parameters 499
Default 499
Command Mode 499
Applicability 499
Example 499
port-channel load-balance 500
Command Syntax 500
Parameters 500
Default 500
Command Mode 500
Applicability 500
Example 501
port-channel min-bandwidth - dynamic LAG min-bandwidth 502
Command Syntax 502

© 2026 IP Infusion Inc. Proprietary

Parameters 502
Default 502
Command Mode 502
Applicability 502
Example 502
port-channel min-bandwidth - static LAG min-bandwidth 503
Command Syntax 503
Parameters 503
Default 503
Command Mode 503
Applicability 503
Example 503
port-channel min-links - dynamic LAG min-links 504
Command Syntax 504
Parameters 504
Default 504
Command Mode 504
Applicability 504
Example 504
port-channel min-links - static LAG min-links 505
Command Syntax 505
Parameters 505
Default 505
Command Mode 505
Applicability 505
Example 505
show debugging lacp 506
Command Syntax 506
Parameters 506
Command Mode 506
Applicability 506
Example 506
show etherchannel 507
Command Syntax 507
Parameters 507
Command Mode 507
Applicability 507
Example 507
show lacp-counter 510
Command Syntax 510
Parameters 510
Command Mode 510
Applicability 510
Example 510
show lacp sys-id 511
Command Syntax 511
Parameters 511

© 2026 IP Infusion Inc. Proprietary

Command Mode 511
Applicability 511
Example 511
show port etherchannel 512
Command Syntax 512
Parameters 512
Command Mode 512
Applicability 512
Example 512
show static-channel-group 515
Command Syntax 515
Parameters 515
Command Mode 515
Applicability 515
Examples 515
show static-channel load-balance 516
Command Syntax 516
Parameters 516
Command Mode 516
Applicability 516
Examples 516
snmp restart lacp 517
Command Syntax 517
Parameters 517
Default 517
Command Mode 517
Applicability 517
Examples 517
static-channel-group 518
Command Syntax 518
Parameter 518
Default 518
Command Mode 518
Applicability 518
Example 518
Multi-chassis Link Aggregation Commands 520
clear mcec statistics 521
Command Syntax 521
Parameters 521
Command Mode 521
Applicability 521
Examples 521
debug mcec 522
Command Syntax 522
Parameters 522
Command Mode 522
Applicability 522

Example ... 522
domain-address ... 523
Command Syntax ... 523
Parameters ... 523
Command Mode ... 523
Applicability ... 523
Examples ... 523
domain hello timeout ... 524
Command Syntax ... 524
Parameters ... 524
Command Mode ... 524
Applicability ... 524
Examples ... 524
domain priority ... 525
Command Syntax ... 525
Parameters ... 525
Default ... 525
Command Mode ... 525
Applicability ... 525
Example ... 525
domain-system-number ... 526
Command Syntax ... 526
Parameters ... 526
Command Mode ... 526
Applicability ... 526
Example ... 526
idl-higig ... 527
Command Syntax ... 527
Parameters ... 527
Default ... 527
Command Mode ... 527
Applicability ... 527
Examples ... 527
intra-domain-peer ... 528
Command Syntax ... 528
Parameters ... 528
Command Mode ... 528
Applicability ... 528
Example ... 528
mcec domain configuration ... 529
Command Syntax ... 529
Parameters ... 529
Command Mode ... 529
Applicability ... 529
Examples ... 529
mlag ... 530
Command Syntax ... 530

Parameters 530
Command Mode 530
Applicability 530
Example 530
mode 531
Command Syntax 531
Parameters 531
Default 531
Command Mode 531
Applicability 531
Examples 531
show mcec statistics 532
Command Syntax 532
Parameters 532
Command Mode 532
Applicability 532
Examples 532
show mlag detail 533
Command Syntax 533
Parameters 533
Command Mode 533
Applicability 533
Examples 533
show mlag domain 535
Command Syntax 535
Parameters 535
Command Mode 535
Applicability 535
Examples 535
show mlag stp-synchronization status 538
Command Syntax 538
Parameters 538
Command Mode 538
Applicability 538
Examples 538
show spanning-tree mlag operational-config 539
Command Syntax 539
Parameters 539
Command Mode 539
Applicability 539
Examples 539
show spanning-tree mlag sync-detail 540
Command Syntax 540
Parameters 540
Command Mode 540
Applicability 540
Examples 540

© 2026 IP Infusion Inc. Proprietary

switchover type 541
Command Syntax 541
Parameters 541
Default 541
Command Mode 541
Applicability 541
Examples 541
Traffic Mirroring Commands 542
description 543
Command Syntax 543
Parameters 543
Default 543
Command Mode 543
Applicability 543
Example 543
destination interface 544
Command Syntax 544
Parameters 544
Default 544
Command Mode 544
Applicability 544
Example 544
filter 545
Command Syntax 545
Parameters 545
Default 545
Command Mode 546
Applicability 546
monitor session 547
Command Syntax 547
Parameters 547
Default 547
Command Mode 547
Applicability 547
Examples 547
monitor session shut 548
Command Syntax 548
Parameters 548
Default 548
Command Mode 548
Applicability 548
Examples 548
no shut 549
Command Syntax 549
Parameters 549
Default 549
Command Mode 549

Applicability 549
Example 549
remote destination 550
Command Syntax 550
Parameters 550
Default 550
Command Mode 550
Applicability 550
Example 550
show filter 551
Command Syntax 551
Parameters 551
Command Mode 551
Applicability 551
Example 551
show monitor 552
Command Syntax 552
Parameters 552
Command Mode 552
Applicability 552
Example 552
show monitor running configuration 553
Command Syntax 553
Parameters 553
Command Mode 553
Applicability 553
Example 553
show monitor session 554
Command Syntax 554
Parameters 554
Command Mode 554
Applicability 554
Example 554
shut 556
Command Syntax 556
Parameters 556
Default 556
Command Mode 556
Applicability 556
Example 556
source interface 557
Command Syntax 557
Parameters 557
Default 557
Command Mode 557
Applicability 557
Example 557

source vlan 559
Command Syntax 559
Parameters 559
Default 559
Command Mode 559
Applicability 559
Example 559
VLAN and Private VLAN Commands 560
feature vlan classifier 562
Command Syntax 562
Parameters 562
Default 562
Command Mode 562
Applicability 562
Example 562
global-bridge-vlan-check enable 563
Command Syntax 563
Parameters 563
Default 563
Command Mode 563
Applicability 563
Example 563
private-vlan association 564
Command Syntax 564
Parameters 564
Default 564
Command Mode 564
Applicability 564
Example 564
private-vlan community 565
Command Syntax 565
Parameters 565
Default 565
Command Mode 565
Applicability 565
Example 565
private-vlan isolated 566
Command Syntax 566
Parameters 566
Default 566
Command Mode 566
Applicability 566
Example 566
private-vlan primary 567
Command Syntax 567
Parameters 567
Default 567

Command Mode 567
Applicability 567
Example 567
show dtag vlan 568
Command Syntax 568
Parameters 568
Command Mode 568
Applicability 568
Example 568
show vlan 569
Command Syntax 569
Parameters 569
Command Mode 569
Applicability 569
Example 569
show vlan access-map 571
Command Syntax 571
Parameters 571
Command Mode 571
Applicability 571
Example 571
show vlan brief 572
Command Syntax 572
Parameters 572
Command Mode 572
Applicability 572
Example 572
show vlan classifier 573
Command Syntax 573
Parameters 573
Command Mode 573
Applicability 573
Example 573
show vlan-reservation 575
Command Syntax 575
Parameters 575
Command Mode 575
Applicability 575
Example 575
switchport access 577
Command Syntax 577
Parameter 577
Default 577
Command Mode 577
Applicability 577
Examples 577
switchport hybrid 578

Command Syntax 578
Parameters 578
Default 578
Command Mode 578
Applicability 578
Examples 578
switchport mode 580
Command Syntax 580
Parameters 580
Command Mode 580
Applicability 580
Example 580
switchport mode access ingress-filter 581
Command Syntax 581
Parameters 581
Default 581
Command Mode 581
Applicability 581
Example 581
switchport mode hybrid acceptable-frame-type 582
Command Syntax 582
Parameters 582
Default 582
Command Mode 582
Applicability 582
Example 582
switchport mode hybrid ingress-filter 583
Command Syntax 583
Parameters 583
Default 583
Command Mode 583
Applicability 583
Example 583
switchport mode private-vlan 584
Command Syntax 584
Parameters 584
Default 584
Command Mode 584
Applicability 584
Example 584
switchport mode trunk disable-native-vlan 585
Command Syntax 585
Parameters 585
Command Mode 585
Applicability 585
Example 585
switchport mode (trunk) disable-native-vlan 586

Command Syntax 586
Parameters 586
Command Mode 586
Applicability 586
Example 586
switchport mode trunk ingress-filter 587
Command Syntax 587
Parameters 587
Default 587
Command Mode 587
Applicability 587
Example 587
switchport private-vlan association-trunk 588
Command Syntax 588
Parameters 588
Command Mode 588
Applicability 588
Example 588
switchport mode trunk ingress-filter 589
Command Syntax 589
Parameters 589
Default 589
Command Mode 589
Applicability 589
Example 589
switchport private-vlan host-association 590
Command Syntax 590
Parameters 590
Default 590
Command Mode 590
Applicability 590
Example 590
switchport private-vlan mapping 591
Command Syntax 591
Parameters 591
Default 591
Command Mode 591
Example 591
switchport trunk allowed 592
Command Syntax 592
Parameters 592
Default 592
Command Mode 592
Applicability 592
Examples 593
switchport trunk allowed vlan dtag 594
Command Syntax 594

Parameters 594
Default 594
Command Mode 594
Applicability 594
Example 594
switchport trunk native 595
Command Syntax 595
Default 595
Command Mode 595
Applicability 595
Examples 595
vlan classifier activate 596
Command Syntax 596
Parameters 596
Default 596
Command Mode 596
Applicability 596
Example 596
vlan classifier group 597
Command Syntax 597
Parameters 597
Default 597
Command Mode 597
Applicability 597
Example 597
vlan classifier rule ipv4 598
Command Syntax 598
Parameters 598
Default 598
Command Mode 598
Applicability 598
Example 598
vlan classifier rule mac 599
Command Syntax 599
Parameters 599
Default 599
Command Mode 599
Applicability 599
Example 599
vlan classifier rule proto 600
Command Syntax 600
Default 601
Command Mode 601
Applicability 601
Example 601
vlan database 602
Command Syntax 602

Parameters 602
Default 602
Command Mode 602
Applicability 602
Example 602
vlan database 603
Command Syntax 603
Parameters 603
Default 603
Command Mode 603
Applicability 603
Example 603
vlan VLAN_RANGE bridge 604
Command Syntax 604
Parameters 604
Default 604
Command Mode 604
Applicability 604
Examples 604
vlan VLAN_RANGE type customer 605
Command Syntax 605
Parameters 605
Default 605
Command Mode 605
Applicability 605
Examples 605
vlan VLAN_RANGE type service 606
Command Syntax 606
Parameters 606
Default 606
Command Mode 606
Applicability 607
Examples 607
VLAN Cross-Connect Commands 608
cross-connect 609
Command Syntax 609
Parameters 609
Command Mode 609
Applicability 609
Example 609
disable 610
Command Syntax 610
Parameters 610
Command Mode 610
Applicability 610
Example 610
outer-vlan VLAN_RANGE2 (inner-vlan VLAN_RANGE2 |) 612

Command Syntax 612
Parameters 612
Command Mode 612
Applicability 612
Example 612
show cross-connect 613
Command Syntax 613
Parameters 613
Command Mode 613
Applicability 613
Example 613
802.1x Commands 614
auth-mac 615
Command Syntax 615
Parameters 615
Default 615
Command Mode 615
Applicability 615
Example 615
auth-mac dynamic-vlan-creation 616
Command Syntax 616
Parameters 616
Default 616
Command Mode 616
Applicability 616
Example 616
auth-mac mac-aging 617
Command Syntax 617
Parameters 617
Default 617
Command Mode 617
Applicability 617
Example 617
auth-mac mode 618
Command Syntax 618
Parameters 618
Default 618
Command Mode 618
Applicability 618
Example 618
auth-mac system-auth-ctrl 619
Command Syntax 619
Parameters 619
Default 619
Command Mode 619
Applicability 619
Examples 619

© 2026 IP Infusion Inc. Proprietary

auth-port ... 620
Command Syntax ... 620
Parameters ... 620
Default ... 620
Command Mode ... 620
Applicability ... 620
Examples ... 620
dot1x port-control ... 621
Command Syntax ... 621
Parameters ... 621
Default ... 621
Command Mode ... 621
Applicability ... 621
Examples ... 621
dot1x protocol-version ... 622
Command Syntax ... 622
Parameters ... 622
Default ... 622
Command Mode ... 622
Applicability ... 622
Example ... 622
dot1x quiet-period ... 623
Command Syntax ... 623
Parameter ... 623
Default ... 623
Command Mode ... 623
Applicability ... 623
Example ... 623
dot1x reauthentication ... 624
Command Syntax ... 624
Parameters ... 624
Default ... 624
Command Mode ... 624
Applicability ... 624
Examples ... 624
dot1x reauthMax ... 625
Command Syntax ... 625
Parameter ... 625
Default ... 625
Command Mode ... 625
Applicability ... 625
Examples ... 625
dot1x system-auth-ctrl ... 626
Command Syntax ... 626
Parameters ... 626
Default ... 626
Command Mode ... 626

Applicability ... 626
Example ... 626
dot1x timeout re-authperiod ... 627
Command Syntax ... 627
Parameter ... 627
Default ... 627
Command Mode ... 627
Applicability ... 627
Example ... 627
dot1x timeout server-timeout ... 628
Command Syntax ... 628
Parameter ... 628
Default ... 628
Command Mode ... 628
Applicability ... 628
Examples ... 628
dot1x timeout supp-timeout ... 629
Command Syntax ... 629
Parameter ... 629
Default ... 629
Command Mode ... 629
Applicability ... 629
Example ... 629
dot1x timeout tx-period ... 630
Command Syntax ... 630
Parameter ... 630
Default ... 630
Command Mode ... 630
Applicability ... 630
Examples ... 630
ip radius source-interface ... 631
Command Syntax ... 631
Parameters ... 631
Default ... 631
Command Mode ... 631
Applicability ... 631
Examples ... 631
key-string ... 632
Command Syntax ... 632
Parameter ... 632
Default ... 632
Command Mode ... 632
Applicability ... 632
Examples ... 632
key-string encrypted ... 633
Command Syntax ... 633
Parameter ... 633

Default 633
Command Mode 633
Applicability 633
Examples 633
radius-server dot1x host 634
Command Syntax 634
Parameters 634
Default 634
Command Mode 634
Applicability 634
Examples 634
retransmit 635
Command Syntax 635
Parameter 635
Default 635
Command Mode 635
Applicability 635
Examples 635
show debugging dot1x 636
Command Syntax 636
Parameters 636
Command Mode 636
Applicability 636
Example 636
show dot1x 637
Command Syntax 637
Parameters 637
Command Mode 637
Applicability 637
Applicability 639
Example 639
Layer 2 Control Protocols Tunneling Commands 640
clear l2protocol interface counters 641
Command Syntax 641
Parameters 641
Command Mode 641
Applicability 641
Examples 641
l2protocol 642
Command Syntax 642
Parameters 642
Default 642
Command Mode 642
Applicability 642
Examples 642
l2protocol encapsulation dest-mac 644
Command Syntax 644

Parameters 644
Command Mode 644
Applicability 644
Examples 644
show l2protocol interface counters 646
Command Syntax 646
Parameters 646
Command Mode 646
Applicability 646
Examples 646
show l2protocol processing interface 647
Command Syntax 647
Parameters 647
Command Mode 647
Applicability 647
Examples 647
Provider Bridging Commands 648
bridge protocol provider-mstp 649
Command Syntax 649
Command Mode 649
Applicability 649
Example 649
bridge protocol provider-rstp 650
Command Syntax 650
Parameters 650
Command Mode 650
Applicability 650
Example 650
cvlan registration table 651
Command Syntax 651
Parameters 651
Command Mode 651
Applicability 651
Example 651
cvlan svlan 652
Command Syntax 652
Parameters 652
Command Mode 652
Applicability 652
Example 653
dot1ad ethertype 654
Command Syntax 654
Parameters 654
Default 654
Command Mode 654
Applicability 654
Examples 654

show cvlan registration table 655
Command Syntax 655
Parameters 655
Command Mode 655
Applicability 655
Example 655
switchport customer-edge 656
Command Syntax 656
Parameters 656
Command Mode 656
Applicability 656
Examples 656
switchport customer-edge hybrid 657
Command Syntax 657
Parameters 657
Command Mode 657
Applicability 657
Examples 657
switchport customer-edge trunk 658
Command Syntax 658
Parameters 658
Command Mode 658
Applicability 658
Examples 658
switchport customer-edge vlan registration 659
Command Syntax 659
Parameters 659
Command Mode 659
Applicability 659
Example 659
switchport customer-network allowed vlan 660
Customer-Network Port Command Syntax 660
Parameters 660
Command Mode 660
Applicability 660
Examples 660
switchport customer-network vlan 661
Command Syntax 661
Parameters 661
Default 661
Command Mode 661
Applicability 661
Examples 661
switchport mode 662
Command Syntax 662
Parameters 662
Command Mode 662

Applicability 662
Example 662
switchport mode customer-edge 663
Command Syntax 663
Parameters 663
Command Mode 663
Applicability 663
Example 663
switchport mode customer-edge hybrid acceptable-frame-type 664
Command Syntax 664
Parameters 664
Command Mode 664
Applicability 664
Example 664
switchport provider-network 665
Command Syntax 665
Parameters 665
Command Mode 665
Applicability 665
Examples 665
switchport provider-network isolated-vlan 666
Command Syntax 666
Parameters 666
Command Mode 666
Applicability 666
Example 666
vlan type 667
Command Syntax 667
Parameters 667
Command Mode 667
Applicability 667
Examples 667
vlan type customer 668
Command Syntax 668
Parameters 668
Command Mode 668
Applicability 668
Examples 668
Port Security Commands 669
port-security 669
Command Syntax 669
Parameters 669
Default 669
Command Mode 669
Applicability 669
Example 669
show port-security 669

Command Syntax 670
Parameters 670
Default 670
Command Mode 670
Applicability 670
Example 670
switchport port-security 670
Command Syntax 671
Parameters 671
Default 671
Command Mode 671
Applicability 671
Example 671
switchport port-security logging 671
Command Syntax 671
Parameters 671
Default 672
Command Mode 672
Applicability 672
Example 672
switchport port-security mac-address 672
Command Syntax 672
Parameters 672
Default 673
Command Mode 673
Applicability 673
Example 673
switchport port-security maximum 673
Command Syntax 673
Parameters 673
Default 673
Command Mode 674
Applicability 674
Example 674
Link Layer Discovery Protocol Commands 675
lldp debug 676
Command Syntax 676
Parameters 676
Command Mode 676
Examples 676
lldp (disable|enable) default-agent 677
Command Syntax 677
Parameters 677
Command Mode 677
Applicability 677
Example 677
lldp ip 678

Command Syntax 678
Parameters 678
Command Mode 678
Examples 678
lldp run 679
Command Syntax 679
Parameters 679
Command Mode 679
Example 679
lldp tlv 680
Command Syntax 680
Parameters 680
Command Mode 680
Example 680
lldp tlv-select 681
Command Syntax 681
Parameters 681
Command Mode 682
Example 682
set lldp chassis-id-tlv 683
Command Syntax 683
Parameters 683
Command Mode 683
Examples 683
set lldp disable 684
Command Syntax 684
Parameters 684
Command Mode 684
Examples 684
set lldp enable 685
Command Syntax 685
Parameters 685
Default 685
Command Mode 685
Examples 685
set lldp locally-assigned 686
Command Syntax 686
Parameters 686
Command Mode 686
Examples 686
set lldp management-address-tlv 687
Command Syntax 687
Parameters 687
Command Mode 687
Examples 687
set lldp msg-tx-hold 688
Command Syntax 688

Parameters 688
Default 688
Command Mode 688
Examples 688
set lldp timer 689
Command Syntax 689
Parameters 689
Default 689
Command Mode 689
Examples 689
set lldp too-many-neighbors 690
Command Syntax 690
Parameters 690
Default 690
Command Mode 690
Examples 690
show lldp 691
Command Syntax 691
Parameters 691
Command Mode 691
Example 691
snmp restart lldp 692
Command Syntax 692
Parameters 692
Command Mode 692
Examples 692
Unidirectional Link Detection Commands 693
udld 694
Command Syntax 694
Parameters 694
Default 694
Command Mode 694
Applicability 694
Examples 694
udld message-time 695
Command Syntax 695
Parameters 695
Default 695
Command Mode 695
Applicability 695
Examples 695
udld mode 696
Command Syntax 696
Parameters 696
Default 696
Command Mode 696
Applicability 696

© 2026 IP Infusion Inc. Proprietary

Examples 696
udld state 697
Command Syntax 697
Parameters 697
Default 697
Command Mode 697
Applicability 697
Examples 697
show udld 698
Command Syntax 698
Parameters 698
Command Mode 698
Applicability 698
Examples 698
show udld interface 699
Command Syntax 699
Parameters 699
Command Mode 699
Applicability 699
Examples 699
Spanning Tree Protocol Commands 700
bridge cisco-interoperability 702
Command Syntax 702
Parameters 702
Default 702
Command Mode 702
Applicability 702
Examples 702
bridge-group instance 703
Command Syntax 703
Parameters 703
Default 703
Command Mode 703
Applicability 703
Examples 703
bridge-group instance path-cost 704
Command Syntax 704
Parameters 704
Default 704
Command Mode 704
Applicability 704
Example 704
bridge-group instance priority 705
Command Syntax 705
Parameters 705
Default 705
Command Mode 705

Applicability 705
Example 705
bridge-group path-cost 706
Command Syntax 706
Parameters 706
Default 706
Command Mode 706
Applicability 706
Examples 706
bridge-group priority 707
Command Syntax 707
Parameters 707
Default 707
Command Mode 707
Applicability 707
Example 707
bridge-group spanning-tree 708
Command Syntax 708
Parameters 708
Default 708
Command Mode 708
Applicability 708
Example 708
bridge instance 709
Command Syntax 709
Parameters 709
Default 709
Command Mode 709
Applicability 709
Examples 709
bridge instance priority 710
Command Syntax 710
Parameters 710
Default 710
Command Mode 710
Applicability 710
Examples 710
bridge instance vlan 711
Command Syntax 711
Parameters 711
Default 711
Command Mode 711
Applicability 711
Examples 711
bridge multiple-spanning-tree 713
Command Syntax 713
Parameters 713

Default 713
Command Mode 713
Applicability 713
Examples 713
bridge protocol ieee 714
Command Syntax 714
Parameters 714
Default 714
Command Mode 714
Applicability 714
Example 714
bridge protocol mstp 715
Command Syntax 715
Parameters 715
Default 715
Command Mode 715
Applicability 715
Examples 715
bridge protocol rstp 716
Command Syntax 716
Parameters 716
Default 716
Command Mode 716
Applicability 716
Examples 716
bridge rapid-spanning-tree 717
Command Syntax 717
Parameters 717
Default 717
Command Mode 717
Applicability 717
Examples 717
bridge region 718
Command Syntax 718
Parameters 718
Default 718
Command Mode 718
Applicability 718
Examples 718
bridge revision 719
Command Syntax 719
Parameters 719
Default 719
Command Mode 719
Applicability 719
Example 719
bridge spanning-tree 720

Command Syntax 720
Parameters 720
Default 720
Command Mode 720
Applicability 720
Examples 720
bridge spanning-tree errdisable-timeout 721
Command Syntax 721
Parameters 721
Default 721
Command Mode 721
Applicability 721
Examples 721
bridge spanning-tree force-version 722
Command Syntax 722
Parameters 722
Default 722
Command Mode 722
Applicability 722
Examples 722
bridge spanning-tree pathcost 723
Command Syntax 723
Parameters 723
Default 723
Command Mode 723
Applicability 723
Examples 723
bridge te-msti 724
Command Syntax 724
Parameters 724
Default 724
Command Mode 724
Applicability 724
Examples 724
bridge te-msti vlan 725
Command Syntax 725
Parameters 725
Default 725
Command Mode 725
Applicability 725
Examples 725
clear spanning-tree detected protocols 727
Command Syntax 727
Parameters 727
Command Mode 727
Applicability 727
Example 727

© 2026 IP Infusion Inc. Proprietary

clear spanning-tree statistics 728
Command Syntax 728
Parameters 728
Command Mode 728
Applicability 728
Example 728
customer-spanning-tree customer-edge priority 729
Command Syntax 729
Parameters 729
Default 729
Command Mode 729
Applicability 729
Example 729
customer-spanning-tree customer-edge path-cost 730
Command Syntax 730
Parameters 730
Default 730
Command Mode 730
Applicability 730
Example 730
customer-spanning-tree hello-time 731
Command Syntax 731
Parameters 731
Default 731
Command Mode 731
Applicability 731
Examples 731
customer-spanning-tree max-age 732
Command Syntax 732
Parameters 732
Default 732
Command Mode 732
Applicability 732
Examples 732
customer-spanning-tree priority 733
Command Syntax 733
Parameters 733
Default 733
Command Mode 733
Applicability 733
Examples 733
customer-spanning-tree provider-edge path-cost 734
Command Syntax 734
Parameters 734
Default 734
Command Mode 734
Applicability 734

Examples 734
customer-spanning-tree provider-edge priority 735
Command Syntax 735
Parameters 735
Default 735
Command Mode 735
Applicability 735
Example 735
customer-spanning-tree transmit-holdcount 736
Command Syntax 736
Parameters 736
Default 736
Command Mode 736
Applicability 736
Examples 736
debug mstp 737
Command Syntax 737
Parameters 737
Command Mode 737
Applicability 738
Examples 738
show debugging mstp 739
Command Syntax 739
Parameters 739
Command Mode 739
Applicability 739
Examples 739
show spanning-tree 740
Command Syntax 740
Parameters 740
Command Mode 741
Applicability 741
Example 741
show spanning-tree mst 744
Command Syntax 744
Parameters 744
Command Mode 744
Applicability 744
Examples 744
show spanning-tree statistics 746
Command Syntax 746
Command Mode 746
Applicability 746
Example 746
snmp restart mstp 748
Command Syntax 748
Parameters 748

© 2026 IP Infusion Inc. Proprietary

Default 748
Command Mode 748
Applicability 748
Example 748
spanning-tree autoedge 749
Command Syntax 749
Default 749
Parameters 749
Command Mode 749
Applicability 749
Example 749
spanning-tree edgeport 750
Command Syntax 750
Default 750
Parameters 750
Command Mode 750
Applicability 750
Example 750
spanning-tree guard 751
Command Syntax 751
Parameters 751
Default 751
Command Mode 751
Applicability 751
Example 751
spanning-tree instance restricted-role 752
Command Syntax 752
Parameters 752
Default 752
Command Mode 752
Applicability 752
Example 752
spanning-tree instance restricted-tcn 753
Command Syntax 753
Parameters 753
Default 753
Command Mode 753
Applicability 753
Example 753
spanning-tree link-type 754
Command Syntax 754
Parameters 754
Default 754
Command Mode 754
Applicability 754
Examples 754
spanning-tree mst configuration 755

Command Syntax 755
Parameters 755
Default 755
Command Mode 755
Applicability 755
Examples 755
spanning-tree restricted-domain-role 756
Command Syntax 756
Parameters 756
Default 756
Command Mode 756
Applicability 756
Example 756
spanning-tree restricted-role 757
Command Syntax 757
Parameters 757
Default 757
Command Mode 757
Applicability 757
Example 757
spanning-tree restricted-tcn 758
Command Syntax 758
Parameters 758
Default 758
Command Mode 758
Applicability 758
Example 758
spanning-tree te-msti configuration 759
Command Syntax 759
Parameters 759
Default 759
Command Mode 759
Applicability 759
Examples 759
Errdisable Commands 760
errdisable cause 761
Command Syntax 761
Parameters 761
Default 761
Command Mode 761
Applicability 761
Examples 762
errdisable link-flap-setting 763
Command Syntax 763
Default 763
Command Mode 763
Applicability 763

Examples 763
errdisable mac-move-limit 764
Command Syntax 764
Parameters 764
Default 764
Command Mode 764
Applicability 764
Examples 764
errdisable storm-control 765
Command Syntax 765
Parameters 765
Default 765
Command Mode 765
Applicability 765
Examples 766
errdisable timeout 767
Command Syntax 767
Parameters 767
Default 767
Command Mode 767
Applicability 767
Examples 767
link-flap errdisable 768
Command Syntax 768
Parameter 768
Default 768
Command Mode 768
Applicability 768
Example 768
mac-move-limit priority 769
Command Syntax 769
Parameters 769
Default 769
Command Mode 769
Applicability 769
Example 769
show errdisable details 770
Command Syntax 770
Parameters 770
Default 770
Command Mode 770
Applicability 770
Example 770
show interface errdisable status 771
Command Syntax 771
Parameters 771
Default 771

Command Mode 771
Applicability 771
Example 771
RPVST+ Commands 772
bridge-group vlan 773
Command Syntax 773
Parameters 773
Command Mode 773
Applicability 773
Examples 773
bridge protocol rpvst+ 774
Command Syntax 774
Parameter 774
Command Mode 774
Applicability 774
Example 774
bridge rapid-pervlan-spanning-tree 775
Command Syntax 775
Parameters 775
Default 775
Command Mode 775
Applicability 775
Examples 775
bridge vlan 776
Command Syntax 776
Parameters 776
Command Mode 776
Applicability 776
Examples 776
bridge vlan priority 777
Command Syntax 777
Parameters 777
Default 777
Command Mode 777
Applicability 777
Examples 777
show spanning-tree rpvst+ 778
Command Syntax 778
Parameters 778
Command Mode 778
Applicability 778
Example 778
spanning-tree rpvst+ configuration 782
Command Syntax 782
Parameters 782
Command Mode 782
Applicability 782

Example 782
spanning-tree vlan restricted-role 783
Command Syntax 783
Parameters 783
Default 783
Command Mode 783
Applicability 783
Example 783
spanning-tree vlan restricted-tcn 784
Command Syntax 784
Parameters 784
Default 784
Command Mode 784
Applicability 784
Example 784

Cross-Connect (XC) Configuration 785

Cross-Connect (XC) Resiliency 786
Topology 786
LFPT (Link-Fault-Pass-Through) 786
Revertive 786
Node-1 786
Node-2 787
Node-3 788
Node-4 789
Validation 790
Cross-connect using Dynamic LAG on Node-1 790
Cross-connect using Dynamic LAG on Node-2 791
Cross-connect using Dynamic LAG on Node-3 792
Cross-connect using Dynamic LAG on Node-4 793
Disable the Cross-connect on Node-1 793
Validation 793
Validation 794
VLAN Cross-Connect (XC) 795
Overview 795
Topology 795
Configuration - Single-tagged VLAN 796
Validation 798
Double-tagged VLAN 799
TOR1 799
TOR2 799
SW2 800
SW1 801
Validation 801
Cross-Connect (XC) 803
Topology 803
Configuration using Topology-1 803

R1 803
XC Node-1 804
Xc Node-2 804
R2 805
Validation 805
Configuration using Topology-2 810
Configuration on R1 Node 810
Configuring Cross connect using dynamic lag interfaces on XC_node1 810
Configuring Cross connect using dynamic lag interfaces on XC_node2 811
Validation 811
Configuring Cross connect using Static lag interfaces 812
Configuration on R1 Node 812
Configuring Cross connect using static lag interfaces on XC_node1 812
Configuring Cross connect using static lag interfaces on XC_node2 813
Validation 814
CFM over xConnect Configuration 816
Topology 816
Configuration 816
Node-1 816
Node-2 818
Node-3 819
Node-4 820
Validation 821
Node-1 821
Node-3 822

Data Center Bridging Configuration 823

Data Center Bridging 824
Overview 824
Feature Characteristics 824
Protocols Supported for DCBX 824
Priority-based Flow Control (PFC) 824
DCBX Configuration for PFC via LLDP 825
Configuration 825
Priority-based Flow Control Configuration 826
Configuring a Bridge and Interface for PFC 827
Configuring Priorities and Link Delay Allowance for PFC 827
Validation 828
PFC with QoS Configuration 829
Overview 829
PFC Configuration for Congestion on Device 829
PFC Configuration for Congestion on Peer Device 831
PFC Configuration for Ingress Service Policy Map 834
PFC Deadlock Detection and Recovery 840
Overview 840
Configuring PFC Deadlock Detection and Recovery 842
CLI Commands 849

© 2026 IP Infusion Inc. Proprietary

Implementation Examples 853
Glossary 854
PFC Frames and ECN Packets Monitoring 855
Overview 855
Configuring PFC Frames and ECN Packets Monitoring 855
Sample Show Running Configuration on Switch 1 859
Validation 862
CLI Commands 868
Glossary 869
Data Centre Bridging Capability Exchange Configuration 870
Overview 870
Benefits 870
DCBX Configuration for PFC via LLDP 870
Configuration 870
Validation 871

Data Center Bridging Command Reference 874

Data Center Bridge Commands 875
data-center-bridging 876
Command Syntax 876
Parameters 876
Default 876
Command Mode 876
Applicability 876
Example 876
show data-center-bridging 877
Command Syntax 877
Parameters 877
Default 877
Command Mode 877
Applicability 877
Example 877
Priority-based Flow Control Commands 879
clear priority-flow-control deadlock-status 880
Command Syntax 880
Parameters 880
Default 880
Command Mode 880
Applicability 880
Example 880
monitor ecn 881
Command Syntax 881
Parameters 881
Default 881
Command Mode 881
Applicability 881
Example 881

monitor pfc ... 882
Command Syntax ... 882
Parameters ... 882
Default ... 882
Command Mode ... 882
Applicability ... 882
Example ... 882
priority-flow-control accept-peer-config ... 883
Command Syntax ... 883
Parameters ... 883
Default ... 883
Command Mode ... 883
Applicability ... 883
Example ... 883
priority-flow-control advertise-local-config ... 884
Command Syntax ... 884
Parameters ... 884
Default ... 884
Command Mode ... 884
Applicability ... 884
Example ... 884
priority-flow-control cap ... 885
Command Syntax ... 885
Parameters ... 885
Default ... 885
Command Mode ... 885
Applicability ... 885
Example ... 885
priority-flow-control deadlock manual-recovery ... 886
Command Syntax ... 886
Parameters ... 886
Default ... 886
Command Mode ... 886
Applicability ... 886
Example ... 886
priority-flow-control enable ... 887
Command Syntax ... 887
Parameters ... 887
Default ... 887
Command Mode ... 887
Applicability ... 887
Example ... 887
priority-flow-control enable priority ... 888
Command Syntax ... 888
Parameters ... 888
Default ... 888
Command Mode ... 888

Applicability ... 888
Example ... 888
priority-flow-control link-delay-allowance ... 889
Command Syntax ... 889
Parameters ... 889
Default ... 889
Command Mode ... 889
Applicability ... 889
Example ... 889
priority-flow-control mode ... 890
Command Syntax ... 890
Parameters ... 890
Default ... 890
Command Mode ... 890
Applicability ... 890
Example ... 890
priority-flow-control deadlock recovery-action drop ... 891
Command Syntax ... 891
Parameters ... 891
Default ... 891
Command Mode ... 891
Applicability ... 891
Example ... 891
priority-flow-control deadlock recovery-mode timer ... 892
Command Syntax ... 892
Parameters ... 892
Default ... 892
Command Mode ... 892
Applicability ... 892
Example ... 892
priority-flow-control deadlock recovery-mode pfc-state-xon ... 893
Command Syntax ... 893
Parameters ... 893
Default ... 893
Command Mode ... 893
Applicability ... 893
Example ... 893
show priority-flow-control details ... 894
Command Syntax ... 894
Parameters ... 894
Default ... 894
Command Mode ... 894
Applicability ... 894
Example ... 894
show priority-flow-control statistics ... 896
Command Syntax ... 896
Parameters ... 896

Default 896
Command Mode 896
Applicability 896
Example 896
show priority-flow-control deadlock-status 897
Command Syntax 897
Parameters 897
Default 897
Command Mode 897
Applicability 897
Example 897

PREFACE

About this Guide

This guide describes how to configure Layer 2 in OcNOS.

Audience

This guide is intended for network administrators and other engineering professionals who configure OcNOS.

Conventions

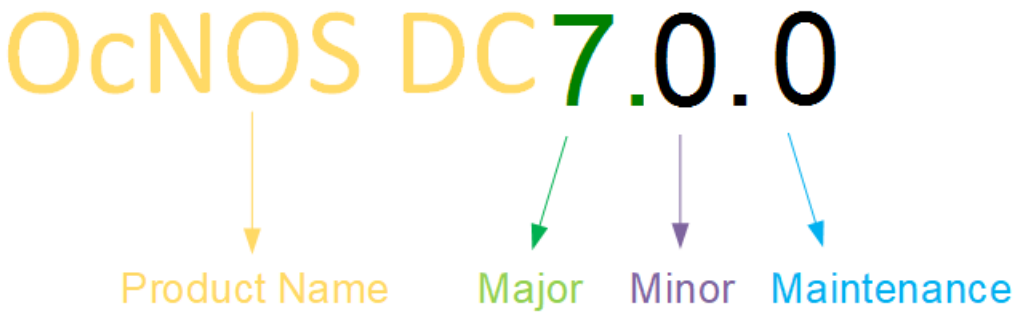
The Table 1 table shows the conventions used in this guide.

Table 1. Conventions

Convention	Description
Italics	Emphasized terms; titles of books
Note:	Special instructions, suggestions, or warnings
`monospaced type`	Code elements such as commands, parameters, files, and directories

IP Infusion Product Release Version

Each integer in release numbers indicates Major, Minor, and Maintenance release versions. Build numbers that follow the release numbers are for internal tracking and verification of the software build process and are visible to customers as part of the software version number.



Product Name: IP Infusion Product Family

Major Version: New customer-facing functionality that represents a significant change to the code base; including a significant marketing change or direction in the product.

Minor Version: Enhancements or extensions to existing features, changes to address external needs, or internal improvements to satisfy new sales regions or marketing initiatives.

Maintenance Version: A collection of product bugs or issues usually scheduled every 30 or 60 days, based on the number of issues.

Related Documentation

For information about installing OcNOS, see the *Installation Guide* for your platform.

Feature Availability

Each OcNOS SKU contains a set of supported features. For a list of available features based on the SKU that you purchased, refer to the *Feature Matrix* .

Migration Guide

Check the *Migration Guide* for necessary configuration changes before migrating from one version of OcNOS to another.

IP Maestro Support

Monitor devices running OcNOS Release 6.3.4-70 and above using IP Maestro software.

Technical Support

IP Infusion maintains an online technical support site that provides a variety of technical support programs for licensed OcNOS customers at the Technical Assistance Center.

Customers and partners enjoy full access to the support website. The site allows customers and partners to open technical support calls, update open calls with new information, and review the status of open or closed calls. The password-protected site includes technical documentation, Release Notes, and descriptions of service offerings.

Technical Sales

Contact the IP Infusion sales representative for more information about the OcNOS solution.

Technical Documentation

For core commands and configuration procedures, visit: Product Documentation.

For training videos, visit: OcNOS Free Training Videos.

For a list of supported platforms and SKUs of OcNOS features, refer to the OcNOS Feature Matrix.

© 2026 IP Infusion Inc. Proprietary

Documentation Disclaimer

The global documentation site is evolving to provide an enhanced website user experience for select topics included in this release. Some guides are now available outside the existing documentation library and can be accessed directly from custom documentation landing pages. These guides offer robust in-built search functionality.

For the latest documentation, visit the product-specific documentation landing page and select the relevant guide.

Comments

If you have comments, or need to report a problem with the content, contact techpubs@ipinfusion.com.

© 2026 IP Infusion Inc. Proprietary

Command Line Interface

This chapter introduces the OcNOS Command Line Interface (CLI) and how to use its features.

Overview

You use the CLI to configure, monitor, and maintain OcNOS devices. The CLI is text-based and each command is usually associated with a specific task.

You can give the commands described in this manual locally from the console of a device running OcNOS or remotely from a terminal emulator such as putty or xterm. You can also use the commands in scripts to automate configuration tasks.

Chapter Organization

The chapters in command references are organized as described in Command Description Format (page 68).

The chapters in configuration guides are organized into these major sections:

- An overview that explains a configuration in words
- Topology with a diagram that shows the devices and connections used in the configuration
- Configuration steps in a table for each device where the left-hand side shows the commands you enter and the right-hand side explains the actions that the commands perform
- Validation which shows commands and their output that verify the configuration

Command Line Interface Help

You access the CLI help by entering a full or partial command string and a question mark “?”. The CLI displays the command keywords or parameters along with a short description. For example, at the CLI command prompt, type:

```
> show ?
```

The CLI displays this keyword list with short descriptions for each keyword:

```
show ?
  application-priority            Application Priority
  arp                             Internet Protocol (IP)
  bfd                             Bidirectional Forwarding Detection (BFD)
  bgp                             Border Gateway Protocol (BGP)
  bi-lsp                          Bi-directional lsp status and configuration
  bridge                          Bridge group commands
  ce-vlan                         COS Preservation for Customer Edge VLAN
  class-map                       Class map entry
  cli                             Show CLI tree of current mode
  clns                            Connectionless-Mode Network Service (CLNS)
  control-adjacency               Control Adjacency status and configuration
  control-channel                 Control Channel status and configuration
  cspf                            CSPF Information
  customer                        Display Customer spanning-tree
  cvlan                           Display CVLAN information
  debugging                       Debugging functions
  etherchannel                    LACP etherchannel
```

© 2026 IP Infusion Inc. Proprietary

```
  ethernet                        Layer-2
...
```

If you type the ? in the middle of a keyword, the CLI displays help for that keyword only.

```
> show de?
debugging  Debugging functions
```

If you type the ? in the middle of a keyword, but the incomplete keyword matches several other keywords, OcNOS displays help for all matching keywords.

```
> show i? (CLI does not display the question mark).
interface  Interface status and configuration
ip         IP information
isis       ISIS information
```

Command Completion

The CLI can complete the spelling of a command or a parameter. Begin typing the command or parameter and then press the tab key. For example, at the CLI command prompt type **sh**:

```
> sh
```

Press the tab key. The CLI displays:

```
> show
```

If the spelling of a command or parameter is ambiguous, the CLI displays the choices that match the abbreviation. Type **show i** and press the tab key. The CLI displays:

```
> show i
  interface  ip         ipv6       isis
> show i
```

The CLI displays the **interface** and **ip** keywords. Type **n** to select **interface** and press the tab key. The CLI displays:

```
> show in
> show interface
```

Type ? and the CLI displays the list of parameters for the **show interface** command.

```
> show interface
  IFNAME  Interface name
  |       Output modifiers
  >       Output redirection
  <cr>
```

The CLI displays the only parameter associated with this command, the **IFNAME** parameter.

Command Abbreviations

The CLI accepts abbreviations that uniquely identify a keyword in commands. For example:

```
> sh int xe0
```

is an abbreviation for:

```
> show interface xe0
```

© 2026 IP Infusion Inc. Proprietary

Command Line Errors

Any unknown spelling causes the CLI to display the error **`Unrecognized command`** in response to the ?. The CLI displays the command again as last entered.

```
> show dd?
% Unrecognized command
> show dd
```

When you press the Enter key after typing an invalid command, the CLI displays:

```
(config)#router ospf here
                        ^
% Invalid input detected at '^' marker.
```

where the ^ points to the first character in error in the command.

If a command is incomplete, the CLI displays the following message:

```
> show
% Incomplete command.
```

Some commands are too long for the display line and can wrap mid-parameter or mid-keyword, as shown below. This does *not* cause an error and the command performs as expected:

```
area 10.10.0.18 virtual-link 10.10.0.19 authentication-key 57393
```

Command Negation

Many commands have a **`no`** form that resets a feature to its default value or disables the feature. For example:

- The **`ip address`** command assigns an IPv4 address to an interface
- The **`no ip address`** command removes an IPv4 address from an interface

Syntax Conventions

Table 2 describes the conventions used to represent command syntax in this reference.

Table 2. Syntax conventions

Convention	Description	Example
`monospaced font`	Command strings entered on a command line	**`show ip ospf`**
`lowercase`	Keywords that you enter exactly as shown in the command syntax.	`show ip ospf`
`UPPERCASE`	See Variable Placeholders (page 67)	`IFNAME`
`()`	Optional parameters, from which you must select one. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>)`
`()`	Optional parameters, from which you select one or none. Vertical bars delimit the	`(A.B.C.D|<0-4294967295>|)`

© 2026 IP Infusion Inc. Proprietary

Table 2. Syntax conventions (continued)

Convention	Description	Example
	selections. Do not enter the parentheses or vertical bars as part of the command.	
`()`	Optional parameter which you can specify or omit. Do not enter the parentheses or vertical bar as part of the command.	`(IFNAME|)`
`{}`	Optional parameters, from which you must select one or more. Vertical bars delimit the selections. Do not enter the braces or vertical bars as part of the command.	`{intra-area <1-255>|inter-area <1-255>|external <1-255>}`
`[]`	Optional parameters, from which you select zero or more. Vertical bars delimit the selections. Do not enter the brackets or vertical bars as part of the command.	`[<1-65535>|AA:NN|internet|local-AS|no-advertise|no-export]`
`?`	Nonrepeatable parameter. The parameter that follows a question mark can only appear once in a command string. Do not enter the question mark as part of the command.	`?route-map WORD`
`.`	Repeatable parameter. The parameter that follows a period can be repeated more than once. Do not enter the period as part of the command.	`set as-path prepend .<1-65535>`

Variable Placeholders

Table 3 shows the tokens used in command syntax use to represent variables for which you supply a value.

Table 3. Variable placeholders

Token	Description
`WORD`	A contiguous text string (excluding spaces)
`LINE`	A text string, including spaces; no other parameters can follow this parameter
`IFNAME`	Interface name whose format varies depending on the platform; examples are: **`eth0`**, **`Ethernet0`**, **`ethernet0`**, **`xe0`**
`A.B.C.D`	IPv4 address
`A.B.C.D/M`	IPv4 address and mask/prefix
`X:X::X:X`	IPv6 address
`X:X::X:X/M`	IPv6 address and mask/prefix
`HH:MM:SS`	Time format
`AA:NN`	BGP community value

© 2026 IP Infusion Inc. Proprietary

Table 3. Variable placeholders (continued)

Token	Description
XX:XX:XX:XX:XX:XX	MAC address
<1-5> <1-65535> <0-2147483647> <0-4294967295>	Numeric range

Command Description Format

The Table 4 table explains the sections used to describe each command in this reference.

Table 4. Command descriptions

Section	Description
Command Name	The name of the command, followed by what the command does and when should it be used
Command Syntax	The syntax of the command
Parameters	Parameters and options for the command
Default	The state before the command is executed
Command Mode	The mode in which the command runs; see Command Modes (page 72)
Applicability	The command introduced in a specific release version and modified or updated in subsequent versions.
Example	An example of the command being executed

Keyboard Operations

The Table 5 table lists the operations you can perform from the keyboard.

Table 5. Keyboard operations

Key combination	Operation
Left arrow or Ctrl+b	Moves one character to the left. When a command extends beyond a single line, you can press left arrow or Ctrl+b repeatedly to scroll toward the beginning of the line, or you can press Ctrl+a to go directly to the beginning of the line.
Right arrow or Ctrl-f	Moves one character to the right. When a command extends beyond a single line, you can press right arrow or Ctrl+f repeatedly to scroll toward the end of the line, or you can press Ctrl+e to go directly to the end of the line.
Esc, b	Moves back one word
Esc, f	Moves forward one word
Ctrl+e	Moves to end of the line

© 2026 IP Infusion Inc. Proprietary

Table 5. Keyboard operations (continued)

Key combination	Operation
Ctrl+a	Moves to the beginning of the line
Ctrl+u	Deletes the line
Ctrl+w	Deletes from the cursor to the previous whitespace
Alt+d	Deletes the current word
Ctrl+k	Deletes from the cursor to the end of line
Ctrl+y	Pastes text previously deleted with Ctrl+k, Alt+d, Ctrl+w, or Ctrl+u at the cursor
Ctrl+t	Transposes the current character with the previous character
Ctrl+c	Ignores the current line and redisplays the command prompt
Ctrl+z	Ends configuration mode and returns to exec mode
Ctrl+l	Clears the screen
Up Arrow or Ctrl+p	Scroll backward through command history
Down Arrow or Ctrl+n	Scroll forward through command history

Show Command Modifiers

Note: The show command output included in the guides is for illustration purposes only. Based on the combination of features enabled and ongoing enhancements made to the commands, the output for these commands may vary. For instance, the actual command output may differ depending on the software version, configuration, and platform. Field names, values, and formats are subject to change.

You can use two tokens to modify the output of a **show** command. Enter a question mark to display these tokens:

```
# show users ?
  | Output modifiers
  > Output redirection
```

You can type the | (vertical bar character) to use output modifiers. For example:

```
> show rsvp | ?
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  last      Last few lines
  redirect  Redirect output
```

Begin Modifier

The **begin** modifier displays the output beginning with the first line that contains the input string (everything typed after the **begin** keyword). For example:

```
# show running-config | begin xe1
...skipping
interface xe1
ipv6 address fe80::204:75ff:fee6:5393/64
!
interface xe2
```

```
ipv6 address fe80::20d:56ff:fe96:725a/64
!
line con 0
login
!
end
```

You can specify a regular expression after the **begin** keyword, This example begins the output at a line with either “xe2” or “xe4”:

```
# show running-config | begin xe[2-4]

...skipping
interface xe2
 shutdown
!
interface xe4
 shutdown
!
interface svlan0.1
 no shutdown
!
route-map myroute permit 2
!
route-map mymap1 permit 10
!
route-map rmap1 permit 2
!
line con 0
 login
line vty 0 4
 login
!
end
```

Include Modifier

The **include** modifier includes only those lines of output that contain the input string. In the output below, all lines containing the word “input” are included:

```
# show interface xe1 | include input
    input packets 80434552, bytes 2147483647, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 1, missed 0
```

You can specify a regular expression after the **include** keyword. This examples includes all lines with “input” or “output”:

```
#show interface xe0 | include (in|out)put
    input packets 597058, bytes 338081476, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 613147, bytes 126055987, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
```

Exclude Modifier

The **exclude** modifier excludes all lines of output that contain the input string. In the following output example, all lines containing the word “input” are excluded:

```
# show interface xe1 | exclude input
Interface xe1
  Scope: both
  Hardware is Ethernet, address is 0004.75e6.5393
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
```

```
  VRF Binding: Not bound
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet6 fe80::204:75ff:fee6:5393/64
    output packets 4438, bytes 394940, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

You can specify a regular expression after the **exclude** keyword. This example excludes lines with “output” or “input”:

```
show interface xe0 | exclude (in|out)put
Interface xe0
  Scope: both
  Hardware is Ethernet  Current HW addr: 001b.2139.6c4a
  Physical:001b.2139.6c4a  Logical:(not set)
  index 2 metric 1 mtu 1500 duplex-full arp ageing timeout 3000
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 100m
  DHCP client is disabled.
  inet 10.1.2.173/24 broadcast 10.1.2.255
  VRRP Master of :  VRRP is not configured on this interface.
  inet6 fe80::21b:21ff:fe39:6c4a/64
    collisions 0
```

Redirect Modifier

The **redirect** modifier writes the output into a file. The output is not displayed.

```
# show cli history | redirect /var/frame.txt
```

The output redirection token (>) does the same thing:

```
# show cli history >/var/frame.txt
```

Last Modifier

The **last** modifier displays the output of last few number of lines (As per the user input). The last number ranges from 1 to 9999.

For example:

```
#show running-config | last 10
```

String Parameters

The restrictions in Table 6 apply for all string parameters used in OcNOS commands, unless some other restrictions are noted for a particular command.

Table 6. String parameter restrictions

Restriction	Description
Input length	1965 characters or less
Restricted special characters	“?”, “,”, “>”, “|”, and “=” The “|” character is allowed only for the **description** command in interface mode.

Command Modes

Commands are grouped into modes arranged in a hierarchy. Each mode has its own set of commands. The table below lists the command modes common to all protocols.

Table 7. Common Command Modes

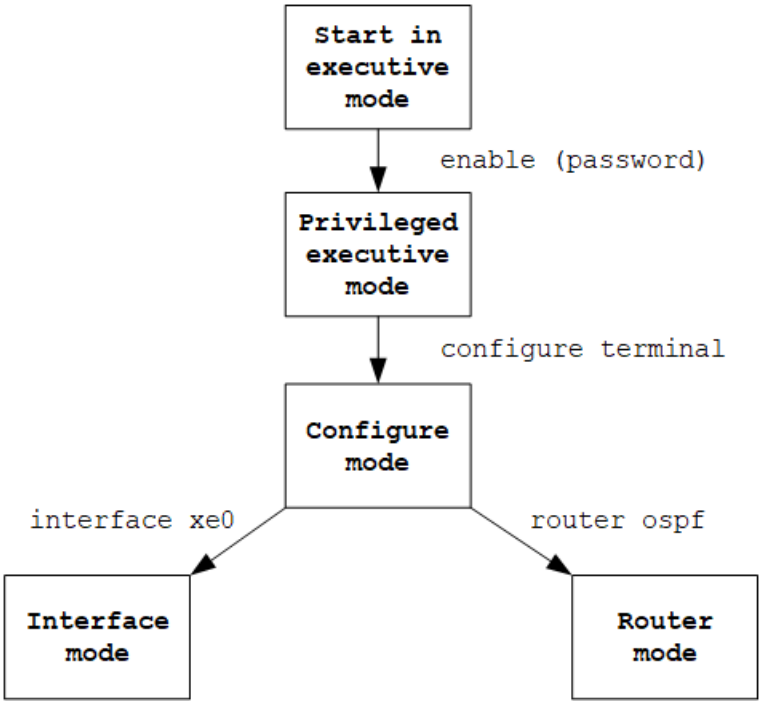
Name	Description
`Execution mode`	Also called *view* mode, this is the first mode to appear after you start the CLI. It is a base mode from where you can perform basic commands such as show, exit, quit, help, and enable.
Privileged execution mode	Also called *enable* mode, in this mode you can run additional basic commands such as debug, write, and show.
Configure mode	Also called *configure terminal* mode, in this mode you can run configuration commands and go into other modes such as interface, router, route map, key chain, and address family. Configure mode is single user. Only one user at a time can be in configure mode.
Interface mode	In this mode you can configure protocol-specific settings for a particular interface. Any setting you configure in this mode overrides a setting configured in router mode.
Router mode	This mode is used to configure router-specific settings for a protocol such as BGP or OSPF.

© 2026 IP Infusion Inc. Proprietary

Command Mode Tree

The diagram below shows the common command mode hierarchy.

Figure 1. Common command modes



To change modes:

1. Enter privileged executive mode by entering **`enable`** in Executive mode.
2. Enter configure mode by entering **`configure terminal`** in Privileged Executive mode.

The example below shows moving from executive mode to privileged executive mode to configure mode and finally to router mode:

```
> enable mypassword
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# router ospf
(config-router)#
```

Note: Each protocol can have modes in addition to the common command modes. See the command reference for the respective protocol for details.

Transaction-based Command-line Interface

The OcNOS command line interface is transaction based:

- Any changes done in configure mode are stored in a separate *candidate* configuration that you can view with the `show transaction current` command.
- When a configuration is complete, apply the candidate configuration to the running configuration with the command.

- If a `commit` fails, no configuration is applied as the entire transaction is considered failed. You can continue to change the candidate configuration and then retry the `commit`.
- Discard the candidate configuration with the `abort transaction` command.
- Check the last aborted transaction with the `show transaction last-aborted` command.
- Multiple configurations cannot be removed with a single . You must remove each configuration followed by a `commit`.

Note: All commands MUST be executed only in the default CML shell (**`cmlsh`**). If you log in as root and start **`imish`**, then the system configurations will go out of sync. The **`imish`** shell is not supported and should not be started manually.

LAYER 2 CONFIGURATION GUIDE

802.1X Configuration 79
Topology 79
Configuration 79
Disabling Native VLAN Configuration 81
Topology 81
Configuration of SW1 and SW2 81
Configuring acceptable-frame-type vlan-tagged on ingress interface 83
Disabling Native VLAN Configuration on Trunk mode 85
Topology 85
Configuration 85
Configuring Disable-Native-VLAN on Trunk mode 87
Layer 2 Control Protocols Tunneling 89
Overview 89
L2CP Tunneling in Provider Bridging 89
L2CP Tunneling in VXLAN 90
Link Aggregation Configuration 92
Topology 92
Dynamic LAG Configuration 92
Static LAG Configuration 95
Static LAG Minimum Link Configuration 98
Static-LAG Minimum Bandwidth Configuration 100
Dynamic-LAG Minimum Link Configuration 103
Dynamic LAG Minimum Bandwidth Configuration 106
LACP Minimum-Link, Minimum-Bandwidth on Dynamic and Static Channel-Groups with MLAG 109
LACP Force-Up 124
LACP Aggregator Force-up 130
Overview 130
Feature Characteristics 130
Benefits 130
LACP Aggregator Force-up for Dynamic LAG Configuration 131
LACP Aggregator Force-up for MLAG Configuration 132
Implementation Examples 136
CLI Command 136
Glossary 137
MLAG Configuration 139
Intra-Domain-Link (IDL) 139
Intra-Domain-Peer (IDP) 139

© 2026 IP Infusion Inc. Proprietary

Options to Configure Intra-Domain 140
Topology 141
Configuration 141
MLAG Active-Active Dynamic Configuration 150
Topology 150
Validation 158
Static Configuration 160
Topology 161
Validation 166
ARP ACL Configuration 168
Topology 168
Validation 174
MSTP Configuration 175
Configuration 175
Validation 183
Port Security Configuration 190
Secured MACs Learned Dynamically 190
Secured MAC Addresses Learned Statically 192
Static Mode 193
Disable Spanning Tree Configuration 195
Disabling MSTP Configuration 195
STP Configuration 200
RSTP Configuration 202
Link Layer Discovery Protocol Configuration 206
Topology 206
LLDPv2 (Interface Mode TLV) 207
Global Mode TLV 214
LLDP-MED 217
Provider Bridging Configuration 222
Overview 222
Single Provider Bridge Configuration 222
Two Provider Bridge Configuration 225
Layer 2 Protocol Tunneling (L2PT/L2CP Tunneling) 229
Provider Bridging with VLAN Translation 230
Provider Bridging QoS Configuration 242
Provider Bridging Untagged-pep Configuration 249
Provider Bridging Configuration (SVLAN) 253
Customer-Network Port (CNP) 253
STAG-based Interface 253
Port-based Interface 253

© 2026 IP Infusion Inc. Proprietary

Topology 254
Configuration 254
Validation 256
Traffic Mirroring Configuration 257
SPAN Overview 257
Topology 258
Port Mirroring Configuration 258
VLAN and Rule Based Mirroring 261
RSPAN Overview 262
VLAN and Rule Based Mirroring Configuration 264
VLAN Mirroring Using VLAN Ranges Configuration 266
Traffic Mirroring using ERSPAN 283
Overview 283
Prerequisites 284
Configuration 284
CLI Commands 287
Revised Command 294
Glossary 294
Private VLAN Configuration 296
Topology 296
Configure PVLAN Trunk and Promiscuous Trunk Port 296
Configure PVLAN Trunk and Promiscuous Access Port 299
Spanning Tree Protocol Configuration 304
Configurations 304
MLAG with Provider Bridging Configuration 313
Configuration 313
RPVST+ Configuration 326
Topology 326
Configuration 326
Validation 328
RSTP Configuration 331
Configuration 331
VLAN Configuration 340
Configuration 340
ErrDisable for Link-Flapping Configuration 347
Topology 347
Automatic Recovery 347
Manual Recovery 349
ErrDisable at the Interface Level 350
ErrDisable for Storm-Control Configuration 351

© 2026 IP Infusion Inc. Proprietary

Topology 351
Automatic Recovery 351
Log Message 352
Manual Recovery 353
Errdisable at the Interface Level 354
Support IGMP Snooping for Provider Bridge 358
Overview 358
Feature Characteristics 358
Prerequisites 358
Configuration 359
Validation 363
Unidirectional Link Detection Configuration 366
Topology 366
Configuration 366
Enable UDLD under bridge-group 368
MAC Authentication Bypass 370
Topology 370
Configuration 370
Configuration 371
Traffic Segmentation-Protected Port 373
Topology 373
Isolated-Promiscuous Configuration 373
Isolated-Isolated Configuration 376
Mirror Filtered Packets to CPU 380
Feature Characteristics 380
Configuration 381
Validation 383
CLI Commands 384

© 2026 IP Infusion Inc. Proprietary

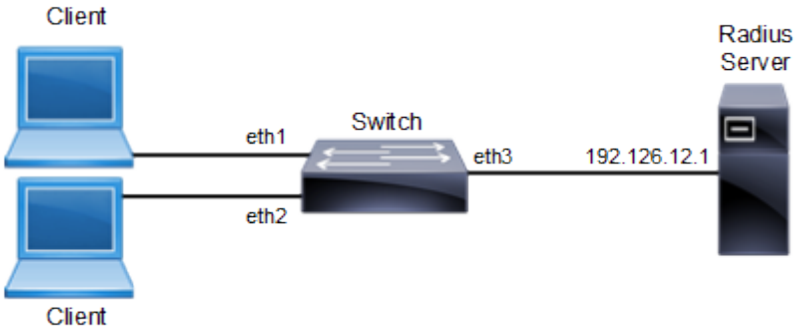
802.1X Configuration

IEEE 802.1x restricts unauthenticated devices from connecting to a switch. Only after authentication is successful, traffic is allowed through the switch.

Topology

In this example, a radius server keeps the client information, validating the identity of the client and updating the switch about the authentication status of the client. The switch is the physical access between the two clients and the server. It requests information from the client, relays information to the server and then back to the client. To configure 802.1x authentication, enable authentication on ports eth1 and eth2 and specify the radius server IP address and port.

Figure 2. 802.1x Topology



Configuration

`Switch#configure terminal`	Enter configure mode.
`Switch(config)#port-security disable`	Disable the port-security.
`Switch(config)#dot1x system-auth-ctrl`	Enable authentication globally.
`Switch(config)#interface eth2`	Enter interface mode.
`Switch(config-if)#switchport`	Enable switch port on interface.
`Switch(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (`eth2`).
`Switch(config-if)#exit`	Exit interface mode.
`Switch(config)#interface eth1`	Enter interface mode.
`Switch(config-if)#switchport`	Enable switch port on interface.
`Switch(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (`eth1`).
`Switch(config-if)#exit`	Exit interface mode.
`Switch(config)#radius-server dot1x key-string testing123`	Specify key with string name between radius server and client
`Switch(config)#radius-server dot1x host 192.126.12.1`	Specify the Radius Server address (192.126.12.1)

© 2026 IP Infusion Inc. Proprietary

`Switch(config-radius-server)#exit`	Exit from radius server mode.
`Switch(config)#interface eth3`	Enter interface mode.
`Switch(config-if)#ip address 192.126.12.2/24`	Set the IP address on interface `eth3`.
`Switch(config-if)#commit`	Commit the transaction.
`Switch(config-if)#exit`	Exit interface mode.

Validation

show dot1x, show dot1x all

```
#show dot1x all
802.1X Port-Based Authentication Enabled
  RADIUS server address: 192.126.12.1:1812
  Next radius message id: 0
  RADIUS client address: not configured

802.1X info for interface ge1
  Supplicant address: 0000.0000.0000
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 1
  protocol version: 2
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connected - portMode: Auto
  PAE: reAuthCount: 0 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Invalid - reqCount: 0 - idFromServer: 0
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false


#show dot1x
802.1X Port-Based Authentication Enabled
  RADIUS server address: 192.126.12.1:1812
  Next radius message id: 0
  RADIUS client address: not configured
```

Disabling Native VLAN Configuration

This section contains sample configurations to check the functionality to drop the untagged traffic by disabling the native vlan by configuring acceptable-frame-type vlan-tagged.

Topology

Figure 3. Native VLAN Topology

Configuration of SW1 and SW2

SW1

`SW1#configure terminal`	Enter configuration mode
`SW1(config)# bridge 1 protocol rstp vlan-bridge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2-10 bridge 1 state enable`	Create 2-10 vlans
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface xe6`	Enter interface configuration mode for xe6
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode hybrid`	Configure port mode as hybrid
`SW1(config-if)# switchport hybrid allowed vlan all`	Allow all the vlans on the xe6 port
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#interface xe21`	Enter interface configuration mode for xe21
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode hybrid`	Configure port mode as hybrid
`SW1(config-if)# switchport hybrid allowed vlan all`	Allow all the vlans on the xe21 port
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#commit`	Commit the candidate configuration to the running configuration

© 2026 IP Infusion Inc. Proprietary

SW2

SW2#configure terminal	Enter configuration mode
SW2(config)# bridge 1 protocol rstp vlan-bridge	Create bridge
SW2(config)#vlan database	Enter VLAN configuration mode
SW2(config-vlan)#vlan 2-10 bridge 1 state enable	Create 2-10 vlans
SW2(config-vlan)#exit	Exit VLAN configuration mode
SW2(config)#interface xe6	Enter interface configuration mode for xe6
SW2(config-if)#switchport	Configure switchport
SW2(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW2(config-if)#switchport mode hybrid	Configure port mode as hybrid
SW2(config-if)# switchport hybrid allowed vlan all	Allow all the vlans on the xe6 port
SW2(config-if)#exit	Exit from interface mode
SW2(config)#interface xe13	Enter interface configuration mode for xe13
SW2(config-if)#switchport	Configure switchport
SW2(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW2(config-if)#switchport mode hybrid	Configure port mode as hybrid
SW2(config-if)# switchport hybrid allowed vlan all	Allow all the vlans on the xe13 port
SW2(config-if)#exit	Exit from interface mode
SW2(config)#commit	Commit the candidate configuration to the running configuration

Validation

Sending untagged, vlan-5 and vlan-6 traffic from ixia-1 to ixia-2. In the show bridge o/p we can see all the mac entries learnt for all the traffics.

In the show vlan brief output for default vlan interface xe21 is having port type as untagged (u).

```
SW1#show bridge
bridge 1 is running on rstp vlan-bridge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe21        0000.0000.0003    1     300
 1         5                   xe21        0000.0000.0005    1     300
 1         6                   xe21        0000.0000.0006    1     300

SW1#sh int counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps   |    Tx mbps  |    Tx pps   |
```

```
+------------------+-------------+------------+-------------+------------+
 ce53               0.00          0            0.00          0
 xe6                0.00          0            2960.63       246719
 xe8                0.00          0            0.00          0
 xe9                0.00          0            0.00          0
 xe21               2960.63       246719       0.00          0

SW1#sh vlan brief
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ========================
1       1       default          ACTIVE  Success    xe6(u) xe21(u)
1       2       VLAN0002         ACTIVE  Success    xe6(t) xe21(t)
1       3       VLAN0003         ACTIVE  Success    xe6(t) xe21(t)
1       4       VLAN0004         ACTIVE  Success    xe6(t) xe21(t)
1       5       VLAN0005         ACTIVE  Success    xe6(t) xe21(t)
1       6       VLAN0006         ACTIVE  Success    xe6(t) xe21(t)
1       7       VLAN0007         ACTIVE  Success    xe6(t) xe21(t)
1       8       VLAN0008         ACTIVE  Success    xe6(t) xe21(t)
1       9       VLAN0009         ACTIVE  Success    xe6(t) xe21(t)
1       10      VLAN0010         ACTIVE  Success    xe6(t) xe21(t)
```

Configuring acceptable-frame-type vlan-tagged on ingress interface

SW1

`SW1(config)#interface xe21`	Enter interface configuration mode for xe21
`SW1(config-if)# switchport mode hybrid acceptable-frame-type vlan-tagged`	Configure acceptable-frame-type vlan-tagged
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#commit`	Commit the candidate configuration to the running configuration

Validation

After configuring acceptable-frame-type vlan-tagged, In the show bridge o/p we can see that un-tagged traffic is dropped (.0003 mac entry is not present), and traffic also getting dropped for that specific stream.

Now on show vlan brief output we can see that xe21 interface is having port type as tagged (t).

```
SW1#sh show bridge
bridge 1 is running on rstp vlan-bridge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         5                   xe21        0010.9400.0003    1     300
 1         6                   xe21        0010.9400.0004    1     300
SW1#sh int counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps   |    Tx mbps  |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 ce53               0.00          0            0.00          0
 xe6                0.00          0            1971.13       164480
 xe8                0.00          0            0.00          0
 xe9                0.00          0            0.00          0
 xe21               2960.64       246720       0.00          0
```

```
SW1#sh vlan brief
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                      (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Success    xe6(u) xe21(t)
1       2       VLAN0002         ACTIVE  Success    xe6(t) xe21(t)
1       3       VLAN0003         ACTIVE  Success    xe6(t) xe21(t)
1       4       VLAN0004         ACTIVE  Success    xe6(t) xe21(t)
1       5       VLAN0005         ACTIVE  Success    xe6(t) xe21(t)
1       6       VLAN0006         ACTIVE  Success    xe6(t) xe21(t)
1       7       VLAN0007         ACTIVE  Success    xe6(t) xe21(t)
1       8       VLAN0008         ACTIVE  Success    xe6(t) xe21(t)
1       9       VLAN0009         ACTIVE  Success    xe6(t) xe21(t)
1       10      VLAN0010         ACTIVE  Success    xe6(t) xe21(t)
```

© 2026 IP Infusion Inc. Proprietary

Disabling Native VLAN Configuration on Trunk mode

This section contains sample configurations to check the functionality to drop the untagged traffic by disabling the native VLAN by configuring disable-native-VLAN.

Topology

Figure 4. Native VLAN Topology

Configuration

SW1

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol mstp`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2-10 bridge 1 state enable`	Create 2-10 vlans
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface xe21`	Enter interface configuration mode for xe21
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Configure port mode as trunk
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe21 port
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#interface xe6`	Enter interface configuration mode for xe6
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Configure port mode as trunk
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe6 port
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#commit`	Commit the candidate configuration to the running configuration

© 2026 IP Infusion Inc. Proprietary

SW2

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 2-10 bridge 1 state enable`	Create 2-10 vlans
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface xe6`	Enter interface configuration mode for xe6
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode trunk`	Configure port mode as trunk
`SW2(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe6 port
`SW2(config-if)#exit`	Exit from interface mode
`SW2(config)#interface xe13`	Enter interface configuration mode for xe13
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode trunk`	Configure port mode as trunk
`SW2(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe13 port
`SW2(config-if)#exit`	Exit from interface mode
`SW2(config)#commit`	Commit the candidate configuration to the running configuration

Validation

Sending untagged, VLAN-5 and VLAN-6 traffic from IXIA-1 to IXIA-2. In the show bridge output we can see all the MAC entries learnt for all the traffics.

In the `show vlan brief` output for default VLAN interface xe21 is having port type as untagged (u).

```
SW1#show bridge
bridge 1 is running on mstp
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe21        0010.9400.0001    1     300

SW1#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe21               621.21         606650        0.00           0
```

```
 xe6               0.00           0             621.21         606651

SW1#show vlan brief
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                      (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Success    xe21(u) xe6(u)
1       2       VLAN0002         ACTIVE  Success    xe21(t) xe6(t)
1       3       VLAN0003         ACTIVE  Success    xe21(t) xe6(t)
1       4       VLAN0004         ACTIVE  Success    xe21(t) xe6(t)
1       5       VLAN0005         ACTIVE  Success    xe21(t) xe6(t)
1       6       VLAN0006         ACTIVE  Success    xe21(t) xe6(t)
1       7       VLAN0007         ACTIVE  Success    xe21(t) xe6(t)
1       8       VLAN0008         ACTIVE  Success    xe21(t) xe6(t)
1       9       VLAN0009         ACTIVE  Success    xe21(t) xe6(t)
1       10      VLAN0010         ACTIVE  Success    xe21(t) xe6(t)
```

Configuring Disable-Native-VLAN on Trunk mode

SW1

`SW1(config)#interface xe21`	Enter interface configuration mode for xe21
`SW1(config-if)#switchport mode trunk disable-native-vlan`	Configure disable native VLAN on trunk mode
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#commit`	Commit the candidate configuration to the running configuration

Validation

After configuring disable-native-vlan, `show vlan brief` output we can see that xe21 interface is having port type as tagged (t).

```
SW1#show bridge
bridge 1 is running on mstp
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+----------+
 1         1                   xe21       0010.9400.0001    1     300

SW1SW1#show vlan brief
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                      (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Success    xe21(t) xe6(u)
1       2       VLAN0002         ACTIVE  Success    xe21(t) xe6(t)
1       3       VLAN0003         ACTIVE  Success    xe21(t) xe6(t)
1       4       VLAN0004         ACTIVE  Success    xe21(t) xe6(t)
1       5       VLAN0005         ACTIVE  Success    xe21(t) xe6(t)
1       6       VLAN0006         ACTIVE  Success    xe21(t) xe6(t)
1       7       VLAN0007         ACTIVE  Success    xe21(t) xe6(t)
1       8       VLAN0008         ACTIVE  Success    xe21(t) xe6(t)
1       9       VLAN0009         ACTIVE  Success    xe21(t) xe6(t)
1       10      VLAN0010         ACTIVE  Success    xe21(t) xe6(t)

SW1#show interface counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps   |    Tx mbps  |    Tx pps   |
```

```
+-------------------+--------------+-------------+--------------+--------------+
 Xe21                864.88          844613         0.00            0
 Xe6                0.00            0              0.00            0

SW1#show interface counters drop-stats
Interface xe21
  Rx Policy Discards: 454522965
  Rx EGR Port Unavail: 454522967
```

Layer 2 Control Protocols Tunneling

Overview

The Layer 2 Control Protocols (L2CP) processing specified here is based largely on the IEEE 802.1Q specification for handling L2CP Frames, i.e. if they should be forwarded, peered, or discarded.

In Provider Bridging (PB), the IEEE 802.1Q provides a mechanism for separating the Layer2 control plane into multiple customer and provider control planes. It allows a certain layer 2 control protocol to operate only within a provider network, or to allow interaction between the customer and the provider network, or to pass transparently through a provider network with complete isolation from other customer networks.

In case of non-Provider Bridging, packet is forwarded without changing any MAC.

L2CP Tunneling in Provider Bridging

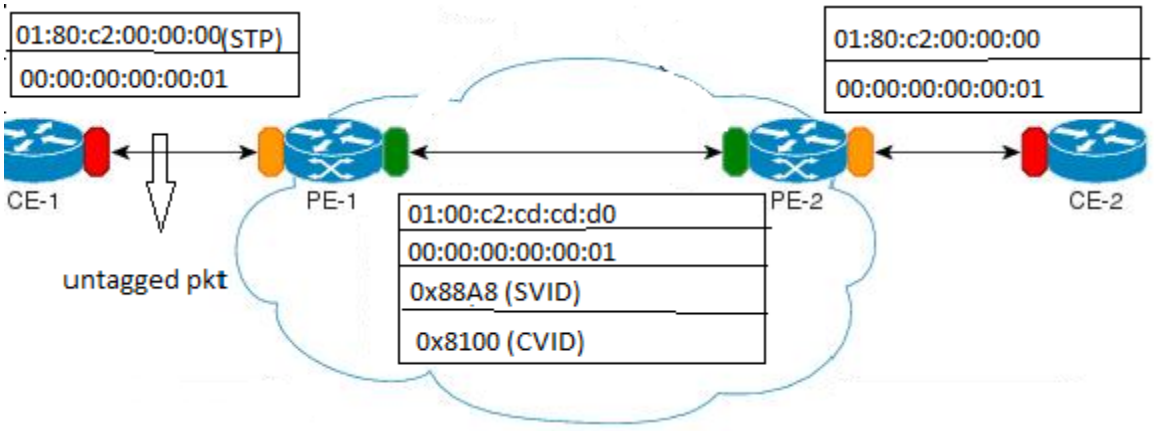
L2CP tunneling provides support for tunneling control plane frames between CE nodes.

In the context of PB, a L2CP frame is defined as any frame containing a destination MAC address as 01:00:0C:CD:CD:D0 or 01:04:DF:CD:CD:D0 (which can be changed via CLI).

When control frames received at CEP port of a PE bridge, predefined multicast address (01-00-C2-CD-CD-D0) is replaced as destination for tunneling the packets across service provider network. If control packets are customer vlan tagged or untagged, then PE bridge will append corresponding service vlan tag to the control packet as per registration table / vlan translation table mapped to the port and send it across the service provider as a data packet.

When tunneled control packet with multicast address (01-00-C2-CD-CD-D0) received on PNP port, the multicast address is replaced with corresponding control packet multicast address and cvlan/svlan removal or update is done as per registration table / vlan translation table.

Figure 5. L2CP Tunneling Process in Provider Bridge



L2CP Configuration in Provider Bridging

Enabling tunneling at interface:

```
(config)#bridge 1 protocol provider-rstp edge
(config)#vlan database
(config-vlan)#vlan 2-10 bridge 1 state enable
```

```
(config-vlan)#vlan 11 type service point-point bridge 1 state enable
(config-vlan)#ex
(config)#cvlan registration table map1 bridge 1
(config-cvlan-registration)#cvlan 2 svlan 11
(config-cvlan-registration)#ex
(config)#interface xe1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode customer-edge hybrid
(config-if)#switchport customer-edge hybrid allowed vlan all
(config-if)#switchport customer-edge vlan registration map1
(config-if)#l2protocol stp tunnel
#show running-config interface xe1
!
 interface xe1
 speed 1g
 switchport
 bridge-group 1
 switchport mode customer-edge hybrid
 switchport customer-edge hybrid allowed vlan all
 switchport customer-edge vlan registration map1
 l2protocol stp tunnel
 customer-spanning-tree provider-edge svlan 11 path-cost 128
(config-if)#commit
```

Configuring egress interfaces:

```
(config)#interface xe2
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode provider-network
(config-if)#switchport provider-network allowed vlan all
(config-if)#commit
```

Validation

To display L2protocol information:

```
#show l2protocol processing interface xe1
Bridge   Interface Name  Protocol     Processing Status     Hardware Status
======   ==============  ========     =================     ===============
1        xe1             stp          Tunnel                Tunnel
1        xe1             lacp         Peer                  Peer
1        xe1             dot1x        Peer                  Peer
1        xe1             lldp         Peer                  Peer
1        xe1             efm          Peer                  Peer
1        xe1             elmi         Peer                  Peer
```

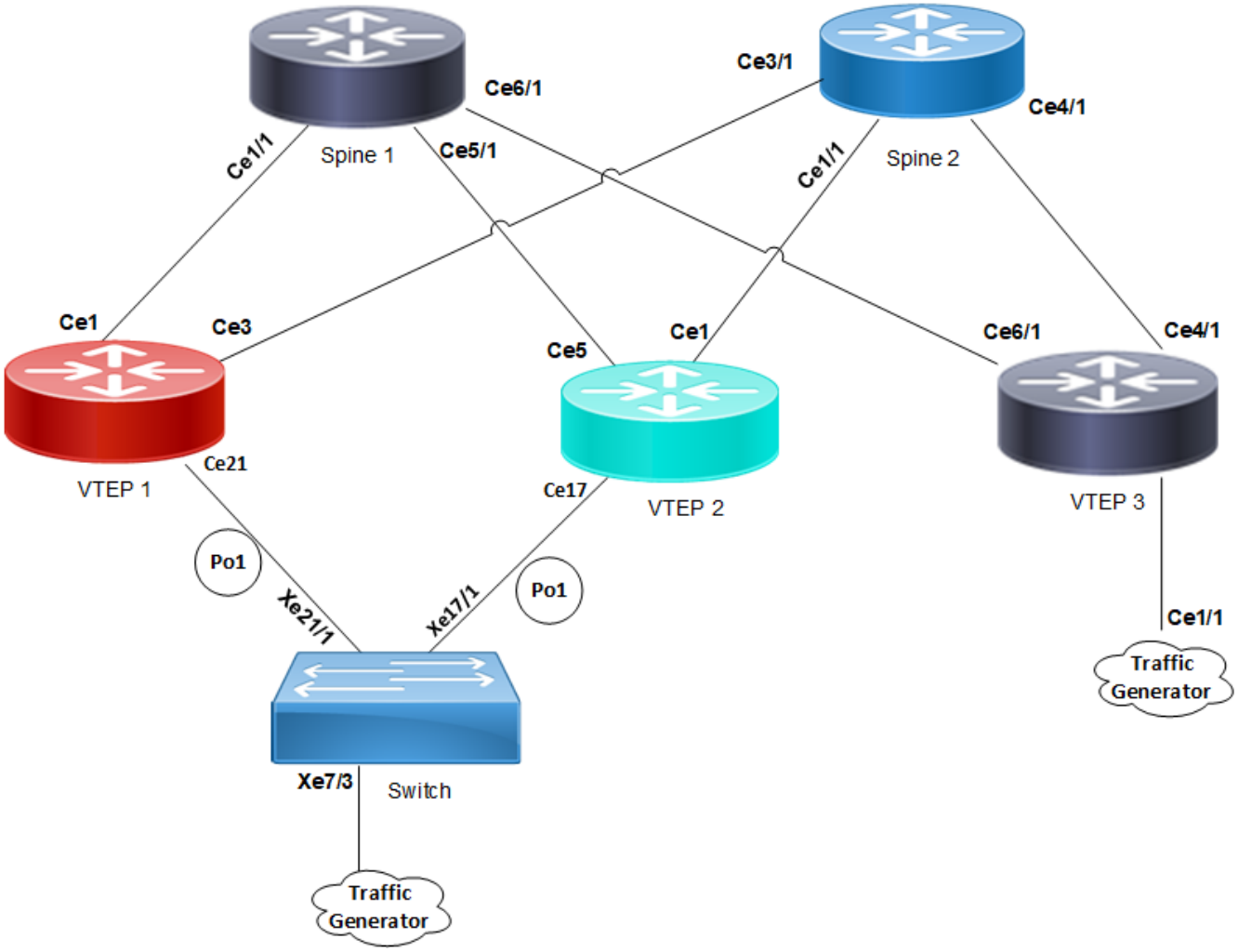
To display L2protocol counters:

```
#show l2protocol interface counters
Interface xe1
Tunnel               :  stp                 : 45
```

L2CP Tunneling in VXLAN

L2CP tunneling provides support for tunneling control plane frames across VxLAN/MH.

Figure 6. L2CP tunneling in VXLAN



VxLAN creates LAN segments using a MAC in IP encapsulation. The encapsulation carries the original L2 frame received from a host to the destination in another server using IP tunnels. The endpoints of the virtualized tunnel formed using VxLAN are called VTEPs (VXLAN Tunnel EndPoints).

L2CP tunneling provides support for tunneling control plane frames across VxLAN with MH/SH combination.

Any L2CP frame that is destined towards other end with a multicast destination MAC Address for L2 protocol is decided by looking at the frame and upon the configured values of the L2CP service attributes.

As and when control packets with default destination MAC address for any L2 protocol is generated, it will be forwarded by VTEPs that are part of MH towards the VTEP that is part of SH and vice versa.

During this operation, the default destination MAC address for any L2 protocol is replaced with predefined multicast address as destination for tunneling the packets across spine nodes. When tunneled control packet with pre-defined multicast address received on ingress port on the other end of the VTEP, the multicast address is replaced with corresponding control packet multicast address.

© 2026 IP Infusion Inc. Proprietary

Link Aggregation Configuration

This section contains a complete sample Link Aggregation Group configuration.

LACP is based on the 802.3ad IEEE specification. It allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The spanning tree views it as one interface and not as two or three interfaces. When there is a failure in one physical interface, the other interfaces stay up and there is no disruption. Traffic can be load balanced within an LACP trunk group in a controlled manner using the hashing algorithm.The maximum number of physical Ethernet links in a single logical channel depends upon the hardware support.

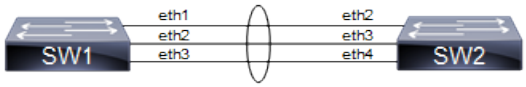
Notes:

- Physical interfaces inherit the properties of LAG port once it is attached to be part of LAG, irrespective of the configuration present on the physical interface.
- In case of Dynamic and Static LAG, it is possible to move member ports from one LAG to another LAG.
- Configure LAG port as a switch or router port, before adding member ports into it.
- LAG configuration is not allowed on inactive subsidiary ports. Configuring LAG on subsidiary ports before executing port breakout commands on control ports causes issues.
- Remove any LAG configuration from subsidiary ports before issuing the no port breakout command.
- Switchport configuration is not allowed on inactive subsidiary ports. Applying switchport configuration on subsidiary ports before executing the port breakout command causes issues.
- Do not execute the no port breakout command on subsidiary ports configured with switchport.

Topology

In the following topology, 3 links are configured between the two switches SW1 and SW2. These three links are assigned the same administrative key (1) so that they aggregate to form a single channel 1. They are viewed by the STP as one interface.

Figure 7. LACP topology



Dynamic LAG Configuration

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge

`SW1(config)# vlan database`	Enter VLAN database mode.
`SW1(config-vlan)# vlan 2-10 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`SW1(config-vlan)# commit`	Commit the candidate configuration to the running Configuration.
`SW1(config-vlan)# exit`	Exit the VLAN configuration mode.
`SW1(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`SW1(config)#interface po10`	Enter into port channel interface po10.
`SW1(config-if)#switchport`	Configure po10 as a layer 2 port.
`SW1(config-if)#bridge-group 1`	Associate bridge to an interface.
`SW1(config-if)#switchport mode trunk`	Configure port as a trunk.
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the po10 interface.
`SW1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW1(config-if)#exit`	Exit interface mode.
`SW1(config)#interface eth1`	Enter interface mode.
`SW1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`SW1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW1(config-if)#exit`	Exit interface mode.
`SW1(config)#interface eth2`	Enter interface mode.
`SW1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`SW1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW1(config-if)#exit`	Exit interface mode.
`SW1(config)#interface eth3`	Enter interface mode.
`SW1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`SW1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW1(config-if)#exit`	Exit interface mode.

© 2026 IP Infusion Inc. Proprietary

SW2

SW2#configure terminal	Enter configure mode.
SW2(config)# bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge
SW2(config)# vlan database	Enter VLAN database mode.
SW2(config-vlan)# vlan 2-10 bridge 1 state enable	Configure a VLAN and add it to the bridge.
SW2(config-vlan)# commit	Commit the candidate configuration to the running Configuration.
SW2(config-vlan)# exit	Exit the VLAN configuration mode.
SW2(config)#lacp system-priority 20000	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
SW2(config)#interface po10	Enter into port channel interface po10.
SW2(config-if)#switchport	Configure po10 as a layer 2 port.
SW2(config-if)#bridge-group 1	Associate bridge to an interface.
SW2(config-if)#switchport mode trunk	Configure port as a trunk.
SW2(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the po10 interface.
SW2(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface eth2	Enter interface mode.
SW2(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW2(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface eth3	Enter interface mode.
SW2(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW2(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface eth4	Enter interface mode.
SW2(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for

© 2026 IP Infusion Inc. Proprietary

	aggregation by the local system.
SW2(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW2(config-if)#exit	Exit interface mode.

Validation

show etherchannel detail, show etherchannel summary, show running-config interface po10, show running-config interface eth1

```
#show etherchannel detail
% Aggregator po10 7
% Aggregator Type: Layer2
%  Mac address: 08:00:27:50:6a:9b
%  Admin Key: 0010 - Oper Key 0010
%  Actor LAG ID- 0x4e20,08-00-27-ab-ea-38,0x000a
%  Receive link count: 3 - Transmit link count: 3
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x4e20,08-00-27-f8-3c-30,0x000a
%   Link: eth1 (3) sync: 1
%   Link: eth2 (4) sync: 1
%   Link: eth3 (5) sync: 1
%   Collector max delay: 5

#show etherchannel summary
% Aggregator po10 7
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
% Aggregator Type: Layer2
%   Link: eth1 (3) sync: 1
%   Link: eth2 (4) sync: 1
%   Link: eth3 (5) sync: 1

#show running-config interface po10
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all

#show running-config interface eth1
!
interface eth1
 channel-group 10 mode active
```

Static LAG Configuration

SW1

SW1#configure terminal	Enter configure mode.
SW1(config)# bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge
SW1(config)# vlan database	Enter VLAN database mode.
SW1(config-vlan)# vlan 2-10 bridge 1 state enable	Configure a VLAN and add it to the bridge.
SW1(config-vlan)# commit	Commit the candidate configuration to the running Configuration.

© 2026 IP Infusion Inc. Proprietary

`SW1(config-vlan)# exit`	Exit the VLAN configuration mode.
`SW1(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`SW1(config)#interface sa10`	Enter into port channel interface sa10.
`SW1(config-if)#switchport`	Configure sa10 as a layer 2 port.
`SW1(config-if)#bridge-group 1`	Associate bridge to an interface.
`SW1(config-if)#switchport mode trunk`	Configure port as a trunk.
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the po10 interface.
`SW1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW1(config-if)#exit`	Exit interface mode.
`SW1(config)#interface eth1`	Enter interface mode.
`SW1(config-if)#static-channel-group 10`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`SW1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW1(config-if)#exit`	Exit interface mode.
`SW1(config)#interface eth2`	Enter interface mode.
`SW1(config-if)#static-channel-group 10`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`SW1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW1(config-if)#exit`	Exit interface mode.
`SW1(config)#interface eth3`	Enter interface mode.
`SW1(config-if)#static-channel-group 10`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`SW1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW1(config-if)#exit`	Exit interface mode.

SW2

`SW2#configure terminal`	Enter configure mode.
`SW2(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge

SW2(config)# vlan database	Enter VLAN database mode.
SW2(config-vlan)# vlan 2-10 bridge 1 state enable	Configure a VLAN and add it to the bridge.
SW2(config-vlan)# commit	Commit the candidate configuration to the running Configuration.
SW2(config-vlan)# exit	Exit the VLAN configuration mode.
SW2(config)#interface sa10	Enter into port channel interface sa10.
SW2(config-if)#switchport	Configure sa10 as a layer 2 port.
SW2(config-if)#bridge-group 1	Associate bridge to an interface.
SW2(config-if)#switchport mode trunk	Configure port as a trunk.
SW2(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the po10 interface.
SW2(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface eth2	Enter interface mode.
SW2(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW2(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface eth3	Enter interface mode.
SW2(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface eth4	Enter interface mode.
SW2(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW2(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW2(config-if)#exit	Exit interface mode.

Validation

```
#show static-channel-group
% Static Aggregator: sa10
% Member status:
   eth1    up
   eth2    up
   eth3    up

#show running-config interface sa10
!
```

```
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all

#show running-config interface eth1
!
interface eth1
 static-channel-group 10
```

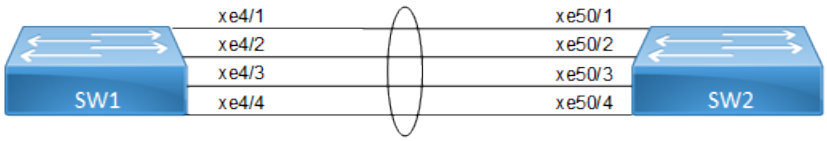
Static LAG Minimum Link Configuration

Configure the minimum number of ports that must be linked up and bundled in the LACP port channel. We can configure the minimum links range from 2 to 32. If the number of ports aggregated to the port channel is less than the minimum number of links configured, then the port channel enters the Protocol Down because of the minimum link state.

Note: Minimum links must be configured only on one side of static channel for optimal performance.

Topology

Figure 8. LAG minimum link



SW1

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface static-lag sa10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4(range is 2-32)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

SW2

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface port-channel sa10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.

© 2026 IP Infusion Inc. Proprietary

`(config-if)#exit`	Exit the configure mode

Validation

SW1

```
#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-Links 4
% Member status:
         xe4/1     up
         xe4/2     up
         xe4/3     up
         xe4/4     up



#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 4
```

SW2

```
#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 4
!

#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-Links 4
% Member status:
         Xe50/1     up
         Xe50/2     up
         Xe50/3     up
         Xe50/4     up
```

Note: When a sa goes down due to the minimum links configured (number of minimum links is greater than the links aggregated to the sa).

```
SW1:
=====
#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
```

```
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
sa10         AGG   1     trunk             down     PD(Min L/B)  0
#

SW2:
=====

#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
sa10         AGG   1     trunk             down     PD(Min L/B)  0
#
```

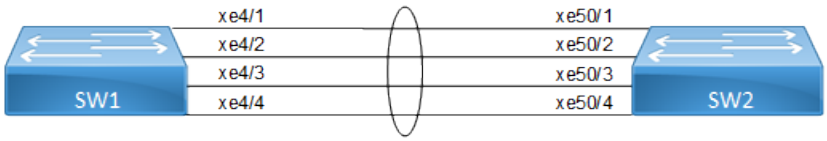
Static-LAG Minimum Bandwidth Configuration

Configure the minimum bandwidth allowed for ports that must be linked up and bundled in the LACP port channel. We can configure the minimum bandwidth range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits. If the Total bandwidth of ports aggregated to the port channel is less than the minimum Bandwidth value configured, then the port channel enters the Protocol Down because of the minimum Bandwidth state.

Note: Minimum Bandwidth should be configured the same on both sides for optimal performance.

Topology

Figure 9. LAG minimum bandwidth



SW1

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface static-lag sa10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

SW2

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface port-channel sa10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

Validation

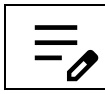
SW1

```
#show static-channel-group 10
% Static Aggregator: sa10
% Minimum- 4
% Member status:
         xe4/1     up
         xe4/2     up
         xe4/3     up
         xe4/4     up

#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 40g
```

SW2

```
#show running-config interface sa10
!
interface sa10
 switchport
```

```
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-bandwidth 40g
!

#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-bandwidth 40g
% Member status:
         Xe50/1     up
         Xe50/2     up
         Xe50/3     up
         Xe50/4     up
```



Note: When sa goes down due to [Total Bandwidth of sa] <[Minimum Bandwidth value Configured]

```
SW1:
=====
#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD - ESI Hold Timer Down


--------------------------------------------------------------------------------
Port-channel Type PVID Mode              Status   Reason Speed
Interface
--------------------------------------------------------------------------------
sa10         AGG   1     trunk             down     PD(Min L/B)  0
#


SW2:
=====

#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
sa10         AGG   1     trunk             down     PD(Min L/B)  0
#
```

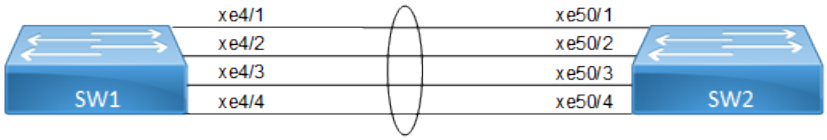
Dynamic-LAG Minimum Link Configuration

Configure the minimum number of ports that must be linked up and bundled in the LACP port channel. We can configure the minimum links range from 2 to 32. If the number of ports aggregated to the port channel is less than the minimum number of links configured, then the port channel enters the Protocol Down because of the minimum link state.

Note: Minimum links should be configured the same on both sides for optimal performance.

Topology

Figure 10. LAG minimum link



SW1

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

SW2

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

Validation

SW1

```
#sh running-config interface po10

interface po10
 switchport
```

```
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
port-channel min-links 4
!

!

#show etherchannel
-------------------------------------
% Lacp Aggregator: po10
% Min-links : 4
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4
-------------------------------------

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
%   Link: xe4/4 (10072) sync: 1
%   Link: xe4/1 (10069) sync: 1
%   Link: xe4/2 (10070) sync: 1
%   Link: xe4/3 (10071) sync: 1
--------------------------------------
```

SW2

```
#show running-config interface po10
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 4
!

#show etherchannel

% Aggregator Type: Layer2
% Lacp Aggregator: po10
% Min-links: 4
% Member:
   xe50/1
   xe50/2
   xe50/3
   xe50/4

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
%   Link: xe50/4 (10072) sync: 1
%   Link: xe50/1 (10069) sync: 1
%   Link: xe50/2 (10070) sync: 1
%   Link: xe50/3 (10071) sync: 1
```

© 2026 IP Infusion Inc. Proprietary

Note: When a PO goes down due to the minimum links configured (number of minimum links is greater than the links aggregated to the PO).

```
SW1:
#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
po10         AGG   1     trunk             down     PD(Min L/B)  0
#


#sh etherchannel
% Lacp Aggregator: po10
% Min-links: 4
% Protocol Down (Min L/B): True
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4

SW2:
#sh etherchannel
% Lacp Aggregator: po10
% Min-links: 4
% Protocol Down (Min L/B): True
% Member:
   Xe50/1
   Xe50/2
   Xe50/3
       xe50/4

#sh int brief po100

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
```

```
po10         AGG   1     trunk             down      PD(Min L/B)   0
#
```

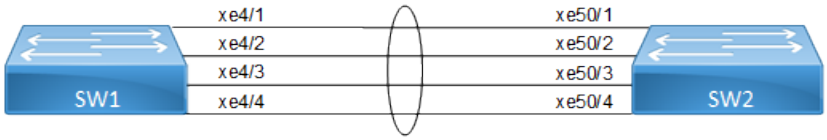
Dynamic LAG Minimum Bandwidth Configuration

Configure the minimum bandwidth allowed for ports that must be linked up and bundled in the LACP port channel. We can configure the minimum bandwidth range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits. If the Total bandwidth of ports aggregated to the port channel is less than the minimum Bandwidth value configured, then the port channel enters the Protocol Down because of the minimum Bandwidth state.

Note: Minimum Bandwidth should be configured the same on both sides for optimal performance.

Topology

Figure 11. LAG minimum bandwidth



SW1

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

SW2

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

© 2026 IP Infusion Inc. Proprietary

Validation

SW1

```
#sh running-config interface po10

interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
port-channel min-bandwidth 40g
!

!

#show etherchannel
-------------------------------------
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4
-------------------------------------

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer3
% Admin Key: 0010 - Oper Key 0010
%   Link: xe4/4 (10072) sync: 1
%   Link: xe4/1 (10069) sync: 1
%   Link: xe4/2 (10070) sync: 1
%   Link: xe4/3 (10071) sync: 1
--------------------------------------
```

SW2

```
#show running-config interface po10
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-bandwidth 40g
!

#show etherchannel

% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Member:
   xe50/1
   xe50/2
   xe50/3
   xe50/4

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
%   Link: xe50/4 (10072) sync: 1
```

© 2026 IP Infusion Inc. Proprietary

```
%   Link: xe50/1 (10069) sync: 1
%   Link: xe50/2 (10070) sync: 1
%   Link: xe50/3 (10071) sync: 1
```

Note: When a PO goes down due to the [Total bandwidth] < [minimum bandwidth configured]

```
SW1:
=====
#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Port-channel Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
po10         AGG   1     trunk             down     PD(Min L/B)  0
#

#sh etherchannel
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Protocol Down (Min L/B): True
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4


SW2:
=====
#sh etherchannel
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Protocol Down (Min L/B): True
% Member:
   Xe50/1
   Xe50/2
   Xe50/3
       xe50/4

#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down
```

```
--------------------------------------------------------------------------------
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
po10         AGG   1     trunk             down     PD(Min L/B)  0
#
```

LACP Minimum-Link, Minimum-Bandwidth on Dynamic and Static Channel-Groups with MLAG

Overview

OcNOS allows the configuration of minimum number of the LAG members per LAG group. Both these configurations are meaningful in case the LAG is used for incremental-BW mode. The minimum configuration controls the minimum number of members /bandwidth that must be operationally up / bandwidth available to declare their LAG as operationally UP.

When static/dynamic LAG interface configured with minimum links / minimum bandwidth, the following conditions are to be met:

- Ports which are admin and operational up are considered for min-link.
- The specified minimum number of links should be up.
- Min-link and min-bandwidth cannot co-exist.
- When ports are down due to min-link/min-bandwidth, in show interface brief command output, port down with the corresponding reason code for the failure due to min-link/min-bandwidth.

Minimum Active Members/Bandwidth

The user can specify the minimum number of members that must be operationally up to declare their LAG as operationally UP. Note that this parameter applies to static/dynamic LAG.

```
port-channel min-links <2 - 32>
```

The minimum active member configuration will be allowed to be modified to be greater than the current number of active members. In such configuration, the LAG operational status will become operationally down.

The user can specify the minimum bandwidth, based on the configured value and the ports that satisfy the conditions LAG will be operationally UP. This parameter is applied for static/dynamic LAG.

```
port-channel min-bandwidth BANDWIDTH
```

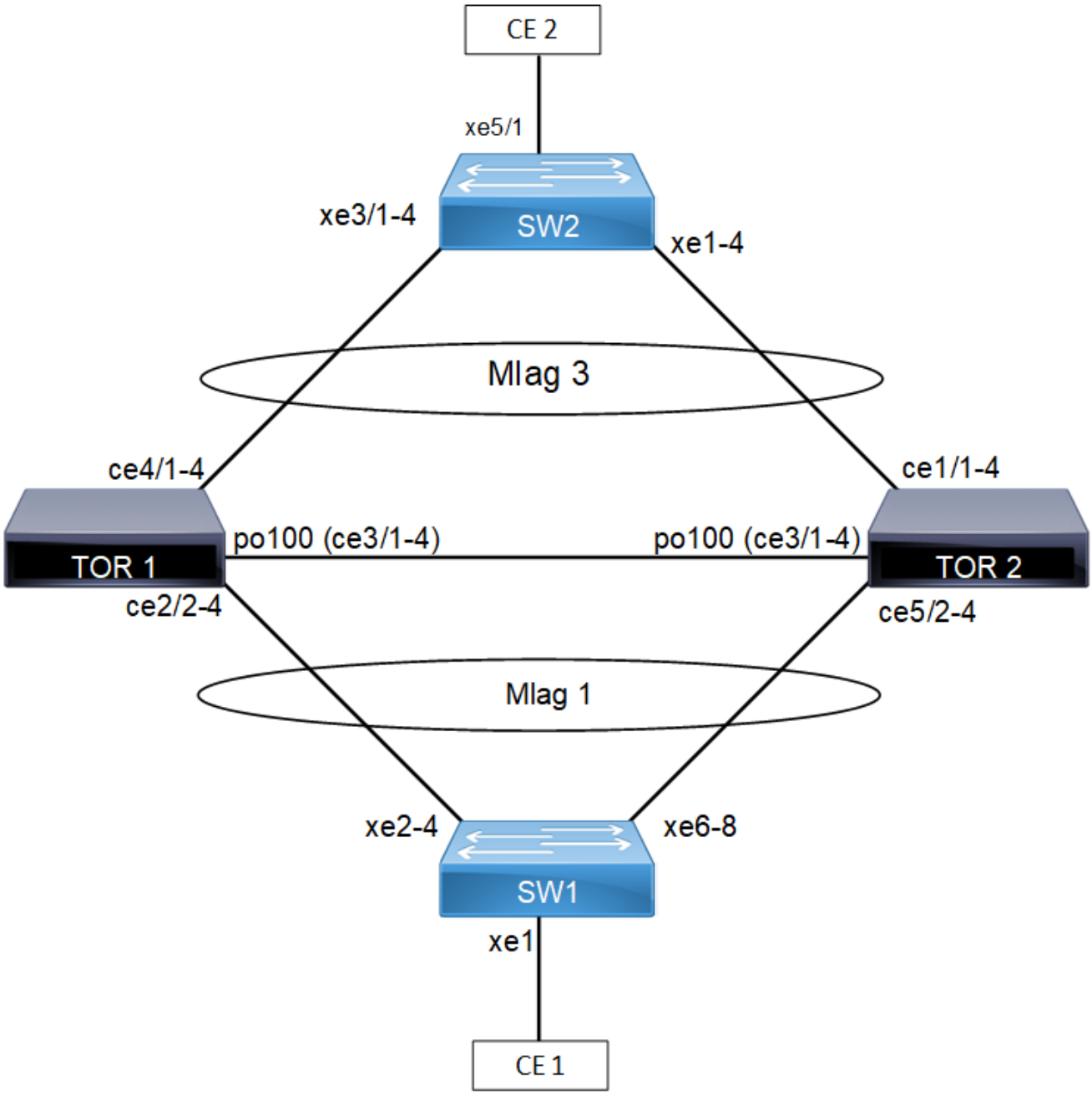
BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.

When condition fails, the operational state changes to DOWN.

Note: Do not configure minimum-link, Minimum Bandwidth both on TORs and Switches at the same time to avoid flaps of MLAG.

Topology

Figure 12. MLAG topology



Configuration

TOR1

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol rstp vlan-bridge`	Configure bridge type
`(config)# vlan database`	Enter vlan database

`(config-vlan)# vlan 600,601,502 bridge 1 state enable`	Configure vlans
`(config-vlan)#commit`	Commit the candidate configuration to the running Configuration.
`(config-vlan)#exit`	Exit the configure mode.
`(config)#interface mlag1`	Enter Interface mode
`(config-if)# switchport`	Make mlag as layer2 port
`(config-if)# bridge-group 1`	Attach interface to bridge
`(config-if)# switchport mode trunk`	Configure trunk port
`(config-if)# switchport trunk allowed vlan add 600,601,502`	Add interface to vlans
`(config-if)# spanning-tree edgeport`	Configure port as edge port to avoid loops
`(config-if)# spanning-tree bpdu-filter enable`	Enable bpdu filter to avoid loops
`(config-if)# mtu 9216`	Configure mtu.
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface mlag3`	Enter Interface mode
`(config-if)# switchport`	Make mlag as layer2 port
`(config-if)# bridge-group 1`	Attach interface to bridge
`(config-if)# switchport mode trunk`	Configure trunk port
`(config-if)# switchport trunk allowed vlan add 600,502`	Add interface to vlans
`(config-if)# spanning-tree edgeport`	Configure port as edge port to avoid loops
`(config-if)# spanning-tree bpdu-filter enable`	Enable bpdu filter to avoid loops
`(config-if)# mtu 9216`	Configure mtu.
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface po100`	Enter Interface mode
`(config-if)# switchport`	Make po as layer2 port
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface sa1`	Enter Interface mode
`(config-if)# switchport`	Make sa1 as layer2 port
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.

© 2026 IP Infusion Inc. Proprietary

`(config-if)#exit`	Exit the configure mode.
`(config)# interface sa3`	Enter interface mode.
`(config-if)# switchport`	Make sa3 as layer2 port.
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce2/1`	Enter Interface mode
`(config-if)#port breakout enable`	Port breakout enabled
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce2/2`	Enter Interface mode
`(config-if)# static-channel-group 1`	Add interface to sa1
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce2/3`	Enter Interface mode
`(config-if)# static-channel-group 1`	Add interface to sa1
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce2/4`	Enter Interface mode
`(config-if)# static-channel-group 1`	Add interface to sa1
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce3/1`	Enter Interface mode
`(config-if)#port breakout enable`	Port breakout enabled
`(config-if)# channel-group 100 mode active`	Add interface to po100
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce3/2`	Enter Interface mode
`(config-if)# channel-group 100 mode active`	Add interface to po100
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.

`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce3/3`	Enter Interface mode
`(config-if)# channel-group 100 mode active`	Add interface to po100
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce3/4`	Enter Interface mode
`(config-if)# channel-group 100 mode active`	Add interface to po100
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce4/1`	Enter Interface mode
`(config-if)#port breakout enable`	Port breakout enabled
`(config-if)# static-channel-group 3`	Add interface to sa3
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce4/2`	Enter Interface mode
`(config-if)# static-channel-group 3`	Add interface to sa3
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce4/3`	Enter Interface mode
`(config-if)# static-channel-group 3`	Add interface to sa3
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#mcec domain configuration`	Enter Multichasis Etherchannel domain configuration mode.
`(config-mcec-domain)# domain-address 1111.2222.3333`	Configure the domain address.
`(config-mcec-domain)# domain-system-number 1`	Configure the domain system number
`(config-mcec-domain)# intra-domain-link po100`	Specify the intra domain link for MLAG communication
`(config-mcec-domain)#commit`	Commit the candidate configuration to the running Configuration.
`(config-mcec-domain)#exit`	Exit the configure mode.

(config)#interface sa1	Enter Interface mode
(config-if)#mlag 1	Map sa1 to mlag1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#int mlag1	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag1
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa3	Enter Interface mode
(config-if)#mlag 3	Map sa3 to mlag3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#int mlag3	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag3
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config-if)# interface sa1	Enter sa interface mode
(config-if)#port-channel min-links 3	Configure min-link value on sa interface
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa3	Enter sa Interface mode
(config-if)#port-channel min-bandwidth 30g	Configure min-bandwidth value on sa/po interface
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

TOR2

#configure terminal	Enter configure mode.
(config)# bridge 1 protocol rstp vlan-bridge	Configure bridge type

(config)# vlan database	Enter vlan database
(config-vlan)# vlan 600,601,502 bridge 1 state enable	Configure vlans
(config-vlan)#commit	Commit the candidate configuration to the running Configuration.
(config-vlan)#exit	Exit the configure mode.
(config)#interface mlag1	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,601,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)# mtu 9216	Configure mtu.
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface mlag3	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)# mtu 9216	Configure mtu.
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface po100	Enter Interface mode
(config-if)# switchport	Make po(IDL) as layer2 port
(config-if)#commit	Commit the candidate configuration to the running Configuration.

© 2026 IP Infusion Inc. Proprietary

`(config-if)#exit`	Exit the configure mode.
`(config)#interface sa1`	Enter Interface mode
`(config-if)# switchport`	Make sa1 as layer2 port
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface sa3`	Enter Interface mode
`(config-if)# switchport`	Make sa3 as layer2 port
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce1/1`	Enter Interface mode
`(config-if)# static-channel-group 3`	Add interface to sa3
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce1/2`	Enter Interface mode
`(config-if)# static-channel-group 3`	Add interface to sa3
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce1/3`	Enter Interface mode
`(config-if)# static-channel-group 3`	Add interface to sa3
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce3/1`	Enter Interface mode
`(config-if)# channel-group 100 mode active`	Add interface to po100
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ce3/2`	Enter Interface mode
`(config-if)# channel-group 100 mode active`	Add interface to po100
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.

© 2026 IP Infusion Inc. Proprietary

(config-if)#exit	Exit the configure mode.
(config)#interface ce3/3	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce3/4	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce5/1	Enter Interface mode
(config-if)# port breakout enable	Port breakout enabled
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce5/2	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce5/3	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce5/4	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config-mcec-domain)# intra-domain-link po100	Specify the intra domain link for MLAG communication
(config-mcec-domain)#commit	Commit the candidate configuration to the running Configuration.

(config-mcec-domain)#exit	Exit the configure mode.
(config)#interface sa1	Enter Interface mode
(config-if)#mlag 1	Map sa1 to mlag1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#int mlag1	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag1
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa3	Enter Interface mode
(config-if)#mlag 3	Map sa3 to mlag3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#int mlag3	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag3
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config-if)# interface sa1	Enter sa interface mode
(config-if)#port-channel min-links 3	Configure min-link value on sa interface
(config)#interface sa3	Enter sa Interface mode
(config-if)#port-channel min-bandwidth 30g	Configure min-bandwidth value on sa interface.
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

SW1

configure terminal	Enter Configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge type

(config)#vlan database	Create vlan database
(config-vlan)#vlan 600,601,502,101,100,300,401,402 bridge 1 state enable	Create Vlans
(config-vlan)#commit	Commit the candidate configuration to the running Configuration.
(config-vlan)#exit	Exit the configure mode.
(config)#interface xe1	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#spanning-tree edgeport	Configure port as edgeport
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa1	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan add 100,101,300,401,402,502	Enable all VLAN identifiers on this interface.
(config-if)#spanning-tree edgeport	Configure port as edgeport
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe2	Enter Interface mode

(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe3	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe4	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe6	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe7	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe8	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

SW2

configure terminal	Enter Configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge type
(config)#vlan database	Create vlan database

(config-vlan)#vlan 600,601,502,101,100,401,402 bridge 1 state enable	Create vlans
(config-vlan)#commit	Commit the candidate configuration to the running Configuration.
(config-vlan)#exit	Exit the configure mode.
(config)#interface xe5/1	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#spanning-tree edgeport	Configure port as edge port
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa3	Enter Interface mode
(config-if)# switchport	Make sa3 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan add 100,101,401,402,600,502	Enable all VLAN identifiers on this interface.
(config-if)#spanning-tree edgeport	Configure port as edge port
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe3/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running

	Configuration.
#configure terminal	Enter Configure mode.
(config)#interface xe3/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe3/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe1/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe1/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe1/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

This configuration is applicable for the dynamic LAG with MLAG topology except dynamic LAG interface creations, which needs to be referred from the dynamic LAG configurations given above.

Validation

When sa or po goes down due to min-link or min-bandwidth not satisfied, below validations to be done:

TOR 1

```
#sh int brief sa1
Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
```

```
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down

--------------------------------------------------------------------------------
Port-channel Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
sa1           AGG   1     trunk             down     PD(Min L/B)  0

#
#sh int brief po100

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
po100         AGG   1     trunk             down     PD(Min L/B)  0

#
#sh etherchannel
% Lacp Aggregator: po100
% Min-Bandwidth : 40g
% Protocol Down (Min L/B) : True
% Member:
   ce3/1
   ce3/2
   ce3/3
   ce3/4
-------------------------------------
% Lacp Aggregator: sa1
% Min-links : 3
% Protocol Down (Min L/B): True
% Member:
   ce2/2
   ce2/3
   ce2/4
-------------------------------------
% Lacp Aggregator: sa3
% Member:
   ce4/1
   ce4/2
   ce4/3
#
#sh running-config interface sa1
!
interface sa1
 switchport
 port-channel load-balance src-dst-mac
 port-channel min-links 3
 mlag 1
!
```

```
#sh static-channel-group 1
 Static Aggregator: sa1
 Minimum-Links 3
 Member Status
  ce2/2          down
  ce2/3          down
  ce2/4          down
#
#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: Layer2
  Admin Key: 0100 - Oper Key 0100
     Link: ce3/1 (5057) sync: 0
     Link: ce3/2 (5058) sync: 0
     Link: ce3/3 (5059) sync: 0
     Link: ce3/4 (5060) sync: 0
--------------------------------------
```

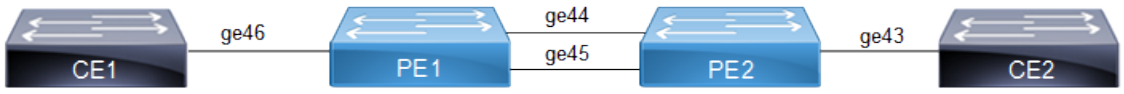
LACP Force-Up

In an aggregated environment, there are some parameters that are set for member ports in lag. Whenever the parameters are set and conditions are satisfied, the port channel will be in SYNC. If force-up mode is enabled for the member port, the port channel will always be in SYNC even if the parameters are not set i.e. the traffic will not be affected and the port channel will never go down.

LACP Force-up with Dynamic LAG

Topology

Figure 13. LACP force-up with dynamic LAG



CE1

`#configure terminal`	Enter configure mode.
`(config)#hostname CE1`	Configure host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan database`	Enter VLAN database mode.
`(config-vlan)#vlan 2-100 bridge 1 state enable`	Configure VLAN for the bridge
`(config-vlan)#commit`	Commit the candidate configuration to the running Configuration.
`(config-vlan)#exit`	Exit the VLAN configure mode.
`(config)#interface ge46`	Enter interface mode
`(config-if)#switchport`	Make interface as Switchport
`(config-if)#bridge-group 1`	Associate the interface to bridge

© 2026 IP Infusion Inc. Proprietary

(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface po1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed vlan all for the hybrid mode
(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ge44	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#exit	Exit interface mode.
(config)#interface ge45	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

CE2

#configure terminal	Enter configure mode.
(config)#hostname CE2	Configure host name
(config)#bridge 1 protocol provider-rstp edge	Create provider rstp edge bridge
(config)#vlan database	Enter vlan database mode
(config-vlan)#vlan 2-100 type customer bridge 1 state enable	Configure customer VLAN for the bridge
(config-vlan)#vlan 100 type service point-point bridge 1 state enable	Configure service VLAN for the bridge
(config)#exit	Exit vlan database mode
(config)#cvlan registration table map1 bridge 1	Creating registration table
(config-cvlan-registration)#cvlan 2-100 svlan 100	Mapping cvlan to svlan
(config-cvlan-registration)#commit	Commit the candidate configuration to the running Configuration.

© 2026 IP Infusion Inc. Proprietary

`(config-cvlan-registration)#exit`	Exit the cvlan registration mode.
`(config)#interface ge43`	Enter interface mode
`(config-if)#switchport`	Make interface as Switchport
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode provider-network`	Configure the mode as provider-network
`(config-if)# switchport provider-network allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface po1`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port
`(config-if)#bridge-group 1`	Associate the interface with bridge group 1
`(config-if)#switchport mode customer-edge hybrid`	Set the switching characteristics of this interface to customer-edge hybrid
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan all
`(config-if)#switchport customer-edge vlan registration map1`	Configuring the registration table mapping on lag interface
`(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ge44`	Enter interface mode
`(config-if)#channel-group 1 mode active`	Adding interface to channel-group 1
`(config-if)#lacp force-up`	Enable lacp force-up for the member port interface
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.
`(config)#interface ge45`	Enter interface mode
`(config-if)#channel-group 1 mode active`	Adding interface to channel-group 1
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode.

Send L2 traffic with incremental source mac of 1000 and with VLAN 100 from CE1 and with incremental source mac of 1000 and with SVLAN 100(TPID 0x88a8), CVLAN 100 from CE2.

© 2026 IP Infusion Inc. Proprietary

Validation

CE1

```
CE1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 2001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 2001

CE1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5043) sync: 1
     Link: ge45 (5046) sync: 1

CE1#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ge44                363.65         710252        772.76         1420506
 ge45                363.63         710222        0.00           0
 ge46                772.77         1420525       727.31         1420526
 po1                 728.56         1422971       774.09         1422966

CE2#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 2001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 2001

CE2#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ge43                774.26         1423267       784.17         1361411
 ge44                774.26         1423268       364.36         711634
 ge45                0.00           0             364.36         711634
 po1                 774.26         1423267       728.71         1423267

CE2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5020) sync: 1
     Link: ge45 (5022) sync: 1
```

On server side (PE1) to make LAG down you can unconfigure the channel-group 1 configurations and verify force-up is getting enabled in PE2.

To simulate the force-up:

`PE1(config)#interface ge44`	Enter interface mode.
`PE1(config-if)#no channel-group`	Removing channel-group configurations from interface.
`PE1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`PE1(config)#interface ge45`	Enter interface mode.

`PE1(config-if)#no channel-group`	Removing channel-group configurations from interface.
`PE1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`PE1(config-if)#exit`	Exit interface mode.

PE2

```
PE2#show interface brief | include po1
po1           AGG   1     customer-edge     up       none    1g

PE2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5020) sync: 0 (force-up)
     Link: ge45 (5022) sync: 0

PE2#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
  Mac address: b8:6a:97:4d:65:d5
  Admin Key: 0001 - Oper Key 0001
   Actor LAG ID- 0x8000,b8-6a-97-28-a5-c0,0x0001
   Receive link count: 0 - Transmit link count: 0
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
    Link: ge44 (5020) sync: 0 (force-up)
    Link: ge45 (5022) sync: 0
  Collector max delay: 5
```

To forward traffic from ge44 of PE1:

`PE1(config)#interface ge44`	Enter interface mode.
`PE1(config-if)#switchport`	Make the interface as switch port.
`PE1(config-if)#bridge-group 1`	Associate the interface to bridge.
`PE1(config-if)#switchport mode hybrid`	Configure the mode as hybrid.
`PE1(config-if)#switchport hybrid allowed vlan all`	Configure allowed vlan all for the hybrid mode.
`PE1(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds.
`PE1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`PE1(config-if)#exit`	Exit the configure mode.

```
PE2#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ge43                774.25         1423257       784.17         1361400
 ge44                774.25         1423258       728.71         1423257
 ge45                0.00           0             0.00           0
 po1                 774.25         1423247       728.70         1423245
 PE2#
PE1#show interface counters rate mbps
```

```
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ge44                657.67         1284505       640.77         1177884
 ge45                0.00           0             0.00           0
 ge46                772.71         1420426       603.08         1177886
```

LACP Aggregator Force-up

Overview

Link Aggregation Control Protocol (LACP) facilitates the bundling of multiple physical interfaces into a single logical link, enhancing bandwidth and providing redundancy. Aggregator Force-Up extends LACP functionality by enabling links to be forced into an active state without successful LACP negotiation. This is crucial in environments where connected devices, such as servers during boot stages, might not support LACP or have temporary configuration limitations.

Feature Characteristics

- Allows all interfaces within a Link Aggregation Group (LAG) or MLAG to be manually set to an active state without requiring successful LACP negotiation.
- In force-up state, each physical interface in a LAG or MLAG acts as an independent bridge-port, handling MAC learning and L2 traffic independently rather than as part of the aggregated link.
- LACP agg force-up can be enabled in LAG or MLAG interface not in physical interface.
- Interfaces automatically transition out of force-up state and resume normal LACP-based operations when LACP communication is successfully established on any of the links.

Notes:

- An LACP link configured with `force-up` enters the force-up state `90 seconds` after the parent LAG stops receiving LACP PDUs on all member links. The 90-second period is the `force-up activation delay timer`, which starts when the links transition to the `expiry or defaulted MUX state`.
- A force-up configured LACP link immediately exits the force-up state when the parent LAG interface receives LACP PDUs on any member link.
- The `force-up activation delay timer` restarts whenever a member LACP link in the parent LAG flaps.

Benefits

- Keeps network traffic flowing even when there's a synchronization issue, preventing data loss and maintaining connectivity.
- Automatically switches the links to independent operation mode without manual intervention, simplifying network management.
- When synchronization is restored on any link, the LAG returns to its efficient, aggregated state.

© 2026 IP Infusion Inc. Proprietary

LACP Aggregator Force-up for Dynamic LAG Configuration

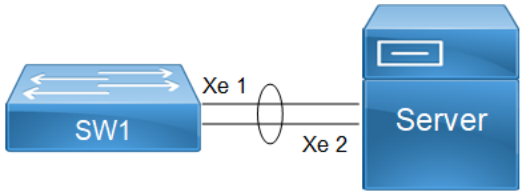
Set up LACP Aggregator Force-Up to maintain network connectivity even when synchronization with the LACP partner is lost all member links in the LAG.

Topology

The provided topology diagram consists of a switch and a server (SW1 and server) connected to each other.

SW1: This the central switch in the topology. They are connected through two interfaces (xe1 and xe2).

Figure 14. LACP Aggregator Force-up for Dynamic LAG



To configure LACP Aggregator Force-up for LAG on switch SW1 and Server, follow the steps:

1. Create VLANs and Bridge:
   a. Establish a bridge instance (`bridge 1`) with RSTP as the spanning tree protocol for VLAN-based bridging.
   b. Define VLANs 2 to 100 and associate it with (`bridge 1`) to enable the VLANs for bridging operations, and commit the changes.

```
SW1(config)# bridge 1 protocol rstp vlan-bridge
SW1(config)# vlan database
SW1(config-vlan)# vlan 2-100 bridge 1 state enable
SW1(config-vlan)# commit
SW1(config-vlan)# exit
```

2. Configure Port-channel Interface (`po1`) Aggregate Link between SW1 and Server:
   a. Enter configuration mode for Port-channel interface 1 (`po1`).
   b. Configure (`po1`) as a Layer 2 switchport.
   c. Associate (`po1`) with `bridge group 1` so that it operates within the defined bridging context.
   d. Set (`po1`) to trunk mode to carry traffic for multiple VLANs.
   e. Configure (`po1`) to carry traffic for all VLANs, facilitating communication across different VLANs within the network.
   f. Configure channel-group 1 for (`po1`) in active mode for LACP operation:

```
SW1(config)# interface po1
SW1(config-if)# switchport
SW1(config-if)# bridge-group 1
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan all
SW1(config-if)# commit
SW1(config-if)# exit
```

3. Configure the Interfaces (`xe1 and xe2`):
   a. Enter configuration mode for each interface (xe1 and xe2).

© 2026 IP Infusion Inc. Proprietary

b. Assign (`xe1` and `xe2)` to channel-group 1 to participate in the LACP bundle formed by po1, ensuring load balancing and redundancy across member links.

> **Note:** Follow similar steps for SW2, adjusting interface names and configurations accordingly to maintain consistency across the network.

```
SW1(config)# interface xe1
  SW1(config-if)# channel-group 1 mode active
  SW1(config-if)# exit

  SW1(config)# interface xe2
  SW1(config-if)# channel-group 1 mode active
  SW1(config-if)# exit
```

4. Enable LACP Aggregator Force-Up on `po1`.

```
SW1(config)# interface po1
SW1(config-if)# lacp agg force-up
SW1(config-if)# commit
SW1(config-if)# exit
```

LACP Aggregator Force-up for MLAG Configuration

Set up LACP Aggregator Force-Up to maintain network connectivity even when synchronization with the LACP partner is lost on all member links in the MLAG.

Topology

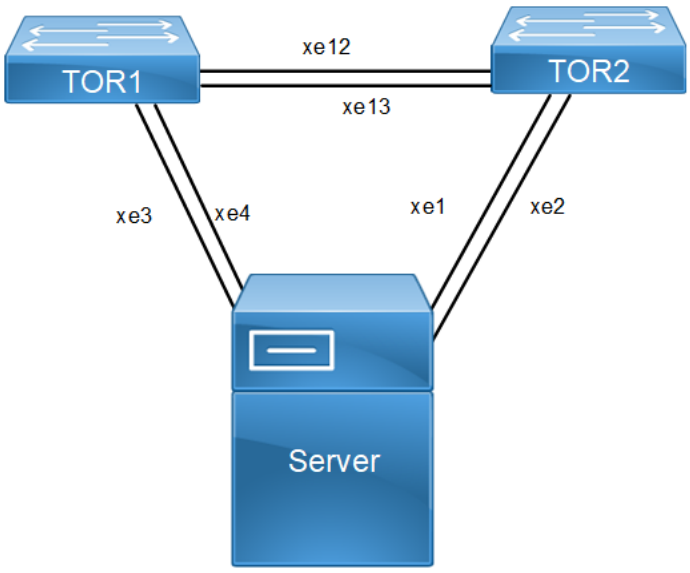
This topology showcases a network setup designed to maximize redundancy, load balancing, and fault tolerance using MLAG and LACP with a Force-Up feature. The network is structured around top-of-rack switches (TOR1 and TOR2).

TOR1 and TOR2 operate as MLAG peers. This setup allows to appear as a single logical switch to connected device (Server).

Traffic can be distributed across the (TOR1 and TOR2), and if one switch fails, the other can handle the load without service interruption. The LACP Aggregator Force-Up feature is enabled to keep port channel member ports operationally up if all member links go down.

This ensures that the remains up, facilitating immediate traffic redirection and avoiding delays associated with LACP negotiation. Both TOR1 and TOR2 connect to server through multiple links, providing path redundancy.If any link or switch fails, the remaining links and switches maintain network connectivity and balance the load, thus avoiding single points of failure.

Figure 15. LACP Aggregator Force-up for MLAG



Configuration

To configure LACP Aggregator Force-up for MLAG on switches TOR1, and TOR2, follow the steps:

1. Create VLANs and Bridge on TOR1,and TOR2:
   a. Establish a bridge instance (`bridge 1`) with RSTP as the spanning tree protocol for VLAN-based bridging.
   b. Define required vlans for example: VLANs 2 to 100 and associate it with (`bridge 1`) to enable the VLANs for bridging operations, and commit the changes.

```
TOR1(config)# bridge 1 protocol rstp vlan-bridge
  TOR1(config)# vlan database
  TOR1(config-vlan)# vlan 2-100 bridge 1 state enable
  TOR1(config-vlan)# commit
  TOR1(config-vlan)# exit
```

2. Configure Port Channels (`po`) as trunk ports allowing all VLANs, and commit the changes: For TORs: Configure interface `mlag1,po1,po3` as needed:
   a. Enter configuration mode for (`mlag1`).
   b. Configure (`mlag1`) as a Layer 2 switchport.
   c. Associate (`mlag1`) with `bridge group 1` so that it operates within the defined bridging context.
   d. Set (`mlag1`) to trunk mode to carry traffic for multiple VLANs.

```
TOR1(config)#interface mlag1
TOR1(config-if)#switchport
TOR1(config-if)#bridge-group 1
TOR1(config-if)#switchport mode trunk
TOR1(config-if)#switchport trunk allowed vlan all
TOR1(config-if)#mode active-active
TOR1(config-if)#commit
TOR1(config-if)#exit
```

   e. Configure po1 and map to mlag1.

```
TOR1(config)#interface po1
TOR1(config-if)#switchport
TOR1(config-if)#mlag 1
TOR1(config-if)#commit
```

   f. Configure po3.

```
TOR1(config)#interface po3
TOR1(config-if)#switchport
TOR1(config-if)#commit
```

3. Configure the Interfaces (For TOR1 `xe3, xe4, xe12, and xe13, and` For TOR2 `xe1, xe2, xe12, and xe13):`
   a. Enter configuration mode for each interface.
   b. Assign to channel-group 1 to participate in the LACP bundle formed by po1, ensuring load balancing and redundancy across member links.
   c. Configure as a Layer 2 switchport with trunk mode and allow all VLANs to facilitate communication across different VLANs within the network.

```
 TOR1(config)#interface xe3
 TOR1(config-if)#channel-group 1 mode active
 TOR1(config-if)#exit
 TOR1(config)#interface xe4
 TOR1(config-if)#channel-group 1 mode active
 TOR1(config-if)#commit
 TOR1(config-if)#exit
 TOR1(config)#interface xe12
 TOR1(config-if)#channel-group 3 mode active
 TOR1(config-if)#exit
 TOR1(config)#interface xe13
 TOR1(config-if)#channel-group 3 mode active
 TOR1(config-if)#commit
 TOR1(config Enable LACP Aggregator Force-up on MLAG interfaces in TOR1 and TOR2:
 TOR1(config)#interface mlag1
 TOR1(config-if)#lacp agg force-up
 TOR1(config-if)#commit
 TOR1(config-if)#exit
```

Note: Similarly, follow the steps to configure `mlag1` for TOR2.

Sample Configuration Snapshot

Dynamic LAG:

```
bridge 1 protocol rstp vlan-bridge
vlan database
 vlan 2-4000 bridge 1 state enable
!
interface po1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 load-interval 30
 port-channel load-balance rtag7
 lacp agg force-up
!
interface xe1
 channel-group 1 mode active
!
interface xe2
 channel-group 1 mode active
!
 exit
```

MLAG:

```
bridge 1 protocol rstp vlan-bridge
```

```
vlan database
 vlan 2-4000 bridge 1 state enable
!
interface mlag1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 load-interval 30
 lacp agg force-up
!
interface po1
 port-channel load-balance rtag7
 switchport
 mlag 1
!
interface po3
 switchport
 port-channel load-balance rtag7
!
interface xe3
 channel-group 1 mode active
!
interface xe4
 channel-group 1 mode active
!
interface xe12
 channel-group 3 mode active
!
interface xe13
 channel-group 3 mode active
!
 exit
!
mcec domain configuration
 domain-address 1111.2222.3333
 domain-system-number 1
 intra-domain-link po3
```

Dynamic LAG Validation

- Verify `agg force-up` is enabled in SW1.

```
SW1#show etherchannel summary
  Aggregator po1 100001
  Port-channel Force-Up Mode : Activated
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: xe1 (5034) sync: 0 (agg-force-up)
     Link: xe2 (5035) sync: 0 (agg-force-up)
```

MLAG Validation

- Verify `agg force-up` is enabled in TOR1.

```
TOR1#show mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : po3
Domain Adjacency                : UP
MCEC PDU local version          : 1
MCEC PDU peer version           : 1
```

```
Domain Sync via                : Intra-domain-interface
Peer SVI interface MAC Address : 5C.07.58.6F.83.5E

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Physical properties Digest   : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22
  Total Bandwidth              : 0
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Active
  Current Mlag state           : Standby
  Aggregator Force-Up Mode     : Activated

TOR1#show etherchannel summary
  Aggregator po1 100001
  Mlag Force-Up Mode : Activated
  Aggregator Type: Layer2
  Parent Aggregator : Active mlag1
  Admin Key: 16385 - Oper Key 16385
     Link: xe3 (5004) sync: 0 (agg-force-up) (Mlag-active-link)
     Link: xe4 (5008) sync: 0 (agg-force-up) (Mlag-active-link)
-------------------------------------

  Aggregator po3 100003
  Aggregator Type: Layer2
  Admin Key: 0003 - Oper Key 0003
     Link: xe12 (5011) sync: 1
     Link: xe13 (5015) sync: 1
```

Implementation Examples

Dynamic Port-Channel configuration:

Both interfaces in the dynamic port-channel must support force-up to allow the server to boot using any connected link.

During the server's boot stage, the force-up feature ensures that any one of the connected interfaces can be used to initiate and complete the boot process, while the other interface remains inactive until LACP communication is established.

MLAG Configuration Requirement:

To support network booting, the MLAG domain is configured with LACP force-up. This allows at least one link to become active, ensuring the server can boot over the network.

Typically, all interfaces (`xe1, xe2, xe3, xe4`) need to be prepared to provide force-up capabilities to handle server booting flexibility.

Traffic Management:

When in force-up state, each interface operates as an individual bridge-port.

CLI Command

The LACP aggregator force-up feature introduces the `lacp agg force-up` configuration command.

lacp agg force-up

Use this command to configure Aggregator Force-up on Dynamic LAG or Dynamic MLAG interface.

If this command is enabled and LACP Partner sync is not established on any of the member links in Aggregator then, all the member links will enter Aggregator Force-up state in which they will act like individual bridge ports with respect to Layer2 Learning, Flooding, or Forwarding. Once LACP Partner sync is established on atleast one member link, the members will exit Aggregator Force-up and become part of the LAG that is normal LAG functioning is retained.

Use `no lacp agg force-up` parameter of this command to disable the aggregator force-up state.

Command Syntax

```
lacp agg force-up
no lacp agg force-up
```

Parameters

None

Default

Disabled

Command Mode

Interface mode

Applicability

Introduced the `lacp agg force-up` parameter in theOcNOS version 6.5.2

Example

The following sequence of commands is used to configure the LACP Aggregator Force-Up feature in MLAG:

```
#configure terminal
(config)#interface mlag1
(config-if)#lacp agg force-up
(config-if)#exit
```

The following sequence of commands is used to configure the LACP Aggregator Force-Up feature in Dynamic LAG:

```
#configure terminal
(config)#interface po1
(config-if)#lacp agg force-up
(config-if)#exit
```

Glossary

The following provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
Link Aggregation Control Protocol (LACP)	A protocol provides a way to bundle several physical ports together to form a single logical channel for the purpose of increasing bandwidth and providing redundancy.
Aggregator	A group of physical interfaces that are combined into a single logical interface (known as a port channel or link aggregation group) for load balancing and redundancy.
Aggregator Force-Up	A feature that keeps the members of LACP aggregator (port channel) operationally

	up, even if all member links are down. This is typically used in scenarios where there is server boot up.
Multi-Chassis Link Aggregation Group (MLAG)	Creation of a single logical link aggregation group across two separate switches, providing redundancy and load balancing across multiple chassis.
Port Channel (Po)	A logical grouping of multiple physical network interfaces, combined to act as a single interface. This allows for increased bandwidth and redundancy.
Active Mode	In LACP, active mode means the device actively initiates LACP negotiations and participates in the formation of LACP port channels.
Passive Mode	In LACP, passive mode means the device only responds to LACP packets but does not initiate the formation of LACP port channels.

© 2026 IP Infusion Inc. Proprietary

MLAG Configuration

This section contains a complete example of Multi-Chassis Link Aggregation (MLAG) configuration.

MLAG expands the concept of link aggregation so that it provides node-level redundancy by allowing two or more nodes to share a common LAG endpoint. It emulates multiple nodes to represent as a single logical node to the remote node running Link aggregation. As a result, even if one of the nodes is down there exists a path to reach the destination through the other nodes.

Note:

- MLAG is only compatible with VPWS.
- MLAG is supported only in Active-Standby mode.
- All MLAG nodes must have the same MAC table size - as specified by each node's switching ASIC forwarding profile limit.
- For multi-ASIC boards, performing measurements (as either sender or reflector) on LAG interfaces requires all LAG members to be located on the same ASIC.

The MLAG primary and secondary physical devices synchronize with each other to create a single logical domain called Multi-Chassis Ether Channel (MCEC) domain. The exchange of information between MLAG primary and secondary devices to maintain this MCEC domain can be done with the use of IDL and IDP.

Intra-Domain-Link (IDL)

This link is used by MLAG primary and secondary devices to synchronize the states between each other via MCEC packets to create the illusion of a single control plane. The MLAG peers use the IDL to exchange control information and coordinate with each other to ensure that data traffic is forwarded properly. The IDL interface is capable of carrying data traffic:

1. If a MLAG interface to which data traffic is destined is operationally down, the data traffic will be sent to MLAG peer device via IDL to avoid any loss.
2. If data traffic received on a MLAG device is destined for a host that is reachable via peer MLAG device only, then, the data traffic is sent over IDL to the peer MLAG device..

Intra-Domain-Peer (IDP)

This is an alternative way to synchronize the states between MLAG primary and secondary devices. In particular, it provides a Layer 3 communication path to carry MCEC packets. No data traffic is carried over the IDP. Hence, data traffic loss is expected, in case of MLAG interface failure.

Following are the possible types of interconnections for the IDP:

3. The `eth0` out-of-band management interface
4. It can be routed in-band over an L3 infrastructure

© 2026 IP Infusion Inc. Proprietary

Options to Configure Intra-Domain

With IDL only

The IDL uses either a single physical or an aggregated ethernet interface. However, if IDL fails, the states between MLAG devices can no longer be synchronized. Configuring the IDL along with backup IDP provides more robustness during network disruptions.

Case-1: IDL Link Failure

- If strict Active-Standby is enabled: The standby node does not become active.
- If strict Active-Standby is disabled: The standby node becomes active, resulting in a split-brain (Active-Active) scenario.

Case-2: MLAG Active Device Failure/Reload

- If the device is reloaded by the admin via OcNOS commands: The standby node becomes active.
- If the device reboots due to any other reason:
  - If strict Active-Standby is enabled: The standby node does not become active.
  - If strict Active-Standby is disabled: The standby node becomes active.

With IDP only

The IDP without IDL can be used in cases where data traffic transmission between the primary and secondary MLAG devices are not needed.

Case 1: IDP link failure

- Behavior is the same as the With IDL only use case.

Case 2: MLAG active device Failure/Reload

- Behavior is the same as the With IDL only use case.

With IDL and IDP

When the IDL fails, the IDP (if configured) can be used as a backup mechanism to synchronize the states between MLAG peer devices. Also, it helps the MLAG switch to determine whether the IDL itself has failed or whether the peer MLAG device is operationally down. When both the IDL and IDP are configured, following are the behavior of the MLAG devices when the link/device fails:

Case-1: IDP Link failure

In this case, no impact on MLAG, therefore, no network downtime.

Case-2: IDL Link Failure

In this case, MCEC domain adjacency comes up via IDP. When the IDL link fails, MLAG Active-Active will be operational as MLAG Active-Standby (Safe Mode) to minimize network disruptions caused by Dual-Active (Split Brain) mode. It is expected that the traffic loss for hosts directly connected to the Standby device as data traffic cannot be carried over in the IDP.

Case-3: MLAG Peer Device Failure/Reload

When MLAG peer device reloads, MCEC domain adjacency goes down. The traffic is forwarded through the operational links in the Active MLAG device.

Case-4: Both IDL and IDP Failure

© 2026 IP Infusion Inc. Proprietary

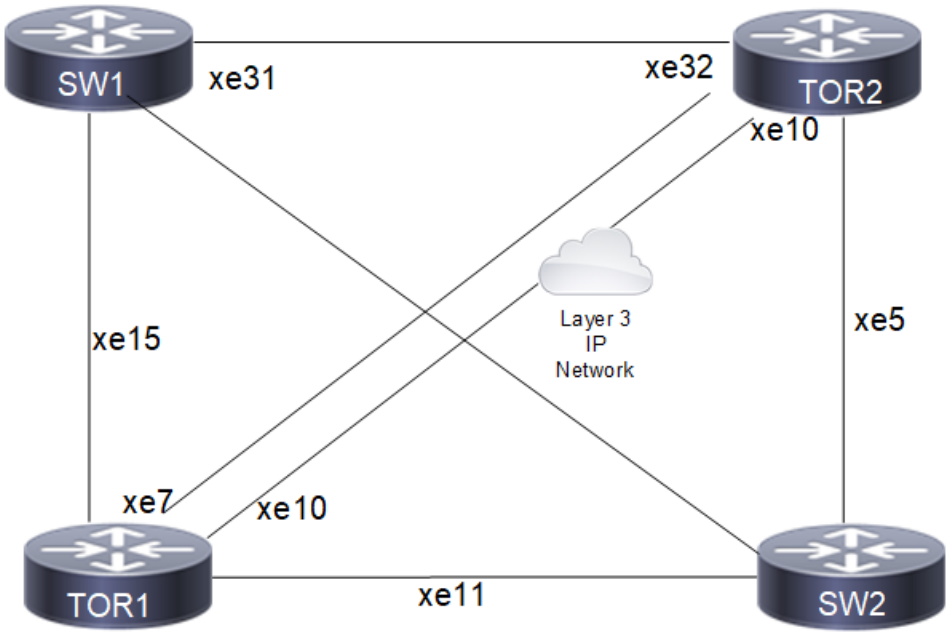
If both IDL and IDP link fails, Dual-Active (Split brain scenario) can be expected. There will be network instability/disruption as both MLAG nodes are operating as Active-Active with MCEC Domain Adjacency down.

In the below example TOR1 and TOR2 forms a MLAG domain.

TOR1 and TOR2 forms a domain and thus provides the redundancy. Even if TOR1 or TOR2 is down, there exist a redundant path to forward the traffic.

Topology

Figure 16. MLAG with IDL and IDP Topology



Configuration

Switch 1

`SW1#configure terminal`	Enter the config terminal.
`(config)#hostname SW1`	Assign the hostname for the router.
`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge.
`SW1(config)#vlan database`	Enter the VLAN database.
`SW1(config-vlan)#vlan 2-1002 bridge 1 state enable`	Create the VLANs.
`SW1(config-vlan)#exit`	Exit the VLAN database.
`SW1(config)#int po1`	Enter the interface mode.
`SW1(config-if)#switchport`	Configure the interface as Layer 2.
`SW1(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface.

© 2026 IP Infusion Inc. Proprietary

`SW1(config-if)#bridge-group 1`	Assign the bridge to the interface.
`SW1(config-if)#switchport mode trunk`	Configure the interface as trunk mode.
`SW1(config-if)#switchport trunk allowed vlan all`	Configure the interface to allow all VLAN ids.
`SW1(config-if)#load-interval 30`	Configure load interval.
`SW1(config-if)#mtu 9216`	Set mtu value.
`SW1(config-if)#mode active-active`	Mode needs to be configured as active-active.
`SW1(config-if)#exit`	Exit the interface mode.
`SW1(config)#int xe15`	Enter the interface mode.
`SW1(config-if)#channel-group 1 mode active`	Add the interface as member of LAG interface.
`SW1(config-if)#int xe31`	Enter the interface mode.
`SW1(config-if)#channel-group 1 mode active`	Add the interface as member of LAG interface.
`SW1(config-if)#commit`	Commit the configure on the node.
`SW1(config-if)#exit`	Exit the interface mode.

TOR-1

`TOR1#configure terminal`	Enter the config terminal.
`TOR1(config)#hostname TOR1`	Assign the hostname for the router.
`TOR1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge.
`TOR1(config)#vlan database`	Enter the VLAN database.
`TOR1(config-vlan)#vlan 2-1002 bridge 1 state enable`	Create the VLANs.
`TOR1(config-vlan)#exit`	Exit the VLAN database.
`TOR1(config)#int mlag1`	Create the MLAG interface.
`TOR1(config-if)#switchport`	Configure the interface as Layer 2.
`TOR1(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface.
`TOR1(config-if)#bridge-group 1`	Assign the bridge to the interface.
`TOR1(config-if)#switchport mode trunk`	Configure the interface as trunk mode.
`TOR1(config-if)#switchport trunk allowed vlan all`	Configure the interface to allow all VLAN ids.
`TOR1(config-if)#load-interval 30`	Configure load interval.
`TOR1(config-if)#mtu 9216`	Set mtu value.
`TOR1(config-if)#mode active-active`	Mode needs to be configured as active-active.
`TOR1(config-if)#exit`	Exit the interface mode.
`TOR1(config)#int mlag2`	Create the MLAG interface.
`TOR1(config-if)#switchport`	Configure the interface as Layer 2.
`TOR1(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface.
`TOR1(config-if)#bridge-group 1`	Assign the bridge to the interface.

© 2026 IP Infusion Inc. Proprietary

`TOR1(config-if)#switchport mode trunk`	Configure the interface as trunk mode.
`TOR1(config-if)#switchport trunk allowed vlan all`	Configure the interface to allow all VLAN ids.
`TOR1(config-if)#load-interval 30`	Configure load interval.
`TOR1(config-if)#mtu 9216`	Set mtu value.
`TOR1(config-if)#mode active-active`	Mode needs to be configured as active-active.
`TOR1(config-if)#exit`	Exit the interface mode.
`TOR1(config)#int po1`	Create the port channel interface.
`TOR1(config-if)#switchport`	Configure the interface as Layer 2.
`TOR1(config-if)#mlag 1`	Bind MLAG to the port channel.
`TOR1(config-if)#exit`	Exit the interface mode.
`TOR1(config)#int po2`	Create the port channel interface
`TOR1(config-if)#switchport`	Configure the interface as Layer 2.
`TOR1(config-if)#mlag 2`	Bind MLAG to the port channel.
`TOR1(config-if)#exit`	Exit the interface mode.
`TOR1(config)#interface xe7`	Configure xe7 interface mode only if the IDL is required.
`TOR1(config-if)#switchport`	Configure the interface as Layer 2 only if the IDL is required.
`TOR1(config-if)#exit`	Exit the interface mode.
`TOR1(config-if)#interface xe10`	Configure xe10 interface mode only if the IDP is required..
`TOR1(config-if)#ip address 2.2.2.2/24`	Configure source IP address for IDP only if the IDP is required.
`TOR1(config)#int xe15`	Enter the interface mode.
`TOR1(config-if)#channel-group 1 mode active`	Add the interface as member of LAG interface.
`TOR1(config-if)#exit`	Exit the interface mode.
`TOR1(config)#int xe11`	Enter the interface mode.
`TOR1(config-if)#channel-group 2 mode active`	Add the interface as member of LAG interface.
`TOR1(config-if)#exit`	Exit the interface mode.
`TOR1(config)#mcec domain configuration`	Enter the MCEC mode.
`TOR1(config-mcec-domain)#domain-system-number 1`	Assign the domain system number for MLAG interface.
`TOR1(config-mcec-domain)#domain-address 1111.2222.3333`	Assign the domain address.
`TOR1(config-mcec-domain)#domain-hello-timeout short`	Assign the domain hello timeout.
`TOR1(config-mcec-domain)#intra-domain-link xe7`	Assign the interface as IDL only if the IDP is required.
`TOR1(config-mcec-domain)#)#intra-domain-peer 2.2.2.3 source-address 2.2.2.2`	Configure source ip address for IDP only if the IDP is required.

`TOR1(config-mcec-domain)#exit`	Exit the MCEC domain.
`TOR1(config-mcec-domain)#commit`	Commit the configure on the node.
`TOR1(config)#exit`	Exit the config terminal.

TOR-2

`TOR2#configure terminal`	Enter the config terminal.
`TOR2(config)#hostname TOR2`	Assign the hostname for the router.
`TOR2(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge.
`TOR2(config)#vlan database`	Enter the VLAN database.
`TOR2(config-vlan)#vlan 2-1002 bridge 1 state enable`	Create the VLANs.
`TOR2(config-vlan)#exit`	Exit the VLAN database.
`TOR2(config)#int mlag1`	Create the MLAG interface.
`TOR2(config-if)#switchport`	Configure the interface as Layer 2.
`TOR2(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface.
`TOR2(config-if)#bridge-group 1`	Assign the bridge to the interface.
`TOR2(config-if)#switchport mode trunk`	Configure the interface as trunk mode.
`TOR2(config-if)#switchport trunk allowed vlan all`	Configure the interface to allow all VLAN ids.
`TOR2config-if)#load-interval 30`	Configure load interval.
`TOR2(config-if)#mtu 9216`	Set mtu value.
`TOR2(config-if)#mode active-active`	Mode needs to be configured as active-active.
`TOR2(config-if)#exit`	Exit the interface mode.
`TOR2(config)#int mlag2`	Create the MLAG interface.
`TOR2(config-if)#switchport`	Configure the interface as Layer 2.
`TOR2(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface.
`TOR2(config-if)#bridge-group 1`	Assign the bridge to the interface.
`TOR2(config-if)#switchport mode trunk`	Configure the interface as trunk mode.
`TOR2(config-if)#switchport trunk allowed vlan all`	Configure the interface to allow all VLAN ids.
`TOR2config-if)#load-interval 30`	Configure load interval.
`TOR2(config-if)#mtu 9216`	Set mtu value.
`TOR2(config-if)#mode active-active`	Mode needs to be configured as active-active.
`TOR2(config-if)#exit`	Exit the interface mode.
`TOR2(config)#int po1`	Create the port channel interface
`TOR2(config-if)#switchport`	Configure the interface as Layer 2
`TOR2(config-if)#mlag 1`	Bind MLAG to the port channel.
`TOR2(config-if)#exit`	Exit the interface mode.

© 2026 IP Infusion Inc. Proprietary

`TOR2(config)#int po2`	Create the port channel interface.
`TOR2(config-if)#switchport`	Configure the interface as Layer 2.
`TOR2(config-if)#mlag 2`	Bind MLAG to the port channel.
`TOR2(config-if)#exit`	Exit the interface mode.
`TOR2(config)#interface xe7`	Enter the interface mode
`TOR2(config-if)#switchport`	Configure the interface as Layer 2.
`TOR2(config-if)#interface xe10`	Enter the interface mode.
`TOR2(config-if)#ip address 2.2.2.3/24`	Configure source ip address for IDP only if the IDP is required.
`TOR2(config-if)#exit`	Exit the interface mode.
`TOR2(config)#int xe32`	Enter the interface mode.
`TOR2(config-if)#channel-group 1 mode active`	Add the interface as member of LAG interface.
`TOR2(config-if)#exit`	Exit the interface mode.
`TOR2(config)#int xe5`	Enter the interface mode
`TOR2(config-if)#channel-group 2 mode active`	Add the interface as member of LAG interface.
`TOR2(config-if)#exit`	Exit the interface mode.
`TOR2(config)#mcec domain configuration`	Enter the MCEC mode.
`TOR2(config-mcec-domain)#domain-system-number 2`	Assign the domain system number for MLAG interface.
`TOR2(config-mcec-domain)#domain-address 1111.2222.3333`	Assign the domain address.
`TOR2(config-mcec-domain)#domain-hello-timeout short`	Assign the domain hello timeout.
`TOR2(config-mcec-domain)#intra-domain-link xe7`	Assign the interface as IDL only if the IDL is required.
`TOR2(config-mcec-domain)#)#intra-domain-peer 2.2.2.2 source-address 2.2.2.3`	Configure source ip address for IDP only if the IDP is required.
`TOR2(config-mcec-domain)#exit`	Exit the MCEC domain.
`TOR2(config-mcec-domain)#commit`	Commit the configure on the node.
`TOR2(config)#exit`	Exit the config terminal.

Switch 2

`SW2#configure terminal`	Enter the config terminal.
`SW2(config)#hostname SW2`	Assign the hostname for the router.
`SW2(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge.
`SW2(config)#vlan database`	Enter the VLAN database
`SW2(config-vlan)#vlan 2-1002 bridge 1 state enable`	Create the VLANs.
`SW2(config-vlan)#exit`	Exit the VLAN database
`SW2(config)#int po2`	Enter the interface mode

© 2026 IP Infusion Inc. Proprietary

SW2(config-if)#switchport	Configure the interface as Layer 2
SW2(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface.
SW2(config-if)#bridge-group 1	Assign the bridge to the interface.
SW2(config-if)#switchport mode trunk	Configure the interface as trunk mode.
SW2(config-if)#switchport trunk allowed vlan all	Configure the interface to allow all VLAN ids.
SW2(config-if)#load-interval 30	Configure load interval.
SW2(config-if)#mtu 9216	Set mtu value.
SW2(config-if)#mode active-active	Mode needs to be configured as active-active.
SW2(config-if)#exit	Exit the interface mode.
SW2(config)#int xe11	Enter the interface mode.
SW2(config-if)#channel-group 2 mode active	Add the interface as member of LAG interface.
SW2(config-if)#int xe5	Enter the interface mode.
SW2(config-if)#channel-group 2 mode active	Add the interface as member of LAG interface.
SW2(config-if)#commit	Commit the configure on the node.
SW2(config-if)#exit	Exit the interface mode.

Validation

Switch 1

```
SW1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: xe15 (5015) sync: 1
     Link: xe31 (5031) sync: 0
SW1#

SW1#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
  Mac address: 34:17:eb:e4:af:10
  Admin Key: 0001 - Oper Key 0001
   Actor LAG ID- 0x8000,34-17-eb-4b-af-00,0x0001
   Receive link count: 1 - Transmit link count: 1
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,11-11-22-22-33-33,0x4001
    Link: xe15 (5015) sync: 1
    Link: xe31 (5031) sync: 0
  Collector max delay: 5
SW1#
```

TOR 1

```
TOR1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 16385 - Oper Key 16385
     Link: xe15 (5015) sync: 1 (Mlag-active-link)
--------------------------------------
  Aggregator po2 100002
  Aggregator Type: Layer2
  Admin Key: 16386 - Oper Key 16386
```

© 2026 IP Infusion Inc. Proprietary

```
     Link: xe11 (5011) sync: 1 (Mlag-active-link)
TOR1#

TOR1#show mlag domain summary

------------------------------------
Domain Configuration
------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : xe7
Source Address                  : 2.2.2.2
Intra-domain-peer               : 2.2.2.3
Domain Adjacency                : UP
MCEC PDU local version          : 1
MCEC PDU peer version           : 1
Domain Sync via                 : Intra-domain-interface
Peer SVI interface MAC Address : E8.C5.7A.69.4C.B3

------------------------------------
MLAG Configuration
------------------------------------

MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22

  Total Bandwidth               : 10g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Standby
  Current Mlag state            : Active
  Switchover-mode               : Revertive


MLAG-2
  Mapped Aggregator             : po2
  Physical properties Digest    : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22

  Total Bandwidth               : 10g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Standby
  Current Mlag state            : Active
  Switchover-mode               : Revertive

TOR1#

TOR1#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
  Mac address: 3c:2c:99:1a:da:89
  Admin Key: 16385 - Oper Key 16385
   Actor LAG ID- 0x8000,11-11-22-22-33-33,0x4001
   Receive link count: 1 - Transmit link count: 1
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,34-17-eb-4b-af-00,0x0001
    Link: xe15 (5015) sync: 1 (Mlag-active-link)
  Collector max delay: 5
-------------------------------------------------
 Aggregator po2 100002
 Aggregator Type: Layer2
  Mac address: 3c:2c:99:1a:da:85
  Admin Key: 16386 - Oper Key 16386
   Actor LAG ID- 0x8000,11-11-22-22-33-33,0x4002
   Receive link count: 1 - Transmit link count: 1
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,3c-2c-99-c0-9f-79,0x0002
```

```
    Link: xe11 (5011) sync: 1 (Mlag-active-link)
  Collector max delay: 5
TOR1#

TOR1#show mcec statistics

Unknown MCCPDU received on the system            : 0

-------------------------------------
IDP                : xe7
-------------------------------------
   Valid RX Hello PDUs                           : 4054
   Valid TX Hello PDUs                           : 4191
   Valid RX Info PDUs                            : 66
   Valid TX Info PDUs                            : 16

   Valid RX Mac Sync PDUs                        : 53
   Valid TX Mac Sync PDUs                        : 61

MLAG 1
  Valid RX Info PDUs                             : 9
  Valid TX Info PDUs                             : 8

MLAG 2
  Valid RX Info PDUs                             : 12
  Valid TX Info PDUs                             : 8
TOR1#
```

TOR 2

```
TOR2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 32769 - Oper Key 16385
     Link: xe32 (5032) sync: 0 (Mlag-standby-link)
-------------------------------------
  Aggregator po2 100002
  Aggregator Type: Layer2
  Admin Key: 32770 - Oper Key 16386
     Link: xe5 (5005) sync: 0 (Mlag-standby-link)
TOR2#

TOR2#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
  Mac address: 80:a2:35:c4:e9:73
  Admin Key: 32769 - Oper Key 16385
   Actor LAG ID- 0x8000,11-11-22-22-33-33,0x4001
   Receive link count: 0 - Transmit link count: 0
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,34-17-eb-4b-af-00,0x0001
    Link: xe32 (5032) sync: 0 (Mlag-standby-link)
  Collector max delay: 5
-------------------------------------------------
 Aggregator po2 100002
 Aggregator Type: Layer2
  Mac address: 80:a2:35:c4:e9:58
  Admin Key: 32770 - Oper Key 16386
   Actor LAG ID- 0x8000,11-11-22-22-33-33,0x4002
   Receive link count: 0 - Transmit link count: 0
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,3c-2c-99-c0-9f-79,0x0002
    Link: xe5 (5005) sync: 0 (Mlag-standby-link)
  Collector max delay: 5
TOR2#
TOR2#
TOR2#show mlag domain summary
```

```
-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 2
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : xe7
Source Address                  : 2.2.2.3
Intra-domain-peer               : 2.2.2.2
Domain Adjacency                : UP
MCEC PDU local version          : 1
MCEC PDU peer version           : 1
Domain Sync via                 : Intra-domain-interface
Peer SVI interface MAC Address : 80.A2.35.3A.40.94

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22

  Total Bandwidth               : 10g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Standby
  Current Mlag state            : Standby
  Switchover-mode               : Revertive


MLAG-2
  Mapped Aggregator             : po2
  Physical properties Digest    : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22

  Total Bandwidth               : 10g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Standby
  Current Mlag state            : Standby
  Switchover-mode               : Revertive


TOR2#


TOR2#show mcec statistics

Unknown MCCPDU received on the system            : 0

-------------------------------------
IDP                 : xe7
-------------------------------------

  Valid RX Hello PDUs                          : 4177
   Valid TX Hello PDUs                          : 4159
   Valid RX Info PDUs                           : 16
   Valid TX Info PDUs                           : 66

   Valid RX Mac Sync PDUs                       : 74
   Valid TX Mac Sync PDUs                       : 30

MLAG 1
  Valid RX Info PDUs                            : 8
  Valid TX Info PDUs                            : 27

MLAG 2
  Valid RX Info PDUs                            : 8
  Valid TX Info PDUs                            : 39
TOR2#
```

Switch 2

```
SW2#show etherchannel summary
  Aggregator po2 100002
  Aggregator Type: Layer2
  Admin Key: 0002 - Oper Key 0002
     Link: xe5 (5005) sync: 0
     Link: xe11 (5011) sync: 1

SW2#show etherchannel detail
 Aggregator po2 100002
 Aggregator Type: Layer2
  Mac address: 3c:2c:99:26:e6:7f
  Admin Key: 0002 - Oper Key 0002
   Actor LAG ID- 0x8000,3c-2c-99-c0-9f-79,0x0002
   Receive link count: 1 - Transmit link count: 1
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,11-11-22-22-33-33,0x4002
    Link: xe5 (5005) sync: 0
    Link: xe11 (5011) sync: 1
  Collector max delay: 5
SW2#
```

MLAG Active-Active Dynamic Configuration

MLAG (also called DRNI, Distributed Resilient Network Interconnect) expands the concept of link aggregation so that it provides node-level redundancy by allowing two or more nodes to share a common LAG endpoint. MLAG emulates multiple nodes to represent as a single logical node to the remote node running link aggregation. As a result, even if one of the nodes is down there exists a path to reach the destination through the other nodes.

Notes:

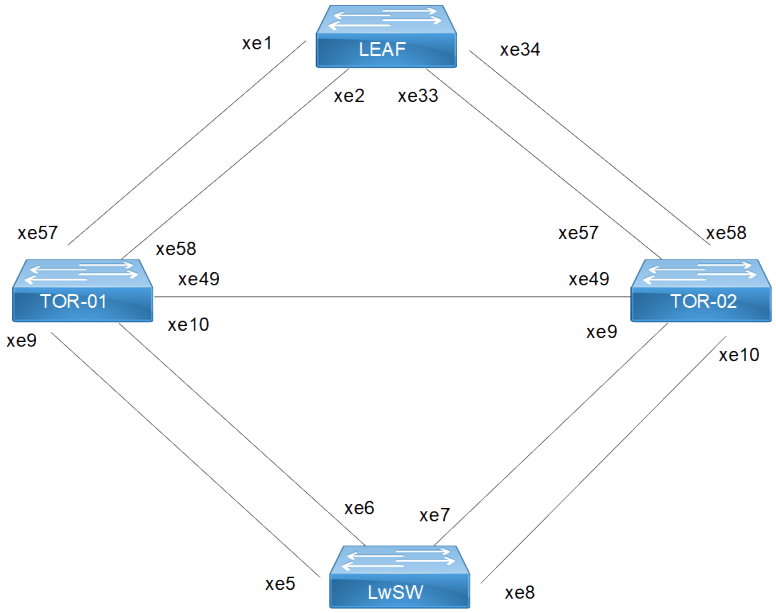
- MLAG is compatible only with a RSTP VLAN-aware bridge or a spanning tree disabled bridge.
- All MLAG nodes must have the same MAC table size as specified by each node's switching ASIC forwarding profile limit.

Topology

As per the topology, TOR 1 and TOR 2 form an MLAG domain. TOR 1 and TOR 2 are a single logical switch to LEAF and LwSW. Even if either TOR 1 or TOR 2 is down, there exists a path to reach other destinations.

© 2026 IP Infusion Inc. Proprietary

Figure 17. MLAG Active-Active Topology



LEAF

`#configure terminal`	Enter configure mode.
`(config)#hardware-profile filter egress-l2 enable`	Enable the hardware-profile filter
`(config)#bridge 1 protocol rstp vlan-bridge`	Create RSTP bridge 1.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)#interface po2`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface.
`(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`(config-if)#switchport trunk allowed vlan all`	Enable all VLAN identifiers on this interface.
`(config-if)#load-interval 30`	Configure load interval.
`(config-if)#mtu 9216`	Set mtu value.
`(config-if)#mode active-active`	Mode needs to be configured as active-active.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#channel-group 2 mode active`	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.

© 2026 IP Infusion Inc. Proprietary

(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe33	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe34	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.

LwSW

#configure terminal	Enter configure mode.
(config)#hardware-profile filter egress-l2 enable	Enable the hardware-profile filter
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface po1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#load-interval 30	Configure load interval.

© 2026 IP Infusion Inc. Proprietary

`(config-if)#mtu 9216`	Set mtu value.
`(config-if)#mode active-active`	Mode needs to be configured as active-active.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe5`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe6`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe7`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe8`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.

TOR-01

`#configure terminal`	Enter configure mode.
`(config)#hardware-profile filter egress-l2 enable`	Enable the hardware-profile filter
`(config)#interface mlag1`	Enter interface mode.
`(config-if)#mode active-active`	Mode need to be configured as active-active
`(config-if)#commit`	Commit the candidate configuration to the running configuration

`(config-if)#exit`	Exit interface mode.
`(config)#interface mlag2`	Enable the hardware-profile filter
`(config-if)#mode active-active`	Mode need to be configured as active-active
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#bridge 1 protocol rstp vlan-bridge`	Create RSTP bridge 1.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)#interface mlag1`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`(config-if)#switchport trunk allowed vlan all`	Enable all VLAN identifiers on this interface.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface mlag2`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`(config-if)#switchport trunk allowed vlan all`	Enable all VLAN identifiers on this interface.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface po1`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#mlag 1`	Enabling MLAG group number
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface po2`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#mlag 2`	enabling Mlag group number
`(config-if)#exit`	Exit interface mode.

© 2026 IP Infusion Inc. Proprietary

`(config)#interface xe9`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe57`	Enter interface mode.
`(config-if)#channel-group 2 mode active`	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe58`	Enter interface mode.
`(config-if)#channel-group 2 mode active`	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe49`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#exit`	Exit interface mode.
`(config)#mcec domain configuration`	Entering MCEC mode
`(config-mcec-domain)#domain-address 1111.2222.3333`	Domain address for the mlag domain
`(config-mcec-domain)#intra-domain link xe49`	Intra domain line between mlag domain
`(config-mcec-domain)#domain-system-number 1`	Number to identify the node in a domain
`(config-mcec-domain)#commit`	Commit the candidate configuration to the running configuration
`(config-mcec-domain)#exit`	Exit MCEC mode

© 2026 IP Infusion Inc. Proprietary

TOR-02

#configure terminal	Enter configure mode.
(config)#hardware-profile filter egress-l2 enable	Enable the hardware-profile filter
(config)#interface mlag1	Enter interface mode.
(config-if)#mode active-active	Mode need to be configured as active-active
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode
(config)#interface mlag2	Enable the hardware-profile filter
(config-if)#mode active-active	Mode need to be configured as active-active
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface mlag1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface mlag1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.

© 2026 IP Infusion Inc. Proprietary

`(config)#interface mlag2`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`(config-if)#switchport trunk allowed vlan all`	Enable all VLAN identifiers on this interface.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface po1`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#mlag 1`	Enabling Mlag group number
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface po2`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#mlag 2`	enabling MLAG group number
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe9`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe57`	Enter interface mode.
`(config-if)#channel-group 2 mode active`	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation

© 2026 IP Infusion Inc. Proprietary

	by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe58	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe49	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the Mlag domain
(config-mcec-domain)#intra-domain link xe49	Intra domain Link between Mlag domains
(config-mcec-domain)#domain-system-number 2	Number to identify the node in domain
(config-mcec-domain)#exit	Exit MCEC mode
(config-mcec-domain)#commit	Commit the candidate configuration to the running configuration

Validation

```
#sh mlag domain details

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number           : 1
Domain Address                 : 1111.2222.3333
Domain Priority                : 1000
Intra Domain Interface         : xe49

Hello RCV State                : Current
Hello Periodic Timer State     : Fast Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP

-------------------------------------
MLAG Configuration
-------------------------------------
```

```
MLAG-1
  Mapped Aggregator           : po1
  Admin Key                   : 16385
  Oper Key                    : 16385
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32769
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active


MLAG-2
  Mapped Aggregator           : po2
  Admin Key                   : 16386
  Oper Key                    : 16386
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32770
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active


#sh etherchannel summary
% Aggregator po1 0
% Aggregator Type: Layer2
% Admin Key: 16385 - Oper Key 16385
%   Link: xe57 (5057) sync: 1 (Mlag-active-link)
%   Link: xe58 (5058) sync: 1 (Mlag-active-link)
% Aggregator po2 0
% Aggregator Type: Layer2
% Admin Key: 16386 - Oper Key 16386
%   Link: xe9 (5009) sync : 1 (Mlag-active-link)
%   Link: xe10 (5010) sync: 1 (Mlag-active-link)

#sh mlag 1 detail

MLAG-1
  Mapped Aggregator           : po1
  Admin Key                   : 16385
  Oper Key                    : 16385
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32769
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Total Bandwidth             : 20g
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active


sh mcec statistics

Unknown MCCPDU received on the system            : 0

-------------------------------------
IDP xe49
-------------------------------------
   Valid RX Hello PDUs                        : 398
```

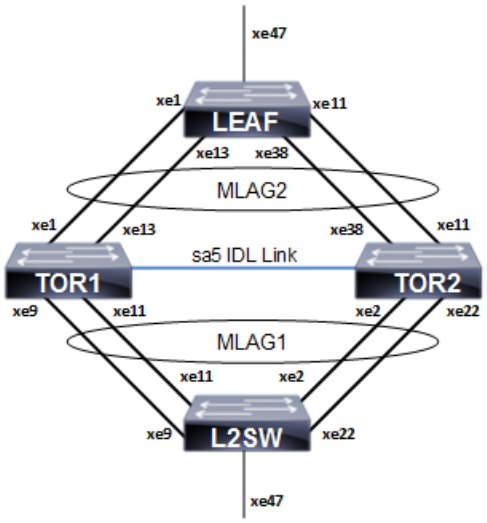
```
    Valid TX Hello PDUs                          : 417
    Valid RX Info PDUs                           : 16
    Valid TX Info PDUs                           : 6

    Valid RX Mac Sync PDUs                       : 3
    Valid TX Mac Sync PDUs                       : 4

MLAG 1
  Valid RX Info PDUs                             : 8
  Valid TX Info PDUs                             : 3

MLAG 2
  Valid RX Info PDUs                             : 8
  Valid TX Info PDUs                             : 3
sh mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 1000
Intra Domain Interface          : xe49
Domain Adjacency                : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator           : po1
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active


MLAG-2
  Mapped Aggregator           : po2
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active
```

Static Configuration

Static MLAG provides node-level redundancy by allowing two or more nodes in the network to share a common static- LAG endpoint. It emulates multiple nodes to represent as a single logical node to the remote node having static Link aggregation. As a result, even if one of the nodes is down there exists a path to reach the destination via other nodes.

Topology

Figure 18. Static MLAG topology



L2SW

`#configure terminal`	Enter configure mode.
`(config)#hostname L2SW`	Configuring host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan 2 bridge 1 state enable`	Configure VLAN for the bridge
`(config)#interface sa1`	Enter the interface mode
`(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface
`(config-if)#switchport mode hybrid`	Configure the mode as hybrid
`(config-if)#switchport hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe2`	Enter the interface mode
`(config-if)#static-channel-group 1`	Map static channel to the interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe9`	Enter the interface mode
`(config-if)#static-channel-group 1`	Map static channel to the interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe11`	Enter the interface mode
`(config-if)#static-channel-group 1`	Map static channel to the interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe22`	Enter the interface mode
`(config-if)#static-channel-group 1`	Map static channel to the interface

© 2026 IP Infusion Inc. Proprietary

(config-if)#exit	Exit the interface mode
(config)#interface xe47	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#exit	Exit the interface mode

TOR1

#configure terminal	Enter configure mode.
(config)#hostname TOR1	Configuring host name
(config)#bridge 1 protocol provider-rstp edge	Create a PROVIDER-RSTP EDGE bridge
(config)#vlan 2 bridge 1 state enable	Configure VLAN for the bridge
(config)#vlan 200 type service point-point bridge 1 state enable	Configure SVLAN for the bridge
(config)#cvlan registration table map1 bridge 1	Configure CVLAN-SVLAN mapping registration table for the bridge
(config-cvlan-registration)#cvlan 2 svlan 200	Map CVLAN to SVLAN
(config-cvlan-registration)#exit	Exit the config-cvlan-registration mode
(config)#interface mlag1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode customer-edge hybrid	Configure the mode as customer-edge hybrid
(config-if)#switchport customer-edge hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#switchport customer-edge vlan registration map1	Map the CVLAN registration table into the MLAG interface
(config-if)#mode active-standby	Configuring MLAG mode
(config-if)#exit	Exit the interface mode
(config)#interface mlag2	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-.if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode provider- network	Configure the mode as provider-network
(config-if)#switchport provider-network allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#mode active-standby	Configuring MLAG mode
(config-if)#exit	Exit the interface mode
(config)#interface sa1	Enter the interface mode

© 2026 IP Infusion Inc. Proprietary

(config-if)#switchport	Make the interface as switch port
(config-if)#mlag 1	Map MLAG on SA interface
(config-if)#exit	Exit the interface mode
(config)#interface sa2	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#mlag 2	Map MLAG on SA interface
(config-if)#exit	Exit the interface mode
(config)#interface xe1	Enter the interface mode
(config-if)#static-channel-group 2	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe13	Enter the interface mode
(config-if)#static-channel-group 2	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe9	Enter the interface mode
(config-if)#static-channel-group 1	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe11	Enter the interface mode
(config-if)#static-channel-group 1	Map static channel to the interface
(config-if)#exit	Exit the interface mode
(config)#interface sa5	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#exit	Exit the interface mode
(config)#interface xe3	Enter the interface mode
(config-if)#static-channel-group 5	Map static channel-group to the interface
(config)#interface xe5	Enter the interface mode
(config-if)#static-channel-group 5	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#mcec domain configuration	Enter the MLAG domain configuration mode
(config-mcec-domain)#domain-address 1111.2222.3333	Configure the MLAG domain address
(config-mcec-domain)#domain-system-number 1	Configure MLAG domain system number
(config-mcec-domain)#intra-domain-link sa5	Configure the intra domain link

TOR2

#configure terminal	Enter configure mode.
(config)#hostname TOR2	Configuring host name
(config)#bridge 1 protocol provider-rstp edge	Create a PROVIDER-RSTP EDGE bridge

`(config)#vlan 2 bridge 1 state enable`	Configure VLAN for the bridge
`(config)#vlan 200 type service point-point bridge 1 state enable`	Configure SVLAN for the bridge
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN-SVLAN mapping registration table for the bridge
`(config-cvlan-registration)#cvlan 2 svlan 200`	Map CVLAN to SVLAN
`(config-cvlan-registration)#exit`	Exit the config-CVLAN-registration mode
`(config)#interface mlag1`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode customer-edge hybrid`	Configure the mode as customer-edge hybrid
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#switchport customer-edge vlan registration map1`	Map the CVLAN registration table into the MLAG interface
`(config-if)#mode active-standby`	Configuring MLAG mode
`(config-if)#exit`	Exit the interface mode
`(config)#interface mlag2`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode provider- network`	Configure the mode as provider-network
`(config-if)#switchport provider-network allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#mode active-standby`	Configuring MLAG mode
`(config-if)#exit`	Exit the interface mode
`(config)#interface sa1`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port
`(config-if)#mlag 1`	Map MLAG on SA interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface sa2`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port
`(config-if)#mlag 2`	Map MLAG on SA interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe11`	Enter the interface mode
`(config-if)#static-channel-group 2`	Map static channel to the interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe38`	Enter the interface mode
`(config-if)#static-channel-group 2`	Map static channel to the interface

© 2026 IP Infusion Inc. Proprietary

(config-if)#exit	Exit the interface mode
(config)#interface xe2	Enter the interface mode
(config-if)#static-channel-group 1	Create static channel group
(config-if)#exit	Exit the interface mode
(config)#interface xe22	Enter the interface mode
(config-if)#static-channel-group 1	Create static channel group
(config-if)#exit	Exit the interface mode
(config)#interface sa5	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#exit	Exit the interface mode
(config)#interface xe3	Enter the interface mode
(config-if)#static-channel-group 5	Map static channel-group to the interface
(config)#interface xe5	Enter the interface mode
(config-if)#static-channel-group 5	Enter the interface mode
(config-if)#exit	Exit the interface mode
(config)#mcec domain configuration	Enter the MLAG domain configuration mode
(config-mcec-domain)#domain-address 1111.2222.3333	Configure the MLAG domain address
(config-mcec-domain)#domain-system-number 2	Configure MLAG domain system number
(config-mcec-domain)#intra-domain-link sa5	Configure the intra domain link
(config-if)#exit	Exit the interface mode

LEAF

#configure terminal	Enter configure mode.
(config)#hostname LEAF	Configuring host name
(config)#bridge 1 protocol provider-rstp edge	Create a PROVIDER-RSTP EDGE bridge
(config)#vlan 2 bridge 1 state enable	Configure VLAN for the bridge
(config)#vlan 200 type service point-point bridge 1 state enable	Configure SVLAN for the bridge
(config)#cvlan registration table map1 bridge 1	Configure CVLAN-SVLAN mapping registration table for the bridge
(config-cvlan-registration)#cvlan 2 svlan 200	Map CVLAN to SVLAN
(config-cvlan-registration)#exit	Exit the config-CVLAN-registration mode
(config)#interface sa2	Enter the interface mode
(config-if)#swtichport	Make the interface a switch port
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode provider-network	Configure the mode as provider-network
(config-if)#)#switchport provider-network allowed	Configure allowed VLAN all on the interface

© 2026 IP Infusion Inc. Proprietary

vlan all	
(config-if)#exit	Exit the interface mode
(config)#interface xe1	Enter the interface mode
(config-if)#static-channel-group 2	Map the interface to the static channel-group
(config-if)#exit	Exit the interface mode
(config)#interface xe13	Enter the interface mode
(config-if)#static-channel-group 2	Create static channel group
(config-if)#exit	Exit the interface mode
(config)#interface xe11	Enter the interface mode
(config-if)#static-channel-group 2	Map the interface to the static channel-group
(config-if)#exit	Exit the interface mode
(config)#interface xe38	Enter the interface mode
(config-if)#static-channel-group 2	Create static channel group
(config-if)#exit	Exit the interface mode
(config)#interface xe47	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode customer-edge hybrid	Configure the mode as customer-edge hybrid
(config-if)#switchport customer-edge hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#switchport customer-edge vlan registration map1	Map the CVLAN registration table into the MLAG interface
(config-if)#exit	Exit the interface mode

Validation

```
TOR1#show mlag 1 detail

MLAG-1
Mapped Aggregator   : sa1
Admin Key   : 16385
Oper Key   : 16385
Physical properties Digest   : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc

Neigh Admin Key   : 32769
Neigh Physical Digest   : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc Info RCV State   : Current
Info Periodic Time State   : Standby Total Bandwidth   : 40g
Mlag Sync   : IN_SYNC
Mode   : Active-Standby
Current Mlag State   : Active
```

Switchover-mode : Revertive TOR1#

```
TOR1#show mlag domain summary


Domain   Configuration
```

```
Domain
System Number   :
1
Domain   Address   :   1111.2222.3333
Domain   Priority   :   32768
Intra Domain Interface   : sa5
Domain Adjacency   : UP
```

MLAG Configuration

MLAG-1

```
Mapped Aggregator   : sa1
Physical properties Digest   : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc Total Bandwidth   : 40g
Mlag Sync   : IN_SYNC
Mode   : Active-Standby
Current Mlag State   : Active
Switchover-mode   : Revertive
```

MLAG-2

```
Mapped Aggregator   : sa2
Physical properties Digest   : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8

Total Bandwidth   : 40g
Mlag Sync   : IN_SYNC
Mode   : Active-Standby
Current Mlag State   : Active
Switchover-mode   : Revertive

TOR1#show mlag domain detail

Domain Configuration
Domain   System Number   :   1
Domain   Address   :   1111.2222.3333
Domain   Priority   :   32768
Intra   Domain Interface   :   sa5

Hello RCV State   : Current Hello Periodic Timer State   : Slow Periodic Domain Sync   : IN_SYNC
Neigh Domain Sync   : IN_SYNC
Domain Adjacency   : UP
```

MLAG Configuration

MLAG-1

```
Mapped Aggregator   : sa1
Admin Key   : 16385
Oper Key   : 16385
Physical properties Digest   : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc

Neigh Admin Key   : 32769
Neigh Physical Digest   : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc Info RCV State   : Current
Info Periodic Time State   : Standby Total Bandwidth   : 40g
Mlag Sync   : IN_SYNC
Mode   : Active-Standby
Current Mlag State   : Active Switchover-mode      : Revertive
```

MLAG-2

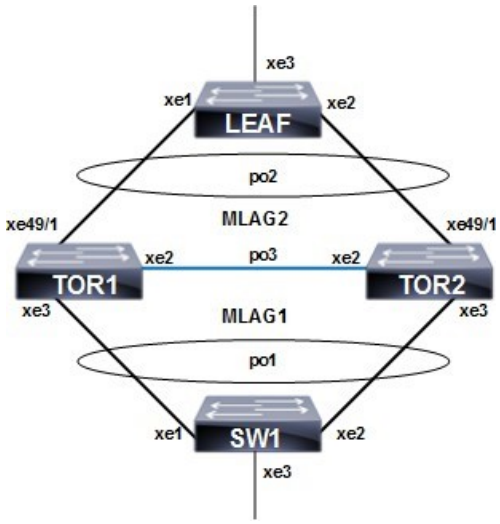
```
Mapped Aggregator   : sa2
```

```
Admin Key   : 16386
Oper Key   : 16386
Physical properties Digest   : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8


Neigh Admin Key   : 32770
Neigh Physical Digest   : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8

Info RCV State   : Current Info Periodic Time State : Standby Total Bandwidth   : 40g
Mlag Sync   : IN_SYNC
Mode   : Active-Standby
Current Mlag State   : Active Switchover-mode   : Revertive
```

ARP ACL Configuration

Topology

Figure 19. ARP ACL configuration with MC LAG



TOR1

`#configure terminal`	Enter configure mode.
`TOR1(config)#bridge 1 protocol provider-rstp edge`	Create provider RSTP bridge
`TOR1(config)#vlan 2-3990 type customer bridge 1 state enable`	Enable customer VLAN for bridge
`TOR1(config)#vlan 2-3990 type service point- point bridge 1 state enable`	Enable service VLAN for bridge
`TOR1(config)#cvlan registration table map1 bridge 1`	Create registration table
`TOR1(config-cvlan-registration)#cvlan 2-3990 svlan 3990`	Map CVLAN to svlan
`TOR1(config-cvlan-registration)#exit`	Exit the CVLAN registration table mode
`TOR1(config-if)#interface mlag1`	Enter MLAG interface

© 2026 IP Infusion Inc. Proprietary

`TOR1(config-if)#switchport`	Configure interface as switchport
`TOR1(config-if)#exit`	Exit the interface mode
`TOR1(config)#interface mlag2`	Enter MLAG interface
`TOR1(config-if)#switchport`	Configure interface as switchport
`TOR1(config-if)#bridge-group 1`	Associate the interface with bridge group 1
`TOR1(config-if)#switchport mode provider- network`	Set the switching characteristics of this interface to provider network
`TOR1(config-if)#switchport provider-network allowed vlan all`	Set the switching characteristics of this interface to provider network and allow all VLAN
`TOR1(config-if)#exit`	Exit the interface mode
`TOR1(config)#interface po1`	Enter dynamic LAG interface
`TOR1(config-if)#switchport`	Configure interface as switchport
`TOR1(config-if)#mlag 1`	Enable MLAG group number
`TOR1(config-if)#exit`	Exit the interface mode
`TOR1(config-if)#interface po2`	Enter dynamic LAG interface
`TOR1(config-if)#switchport`	Configure interface as switchport
`TOR1(config-if)#mlag 2`	Enable MLAG group number
`TOR1(config-if)#exit`	Exit the interface mode
`TOR1(config)#interface po3`	Enter dynamic LAG interface
`TOR1(config-if)#switchport`	Configure interface as switchport
`TOR1(config-if)#exit`	Exit the interface mode
`TOR1(config)#interface xe2`	Enter interface mode
`TOR1(config-if)#channel-group 3 mode active`	Make part of channel group 3
`TOR1(config-if)#exit`	Exit the interface mode
`TOR1(config)#interface xe3`	Enter interface mode
`TOR1(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
`TOR1(config-if)#exit`	Exit the interface mode
`TOR1(config-if)#interface xe49/1`	Enter interface mode
`TOR1(config-if)#channel-group 2 mode active`	Enable channel-group 2
`TOR1(config-if)#exit`	Exit the interface mode
`TOR1(config)#mcec domain configuration`	Enter MCEC mode
`TOR1(config-mcec-domain)#domain-address 2222.3333.4444`	Domain address for the MLAG domain
`TOR1(config-mcec-domain)#domain-system- number 1`	Number to identify the node in a domain
`TOR1(config-mcec-domain)#intra-domain-link po3`	Intra domain line between MLAG domain
`TOR1(config)#hardware-profile filter ingress-arp`	Enable globally hardware profile for ARP

© 2026 IP Infusion Inc. Proprietary

enable	
TOR1(config)#arp access-list cep	Create access list with name as CEP
TOR1(config-arp-acl)#30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner- vlan 2	Create permit rule for particular ARP request
TOR1(config-arp-acl)#40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan 3990 inner-vlan 2	Create permit rule for particular ARP response
TOR1(config)#arp access-list pnp	Create access list with name as PNP
TOR1(config-arp-acl)#20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner- vlan 2	Create permit rule for particular ARP request
TOR1(config-arp-acl)#30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan 3990 inner-vlan 2	Create permit rule for particular ARP response
TOR1(config-if)#interface mlag1	Enter mlag1 interface
TOR1(config-if)#arp access-group cep in	Attach rule with access-group CEP
TOR1(config-if)#interface mlag2	Enter mlag2 interface
TOR1(config-if)#arp access-group pnp in	Attach rule with access-group PNP

TOR2

#configure terminal	Enter configure mode.
TOR2(config)#bridge 1 protocol provider-rstp edge	Create provider RSTP bridge
TOR2(config)#vlan 2-3990 type customer bridge 1 state enable	Enable customer VLAN for bridge
TOR2(config)#vlan 2-3990 type service point- point bridge 1 state enable	Enable service VLAN for bridge
TOR2(config)#cvlan registration table map1 bridge 1	Create registration table
TOR2(config-cvlan-registration)#cvlan 2-3990 svlan 3990	Map CVLAN to svlan
TOR2(config-cvlan-registration)#exit	Exit the CVLAN registration table mode
TOR2(config)#interface mlag1	Enter MLAG interface
TOR2(config-if)#switchport	Configure interface as switchport
TOR2(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
TOR2(config-if)#switchport mode customer- edge hybrid	Set the switching characteristics of this interface to customer- edge hybrid
TOR2(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer- edge hybrid and allow VLAN all
TOR2(config-if)#switchport customer-edge vlan registration map1	Configure the registration table mapping on MLAG interface
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface mlag2	Enter MLAG interface
TOR2(config-if)#switchport	Configure interface as switchport

© 2026 IP Infusion Inc. Proprietary

`TOR2(config-if)#bridge-group 1`	Associate the interface with bridge group 1
`TOR2(config-if)#switchport mode provider- network`	Set the switching characteristics of this interface to provider network
`TOR2(config-if)#switchport provider-network allowed vlan all`	Set the switching characteristics of this interface to provider network and allow all VLAN
`TOR2(config-if)#exit`	Exit the interface mode
`TOR2(config)#interface po1`	Enter dynamic LAG interface
`TOR2(config-if)#switchport`	Configure interface as switchport
`TOR2(config-if)#mlag 1`	Enable MLAG group number
`TOR2(config-if)#exit`	Exit the interface mode
`TOR2(config)#interface po2`	Enter dynamic LAG interface
`TOR2(config-if)#switchport`	Configure interface as switchport
`TOR2(config-if)#mlag 2`	Enable MLAG group number
`TOR2(config-if)#exit`	Exit the interface mode
`TOR2(config)#interface po3`	Enter dynamic LAG interface
`TOR2(config-if)#switchport`	Configure interface as switchport
`TOR2(config-if)#exit`	Exit the interface mode
`TOR2(config)#interface xe2`	Enter interface mode
`TOR2(config-if)#channel-group 3 mode active`	Make part of channel group 3
`TOR2(config-if)#interface xe3`	Enter interface mode
`TOR2(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
`TOR2(config-if)#exit`	Exit the interface mode
`TOR2(config)#Interface xe49/1`	Enter interface mode
`TOR2(config-if)#channel-group 2 mode active`	Enable channel-group 2
`TOR2(config)#mcec domain configuration`	Configure MCEC domain information
`TOR2(config-mcec-domain)#domain-address 2222.3333.4444`	Domain address for the MLAG domain
`TOR2(config-mcec-domain)#domain-system- number 2`	Number to identify the node in a domain
`TOR2(config-mcec-domain)#intra-domain-link po3`	Intra domain line between MLAG domain
`TOR2(config)#hardware-profile filter ingress-arp enable`	Enable globally hardware profile for ARP
`TOR2(config)#arp access-list cep`	Create access list with name as CEP
`TOR2(config-arp-acl)#30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner- vlan 2`	Create permit rule for particular ARP request
`TOR2(config-arp-acl)#40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan 3990 inner-vlan 2`	Create permit rule for particular ARP response

© 2026 IP Infusion Inc. Proprietary

TOR2(config)#arp access-list pnp	Create access list with name as PNP
TOR2(config-arp-acl)#20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner- vlan 2	Create permit rule for particular ARP request
TOR2(config-arp-acl)#30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan 3990 inner-vlan 2	Create permit rule for particular ARP response
TOR2(config-if)#interface mlag1	Enter mlag1 interface
TOR2(config-if)#arp access-group cep in	Attach rule with access-group CEP
TOR2(config-if)#interface mlag2	Enter mlag2 interface
TOR2(config-if)#arp access-group pnp in	Attach rule with access-group PNP

SW1

#configure terminal	Enter configure mode.
SW1(config)#bridge 1 protocol rstp vlan- bridge	Configure the RSTP VLAN bridge
SW1(config)#vlan 2-3990 type customer bridge 1 state enable	Enable customer VLAN for bridge
SW1(config-if)#interface po1	Enter dynamic LAG interface
SW1(config-if)#switchport	Configure interface as switchport
SW1(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
SW1(config-if)#switchport mode hybrid	Set the switching characteristics of this interface hybrid
SW1(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all VLAN
SW1(config-if)#exit	Exit the interface mode
SW1(config)#interface xe1	Enter interface mode
SW1(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
SW1(config-if)#exit	Exit the interface mode
SW1(config)#interface xe2	Enter interface mode
SW1(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
SW1(config-if)#exit	Exit the interface mode
SW1(config)#interface xe3	Enter interface mode
SW1(config-if)#switchport	Configure interface as switchport
SW1(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
SW1(config-if)#switchport mode hybrid	Set the switching characteristics of this interface

© 2026 IP Infusion Inc. Proprietary

	hybrid
SW1(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all VLAN
SW1(config-if)#exit	Exit the interface mode

LEAF

#configure terminal	Enter configure mode.
Leaf(config)#bridge 1 protocol provider-rstp edge	Configure the RSTP VLAN bridge
Leaf(config)#vlan 2-3990 type customer bridge 1 state enable	Enable customer VLAN for bridge
Leaf(config)#vlan 2-3990 type service point- point bridge 1 state enable	Enable service VLAN for bridge
Leaf(config)#cvlan registration table map1 bridge 1	Create registration table
Leaf(config-cvlan-registration)#cvlan 2-3990 svlan 3990	Map CVLAN to SVLAN
Leaf(config-if)#exit	Exit the CVLAN registration table mode
Leaf(config)#interface po2	Enter interface mode
Leaf(config-if)#switchport	Configure interface as switchport
Leaf(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
Leaf(config-if)#switchport mode provider- network	Set the switching characteristics of this interface provider network
Leaf(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface provider and allowing all VLAN
Leaf(config-if)#exit	Exit the interface mode
Leaf(config)#interface xe1	Enter interface mode
Leaf(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
Leaf(config-if)#exit	Exit the interface mode
Leaf(config)#interface xe2	Enter interface mode
Leaf(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
Leaf(config-if)#exit	Exit the interface mode
Leaf(config)#Interface xe3	Enter interface mode
Leaf(config-if)#switchport	Configure interface as switchport
Leaf(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
Leaf(config-if)#switchport mode customer- edge hybrid	Set the switching characteristics of this interface to

© 2026 IP Infusion Inc. Proprietary

	customer- edge hybrid
`Leaf(config-if)#switchport customer-edge hybrid allowed vlan all`	Set the switching characteristics of this interface to customer- edge hybrid and allow vlan all
`Leaf(config-if)#switchport customer-edge vlan registration map1`	Configure the registration table mapping on mlag interface
`Leaf(config-if)#exit`	Exit the interface mode

Validation

```
TOR1#show access-lists
ARP access list cep
       30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner-vlan 2
       40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan 3990 inner-vlan
2
       default deny-all ARP access list pnp
       20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner-vlan 2 [match=1]
       30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan 3990 inner-vlan
2 [match=1]
       default deny-all log

TOR2#show access-lists
ARP access list cep
       30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner-vlan 2 [match=1]
       40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan 3990 inner-vlan
2 [match=1]
       default deny-all log ARP access list pnp
       20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner-vlan 2
       30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan 3990 inner-vlan
2
       default deny-all
```

© 2026 IP Infusion Inc. Proprietary

MSTP Configuration

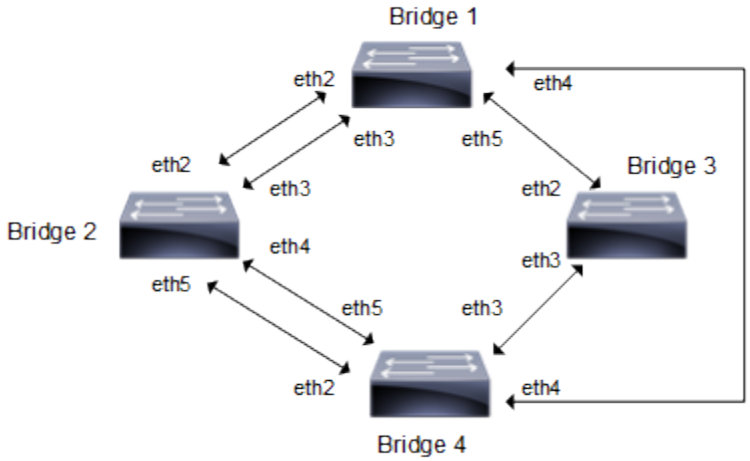
This section contains a complete sample Multiple Spanning Tree Protocol (MSTP) configuration. MSTP allows multiple VLANs to be grouped into one spanning-tree instance. Every MST instance has a spanning-tree that is independent of other spanning-tree instances providing multiple forwarding paths for data traffic.

Configuration

Topology

This example gives a simple multi-bridge topology and its configuration.

Figure 20. MSTP Topology



Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol mstp`	Add a bridge (1) to the multiple spanning tree table.
`Bridge1(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge1(config-vlan)#vlan 2 bridge 1 state enable`	Enable the state of VLAN 2 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 1.
`Bridge1(config-vlan)#vlan 3 bridge 1 state enable`	Enable the state of VLAN 3 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 1.
`Bridge1(config-vlan)#vlan 4 bridge 1 state enable`	Enable the state of VLAN 4 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 1.

© 2026 IP Infusion Inc. Proprietary

`Bridge1(config-vlan)#vlan 5 bridge 1 state enable`	Enable the state of VLAN 5 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 1.
`Bridge1(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge1(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree
`Bridge1(config-mst)#bridge 1 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 3 vlan 3`	Create another instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 4 vlan 4`	Create another instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 5 vlan 5`	Create another instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-mst)#exit`	Exit MST Configuration mode.
`Bridge1(config)#interface eth2`	Enter interface mode for eth2
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode for eth3.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance

© 2026 IP Infusion Inc. Proprietary

`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode for eth4.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter interface mode for eth5.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol mstp`	Add a bridge (2) to the multiple spanning
`Bridge2(config)#bridge 2 priority 4096`	Assign priority to this bridge.
`Bridge2(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge2(config-vlan)#vlan 2 bridge 2 state enable`	Enable the state of VLAN 2 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 2.
`Bridge2(config-vlan)#vlan 3 bridge 2 state enable`	Enable the state of VLAN 3 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 2
`Bridge2(config-vlan)#vlan 4 bridge 2 state enable`	Enable the state of VLAN 4 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 4

© 2026 IP Infusion Inc. Proprietary

	on bridge 2
`Bridge2(config-vlan)#vlan 5 bridge 2 state enable`	Enable the state of VLAN 5 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 2
`Bridge2(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge2(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree configuration mode
`Bridge2(config-mst)#bridge 2 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#bridge 2 instance 3 vlan 3`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#bridge 2 instance 4 vlan 4`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#bridge 2 instance 5 vlan 5`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-mst)#exit`	Exit MST Configuration mode.
`Bridge2(config)#interface eth2`	Enter interface mode for eth2
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode for eth3
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance

© 2026 IP Infusion Inc. Proprietary

`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3 priority 16`	Assign bridge-group 2 to this instance and set a port priority in order of 16 for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4 priority 16`	Assign bridge-group 2 to this instance and set a port priority in order of 16 for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode
`Bridge2(config)#interface eth4`	Enter interface mode for eth4
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode for eth5
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol mstp`	Add a bridge (3) to the multiple spanning tree table
`Bridge3(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge3(config-vlan)#vlan 2 bridge 3 state enable`	Enable the state of VLAN 2 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 3.
`Bridge3(config-vlan)#vlan 3 bridge 3 state enable`	Enable the state of VLAN 3 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 3.
`Bridge3(config-vlan)#vlan 4 bridge 3 state enable`	Enable the state of VLAN 4 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 3.
`Bridge3(config-vlan)#vlan 5 bridge 3 state enable`	Enable the state of VLAN 5 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 3.
`Bridge3(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge3(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.
`Bridge3(config-mst)#bridge 3 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#bridge 3 instance 3 vlan 3`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#bridge 3 instance 4 vlan 4`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#bridge 3 instance 5 vlan 5`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-mst)#exit`	Exit MST Configuration mode.
`Bridge3(config)#interface eth2`	Enter interface mode for eth2
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.

© 2026 IP Infusion Inc. Proprietary

`Bridge3(config-if)#bridge-group 3`	Associating the interface to bridge-group 3
`Bridge3(config-if)#bridge-group 3 instance 2`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 3`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 4`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 5`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode for eth3
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associating the interface to bridge-group 3
`Bridge3(config-if)#bridge-group 3 instance 2`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 3`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 4`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 5`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit interface mode.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol mstp`	Add a bridge (4) to the multiple spanning tree table
`Bridge4(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge4(config-vlan)#vlan 2 bridge 4 state enable`	Enable the state of VLAN 2 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 4.
`Bridge4(config-vlan)#vlan 3 bridge 4 state enable`	Enable the state of VLAN 3 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 4.
`Bridge4(config-vlan)#vlan 4 bridge 4 state enable`	Enable the state of VLAN 4 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 4.
`Bridge4(config-vlan)#vlan 5 bridge 4 state enable`	Enable the state of VLAN 5 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 4.
`Bridge4(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge4(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.

© 2026 IP Infusion Inc. Proprietary

`Bridge4(config-mst)#bridge 4 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#bridge 4 instance 3 vlan 3`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#bridge 4 instance 4 vlan 4`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#bridge 4 instance 5 vlan 5`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-mst)#exit`	Exit MST Configuration mode.
`Bridge4(config)#interface eth2`	Enter interface mode for eth2
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode for eth3
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode for eth4
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.

`Bridge4(config-if)#bridge-group 4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode for eth5
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.

Validation

show spanning-tree, show spanning-tree mst detail

```
# show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 4 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Max-hops 20
% 1: CIST Root Id 1000525400751db5
% 1: CIST Reg Root Id 1000525400751db5
% 1: CIST Bridge Id 80005254009cb7e6
% 1: 32 topology change(s)  - last topology change Mon Aug 17 10:45:25 2020

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Rootport - State Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
%   eth2: CIST Root 1000525400751db5
%   eth2: Regional Root 1000525400751db5
%   eth2: Designated Bridge 1000525400751db5
%   eth2: Message Age 0 - Max Age 20
%   eth2: CIST Hello Time 2 - Forward Delay 15
%   eth2: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
```

© 2026 IP Infusion Inc. Proprietary

```
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State Discarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400751db5
%   eth3: Regional Root 1000525400751db5
%   eth3: Designated Bridge 1000525400751db5
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 2
%   eth3: Restricted-role OFF
%   eth3: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Alternate - State Discarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400751db5
%   eth4: Regional Root 1000525400751db5
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer 0
%   eth4: forward-transitions 3
%   eth4: Restricted-role OFF
%   eth4: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State Forwarding
%   eth5: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth5: Designated Port Id 0x8007 - CIST Priority 128  -
%   eth5: CIST Root 1000525400751db5
%   eth5: Regional Root 1000525400751db5
%   eth5: Designated Bridge 80005254009cb7e6
%   eth5: Message Age 0 - Max Age 20
%   eth5: CIST Hello Time 2 - Forward Delay 15
%   eth5: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth5: forward-transitions 4
%   eth5: Restricted-role OFF
%   eth5: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800252540046f549
% 1: MSTI Bridge Id 80025254009cb7e6
```

```
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 800252540046f549
%   eth2: Designated Bridge 80025254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State Discarding
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 800252540046f549
%   eth3: Designated Bridge 80025254009cb7e6
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 800252540046f549
%   eth4: Designated Bridge 80025254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 800252540046f549
%   eth5: Designated Bridge 80025254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1


% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800352540046f549
% 1: MSTI Bridge Id 80035254009cb7e6
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 800352540046f549
%   eth2: Designated Bridge 80035254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State Discarding
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x1005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 800352540046f549
%   eth3: Designated Bridge 80035254009cb7e6
```

```
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 800352540046f549
%   eth4: Designated Bridge 80035254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 800352540046f549
%   eth5: Designated Bridge 80035254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1


% Instance  4:  Vlans: 4

% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800452540046f549
% 1: MSTI Bridge Id 80045254009cb7e6
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 800452540046f549
%   eth2: Designated Bridge 80045254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State Discarding
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x1005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 800452540046f549
%   eth3: Designated Bridge 80045254009cb7e6
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 800452540046f549
%   eth4: Designated Bridge 80045254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
```

```
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 800452540046f549
%   eth5: Designated Bridge 80045254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1


% Instance  5:  Vlans: 5

% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8005525400046f549
% 1: MSTI Bridge Id 80055254009cb7e6
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8005525400046f549
%   eth2: Designated Bridge 80055254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State Discarding
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 8005525400046f549
%   eth3: Designated Bridge 80055254009cb7e6
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 8005525400046f549
%   eth4: Designated Bridge 80055254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 8005525400046f549
%   eth5: Designated Bridge 80055254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

    #show spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 4 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Max-hops 20
% 1: CIST Root Id 1000525400751db5
% 1: CIST Reg Root Id 1000525400751db5
% 1: CIST Bridge Id 80005254009cb7e6
% 1: 32 topology change(s)  - last topology change Mon Aug 17 10:45:25 2020

% 1: portfast bpdu-filter disabled
```

```
% 1: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Rootport - State Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
%   eth2: CIST Root 1000525400751db5
%   eth2: Regional Root 1000525400751db5
%   eth2: Designated Bridge 1000525400751db5
%   eth2: Message Age 0 - Max Age 20
%   eth2: CIST Hello Time 2 - Forward Delay 15
%   eth2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State Discarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400751db5
%   eth3: Regional Root 1000525400751db5
%   eth3: Designated Bridge 1000525400751db5
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer 0
%   eth3: forward-transitions 2
%   eth3: Restricted-role OFF
%   eth3: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Alternate - State Discarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400751db5
%   eth4: Regional Root 1000525400751db5
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 3
%   eth4: Restricted-role OFF
%   eth4: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State Forwarding
%   eth5: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth5: Designated Port Id 0x8007 - CIST Priority 128  -
%   eth5: CIST Root 1000525400751db5
%   eth5: Regional Root 1000525400751db5
%   eth5: Designated Bridge 80005254009cb7e6
```

```
%   eth5: Message Age 0 - Max Age 20
%   eth5: CIST Hello Time 2 - Forward Delay 15
%   eth5: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth5: forward-transitions 4
%   eth5: Restricted-role OFF
%   eth5: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
```

Port Security Configuration

The Port Security feature allows network administrators to block unauthorized access to the network. Network administrators can configure each port of the switch to allow network access from only secured MACs, so that the switch forwards traffic from only secured MACs.

Users can limit each port's ingress traffic by limiting MAC addresses (source MACs) that are used to send traffic into ports. Port Security enables users to configure the maximum number of secured MACs for each port. Switches learn secured MAC dynamically (learned by switch during traffic inflow) or statically (User configured MACs). Dynamically Learned or statically programmed MAC addresses cannot exceed the maximum number of secured MACs configured for a particular port. Once the switch reaches the maximum limit for secured MACs, traffic from all other MAC addresses are dropped.

The violated MACs are logged in syslog messages. Refer to `cpu queue portsec-drop` using the command `show interface cpu counter queue-stats` for information on the number of violated MACs.

Secured MACs Learned Dynamically

Figure 21. Secured MACs learned dynamically

Send Layer 2 traffic with incremental source MAC of 100 and with VLAN 100 from IXIA1. Because the maximum limit is configured to 3, only 3 secure MAC addresses will be learned by SW1.

SW1

`#configure terminal`	Enter configure mode.
`(config)#hostname SW1`	Set the host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan database`	Enter vlan database mode.
`(config)#vlan 2-200 bridge 1 state enable`	Configure VLAN for the bridge
`(config-vlan)#eixt`	Exit from vlan database mode.
`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as trunk
`(config-if)#switchport hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#switchport port-security`	Enable port security mode dynamic
`(config-if)#switchport port-security maximum 3`	Limit secure MAC to 3 mac addresses.

© 2026 IP Infusion Inc. Proprietary

(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit interface mode
(config)#interface ge2	Enter interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode hybrid	Configure the mode as trunk
(config-if)#switchport hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit interface mode
(config)#logging monitor 7	Enable logging level as 7 for debugging
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit interface mode

Validation

Validation commands are `show port-security`, `show port-security interface <ifname>`, `show mac address-table count bridge 1`, `show bridge`, and `show mac address-table bridge 1`.

```
SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
-------+-------------------+---------+------+------+-----------------
ge1     dynamic             3

SW1#show port-security interface ge1
Port Security Mode     : Dynamic
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+----------------

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 3
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         100                 ge1         0000.0300.0500    1     100
 1         100                 ge1         0000.0300.055b    1     100
 1         100                 ge1         0000.0300.055c    1     100

SW1#show mac address-table bridge 1

CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
 100               0000.0300.0500   dynamic   ge1       Enable
 100               0000.0300.055b   dynamic   ge1       Enable
 100               0000.0300.055c   dynamic   ge1       Enable
```

Secured MAC Addresses Learned Statically

1. Stop the traffic from IXIA1 and do a `clear mac address-table dynamic bridge 1` on SW1.
2. Verify all dynamic secured MAC addresses are cleared.
3. Configure 3 static secure MAC addresses using the commands below in port security configured interface.
4. Try to add a fourth static secure MAC address.
5. Verify operator log message is displayed, saying "`port security mac limit reached`."

`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaaa vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaab vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaac vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode

Validation

```
SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
------+-------------------+---------+------+------+-----------------
ge1     dynamic             3          100          0000.0000.aaaa
                                       100          0000.0000.aaab
                                       100          0000.0000.aaac

SW1#show port-security interface ge1
Port Security Mode     : Dynamic
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+----------------
 100          0000.0000.aaaa
 100          0000.0000.aaab
 100          0000.0000.aaac

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 0
Static (User-defined) Unicast MAC Address Count: 3
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+----------+
 1         100                 ge1         0000.0000.aaaa    1     -
 1         100                 ge1         0000.0000.aaab    1     -
 1         100                 ge1         0000.0000.aaac    1     -

SW1#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
```

```
------+------+---------------+---------+---------+--------------
100           0000.0000.aaaa  static    ge1       Enable
100           0000.0000.aaab  static    ge1       Enable
100           0000.0000.aaac  static    ge1       Enable

SW1#
```

Remove the port-security configuration method using the two commands below:

`config)#interface ge1`	Enter interface mode
`(config-if)#no switchport port-security`	Set the port-security method to static.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode

Static Mode

Use the below command to configure the port-security method to static and configure static secure MAC addresses using the commands in static port-security method, below.

`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport port-security static`	Set the port-security method as static.
`(config-if)#switchport port-security max 3`	Limit static secure MAC to 3 mac addresses.
`(config-if)#switchport port-security mac-address 0000.0000.aaaa vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode.
`(config-if)#switchport port-security mac-address 0000.0000.aaab vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode.
`(config-if)#switchport port-security mac-address 0000.0000.aaac vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode .
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode

Verify the 3 secure static MAC addresses are added in interface ge1 using show running-config and also verify the port-security method should be static using below show commands.

Validation

```
SW1#show running-config interface ge1
interface ge1
 switchport
 bridge-group 1
 switchport mode hybrid
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan all
 switchport port-security static
 switchport port-security maximum 3
 switchport port-security mac-address 0000.0000.aaaa vlanId 100
```

© 2026 IP Infusion Inc. Proprietary

```
 switchport port-security mac-address 0000.0000.aaab vlanId 100
 switchport port-security mac-address 0000.0000.aaac vlanId 100

SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
-------+-------------------+---------+------+------+-----------------
ge1     static              3         100           0000.0000.aaaa
                                      100           0000.0000.aaab
                                      100           0000.0000.aaac

SW1#show port-security interface ge1
Port Security Mode     : Static
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+----------------
 100          0000.0000.aaaa
 100          0000.0000.aaab
 100          0000.0000.aaac

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 0
Static (User-defined) Unicast MAC Address Count: 3
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         100                 ge1         0000.0000.aaaa    1     -
 1         100                 ge1         0000.0000.aaab    1     -
 1         100                 ge1         0000.0000.aaac    1     -

SW1#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
100           0000.0000.aaaa  static    ge1       Enable
100           0000.0000.aaab  static    ge1       Enable
100           0000.0000.aaac  static    ge1       Enable
```

Configure one more static secure MAC address on interface ge1 and try to verify "`port security mac limit reached`" operator log message is displayed.

Start sending Layer-2 traffic with incremental source MAC of 100 and with VLAN 100 from IXIA1, and verify no dynamic secure MAC addresses are being learned using all the validation commands used.

© 2026 IP Infusion Inc. Proprietary

Disable Spanning Tree Configuration

This section describes disabling spanning tree operation on a per Multiple Spanning Tree Instance (MSTI) basis.

Disabling MSTP Configuration

Topology

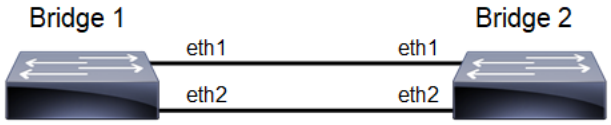


Figure 22. Disable Spanning Tree Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Disabling MSTP per instance

Bridge 1

`Bridge1(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 2
`Bridge1(config-mst)#no bridge 1 instance 3`	Disable spanning tree for MSTP on instance 3
`Bridge1(config-mst)#commit`	Commit the configure on the node.

Disabling MSTP globally

`Bridge1(config)#no bridge 1 multiple-spanning-tree enable bridge-forward`	Disable spanning tree globally for MSTP and keeping the ports in forwarding state.
`Bridge1(config)#commit`	Commit the configure on the node.

Disabling MSTP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for MSTP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge1(config-if)#commit`	Commit the configure on the node.

Disabling MSTP per instance

Bridge 2

`Bridge2(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 2

© 2026 IP Infusion Inc. Proprietary

`Bridge2(config-mst)#no bridge 1 instance 3`	Disable spanning tree for MSTP on instance 3
`Bridge2(config-mst)#commit`	Commit the configure on the node.

Disabling MSTP globally

`Bridge2(config)#no bridge 1 multiple-spanning-tree enable bridge-forward`	Disable spanning tree globally for MSTP.
`Bridge2(config)#commit`	Commit the configure on the node.

Disabling MSTP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for MSTP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge2(config-if)#commit`	Commit the configure on the node.

MSTP Validation

Bridge 1

Verify MSTP details with the show spanning-tree mst detail command.

```
#show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 905 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -   Max-hops 20
% 1: CIST Root Id 80003417ebfbe9c4
% 1: CIST Reg Root Id 80003417ebfbe9c4
% 1: CIST Bridge Id 800064006ac779a0
% 1: 9 topology change(s)  - last topology change Thu Nov 17 15:06:17 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State Forwarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge2: Designated Port Id 0x838a - CIST Priority 128  -
%   ge2: CIST Root 80003417ebfbe9c4
%   ge2: Regional Root 80003417ebfbe9c4
%   ge2: Designated Bridge 80003417ebfbe9c4
%   ge2: Message Age 0 - Max Age 20
%   ge2: CIST Hello Time 2 - Forward Delay 15
%   ge2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0
%   ge2: forward-transitions 1
%   ge2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Alternate - State Discarding
%   ge3: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge3: Designated Port Id 0x838b - CIST Priority 128  -
%   ge3: CIST Root 80003417ebfbe9c4
```

```
%   ge3: Regional Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: CIST Hello Time 2 - Forward Delay 15
%   ge3: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change timer 0
%   ge3: forward-transitions 2
%   ge3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 20000 -MSTI Root Port 5001 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80023417ebfbe9c4
% 1: MSTI Bridge Id 800264006ac779a0
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State Forwarding
%   ge2: Designated Internal Path Cost 0  - Designated Port Id 0x838a
%   ge2: Configured Internal Path Cost 20000
%   ge2: Configured CST External Path cost 20000
%   ge2: CST Priority 128  - MSTI Priority 128
%   ge2: Designated Root 80023417ebfbe9c4
%   ge2: Designated Bridge 800264006ac779a0
%   ge2: Message Age 0
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0

% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800364006ac779a0
% 1: MSTI Bridge Id 800364006ac779a0
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State Forwarding
%   ge3: Designated Internal Path Cost 0  - Designated Port Id 0x838c
%   ge3: Configured Internal Path Cost 20000
%   ge3: Configured CST External Path cost 20000
%   ge3: CST Priority 128  - MSTI Priority 128
%   ge3: Designated Root 800364006ac779a0
%   ge3: Designated Bridge 800364006ac779a0
%   ge3: Message Age 0
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
```

Verify MSTP configurations when MSTP is enabled globally.

```
#show running-config
!
bridge 1 protocol mstp
!
```

Verify MSTP configurations when MSTP is disabled globally.

```
#show running-config
!
bridge 1 protocol mstp
no bridge 1 multiple-spanning-tree enable bridge-forward
!
```

Verify MSTP configurations when MSTP instance 2 and 3 is enabled.

```
#show running-config spanning-tree
!
spanning-tree mst configuration
```

```
bridge 1  instance 2
bridge 1  instance 2 vlan 2
bridge 1  instance 3
bridge 1  instance 3 vlan 3
!
interface xe2
bridge-group 1 instance 2
!
interface xe3
bridge-group 1 instance 3
!
```

Verify MSTP configurations when MSTP instance 2 is disabled

```
#show running-config spanning-tree
!
spanning-tree mst configuration
bridge 1 instance 3
bridge 1 instance 3 vlan 3
!
interface ge3
bridge-group 1 instance 3
!
```

Verify MSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode access
switchport access vlan 2
bridge-group 1 instance 2
!
```

Verify MSTP configurations when spanning-tree is disabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode access
switchport access vlan 2
bridge-group 1 instance 2
```

Verify MSTP details after disabling spanning-tree on interface ge2 with the `show spanning-tree mst details` command.

```
#show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 908 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Max-hops 20
% 1: CIST Root Id 80003417ebfbe9c4
% 1: CIST Reg Root Id 80003417ebfbe9c4
% 1: CIST Bridge Id 800064006ac779a0
% 1: 10 topology change(s)  - last topology change Fri Nov 25 21:21:05 2016

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled - State Forwarding
```

```
%   ge2: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge2: Designated Port Id 0x838a - CIST Priority 128  -
%   ge2: Message Age 0 - Max Age 20
%   ge2: CIST Hello Time 2 - Forward Delay 15
%   ge2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0
%   ge2: forward-transitions 2
%   ge2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport - State Forwarding
%   ge3: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge3: Designated Port Id 0x838b - CIST Priority 128  -
%   ge3: CIST Root 80003417ebfbe9c4
%   ge3: Regional Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: CIST Hello Time 2 - Forward Delay 15
%   ge3: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer 0
%   ge3: forward-transitions 3
%   ge3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800264006ac779a0
% 1: MSTI Bridge Id 800264006ac779a0
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled - State Discarding
%   ge2: Designated Internal Path Cost 0  - Designated Port Id 0x8389
%   ge2: Configured Internal Path Cost 20000
%   ge2: Configured CST External Path cost 20000
%   ge2: CST Priority 128  - MSTI Priority 128
%   ge2: Designated Root 800264006ac779a0
%   ge2: Designated Bridge 800264006ac779a0
%   ge2: Message Age 0
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 20000 -MSTI Root Port 5004 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80033417ebfbe9c4
% 1: MSTI Bridge Id 800364006ac779a0
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport - State Forwarding
%   ge3: Designated Internal Path Cost 0  - Designated Port Id 0x838b
%   ge3: Configured Internal Path Cost 20000
%   ge3: Configured CST External Path cost 20000
%   ge3: CST Priority 128  - MSTI Priority 128
%   ge3: Designated Root 80033417ebfbe9c4
%   ge3: Designated Bridge 800364006ac779a0
%   ge3: Message Age 0
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1
```

STP Configuration

Disabling STP globally

Bridge 1

`Bridge1(config)#no bridge 1 spanning-tree enable bridge-forward`	Disable spanning tree globally for STP.
`Bridge1(config)#commit`	Commit the configure on the node.

Disabling STP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for STP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge1(config-if)#commit`	Commit the configure on the node.

Disabling STP globally

Bridge 2

`Bridge2(config)#no bridge 1 spanning-tree enable bridge-forward`	Disable spanning tree globally for STP.
`Bridge2(config)#commit`	Commit the configure on the node.

Disabling STP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for STP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge2(config-if)#commit`	Commit the configure on the node.

STP Validation

Bridge 1

Verify STP details when stp is enabled globally and ge2 and ge3 are part of the bridge using the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled - topology change
% 1: Root Path Cost 4 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 905
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: 3 topology changes - last topology change Tue Nov 15 21:33:53 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
```

```
%ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 -      designated cost 0
%ge2: Designated Port Id 0x838a - state Forwarding -Priority 128
%ge2: Designated root 80003417ebfbe9c4
%ge2: Designated Bridge 80003417ebfbe9c4
%ge2: Message Age 0 - Max Age 20
%ge2: Hello Time 2 - Forward Delay 15
%ge2: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 1 - topo change  timer0
%ge2: forward-transitions 1
%ge2: No portfast configured – Current  portfast
%ge2: bpdu-guard default- Current bpdu-guard off
%ge2: bpdu-filter default- Current bpdu-filter off
%ge2: no root guard configured- Current root guard off
%ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - path cost 4 - designated cost 0
%ge3: Designated Port Id 0x838b - state Blocked -Priority 128
%ge3: Designated root 80003417ebfbe9c4
%ge3: Designated Bridge 80003417ebfbe9c4
%ge3: Message Age 0 - Max Age 20
%ge3: Hello Time 2 - Forward Delay 15
%ge3: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 1 - topo change timer0
%ge3: forward-transitions 0
%ge3: No portfast configured - Currentportfast off
%ge3: bpdu-guarddefault- Current bpdu-guard off
%ge3: bpdu-filter default- Current bpdu-filter off
%ge3: no root guard configured- Current root guard off
%
```

Verify STP configurations when STP is enabled globally.

```
#show running-config
!
bridge 1 protocol ieee vlan-bridge
!
```

Verify STP configurations when STP is disabled globally.

```
#show running-config
!
bridge 1 protocol ieee vlan-bridge
no bridge 1 spanning-tree enable bridge-forward
!
```

Verify STP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
!
```

Verify STP configurations when spanning-tree is disabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode trunk
switchport trunk allowed vlan all
!
```

© 2026 IP Infusion Inc. Proprietary

Verify STP details after disabling spanning-tree on interface ge2 with the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 4 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 908
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: 5 topology changes - last topology change Fri Nov 25 21:15:35 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 - designated cost 0
%   ge2: Designated Port Id 0x838a - state Disabled -Priority 128
%   ge2: Message Age 0 - Max Age 20
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change timer 23
%   ge2: forward-transitions 2
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - path cost 4 - designated cost 0
%   ge3: Designated Port Id 0x838b - state Forwarding -Priority 128
%   ge3: Designated root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 1 - topo change timer 23
%   ge3: forward-transitions 2
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
```

RSTP Configuration

Disabling RSTP globally

Bridge 1

`Bridge1(config)#no bridge 1 rapid-spanning-tree enable bridge-forward`	Disable spanning tree globally for RSTP.
`Bridge1(config)#commit`	Commit the configure on the node.

Disabling RSTP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for RSTP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge1(config-if)#commit`	Commit the configure on the node.

Disabling RSTP globally

Bridge 2

`Bridge2(config)#no bridge 1 rapid-spanning-tree enable bridge-forward`	Disable spanning tree globally for RSTP.
`Bridge2(config)#commit`	Commit the configure on the node.

Disabling RSTP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for RSTP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge2(config-if)#commit`	Commit the configure on the node.

RSTP Validation

Bridge 1

Verify RSTP details when rstp is enabled globally and ge2 and ge3 are part of the bridge using the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled   - topology change detected
% 1: Root Path Cost 20000 - Root Port 905 -   Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: last topology change Tue Nov 15 21:44:31 2016
% 1: 7 topology change(s)   - last topology change Tue Nov 15 21:44:31 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State Forwarding
% ge2: Designated Path Cost 0
% ge2: Configured Path Cost 20000   - Add type Explicit ref count 1
% ge2: Designated Port Id 0x838a - Priority 128   -
% ge2: Root 80003417ebfbe9c4
% ge2: Designated Bridge 80003417ebfbe9c4
% ge2: Message Age 0 - Max Age 20
% ge2: Hello Time 2 - Forward Delay 15
% ge2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer
0
% ge2: forward-transitions 1
% ge2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge2: No portfast configured - Current   portfast off
% ge2: bpdu-guard   default   - Current bpdu-guard off
% ge2: bpdu-filter default   - Current bpdu-filter off
% ge2: no root guard configured   - Current root guard off
% ge2: Configured Link Type point-to-point - Current point-to-point
% ge2: No auto-edge configured - Current port Auto Edge off
% ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Alternate - State Discarding
% ge3: Designated Path Cost 0
% ge3: Configured Path Cost 20000   - Add type Explicit ref count 1
% ge3: Designated Port Id 0x838b - Priority 128   -
% ge3: Root 80003417ebfbe9c4
% ge3: Designated Bridge 80003417ebfbe9c4
% ge3: Message Age 0 - Max Age 20
```

© 2026 IP Infusion Inc. Proprietary

```
% ge3: Hello Time 2 - Forward Delay 15
% ge3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer
0
% ge3: forward-transitions 2
% ge3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge3: No portfast configured - Current   portfast off
% ge3: bpdu-guard   default   - Current bpdu-guard off
% ge3: bpdu-filter default   - Current bpdu-filter off
% ge3: no root guard configured   - Current root guard off
% ge3: Configured Link Type point-to-point - Current point-to-point
% ge3: No auto-edge configured - Current port Auto Edge off
%
```

Verify RSTP configurations when RSTP is enabled globally.

```
#show running-config
!
bridge 1 protocol rstp vlan-bridge
!
```

Verify RSTP configurations when RSTP is disabled globally

```
#show running-config
!
bridge 1 protocol rstp vlan-bridge
no bridge 1 rapid-spanning-tree enable bridge-forward
!
```

Verify RSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
!
```

Verify RSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode trunk
switchport trunk allowed vlan all
```

Verify RSTP details after disabling spanning-tree on interface ge2 with the `show spanning-tree` command.

```
#sh spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 20000 - Root Port 908 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: last topology change Fri Nov 25 21:08:56 2016
% 1: 11 topology change(s)  - last topology change Fri Nov 25 21:08:56 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled - State Forwarding
```

© 2026 IP Infusion Inc. Proprietary

```
%   ge2: Designated Path Cost 0
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge2: Designated Port Id 0x838a - Priority 128  -
%   ge2: Message Age 0 - Max Age 20
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer 0
%   ge2: forward-transitions 2
%   ge2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport - State Forwarding
%   ge3: Designated Path Cost 0
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge3: Designated Port Id 0x838b - Priority 128  -
%   ge3: Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change timer 0
%   ge3: forward-transitions 3
%   ge3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off
```

Link Layer Discovery Protocol Configuration

This section contains a complete sample Link Layer Discovery Protocol (LLDP) configuration.

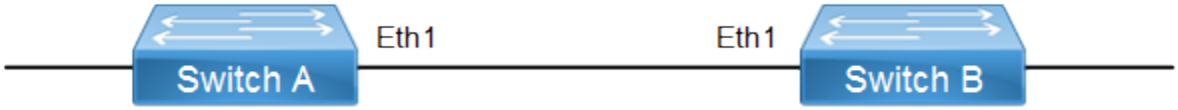
LLDP is a neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise themselves to other devices on the same physical LAN, and then to store information about the network. It allows a device to learn higher-layer management reachability and connection endpoint information from adjacent devices. Using LLDP, a network device is able to advertise its identity, its capabilities and its media-specific configuration, as well as learn the same information from other connected devices.

Note: The `lldp-agent` command is not supported for SVLAN, VLAN, and loop-back interfaces.

Topology

The following figure displays a sample LLDP topology.

Figure 23. LLDP Topology



LLDPv2 (Interface Mode TLV)

Default Agent

All configuration commands in the table below should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the port-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the system-name TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the system-capabilities TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the system-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the management-address TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the VLAN-id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the VLAN-NAME TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the Protocol Identity TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the Management VID TLV to be transmitted on the port

© 2026 IP Infusion Inc. Proprietary

`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the Link Aggregation TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLDPDUs that are transmitted during a fast transmission period
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch

```
#show running-config lldp
!
interface eth1
lldp-agent
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
  lldp tlv ieee-8021-org-specific mgmt-vid select
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6
!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 nearest-bridge

Agent Mode                   : Nearest bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 5
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Not Defined
 Traffic statistics          :
  Total frames transmitted   : 4
  Total entries aged         : 0
  Total frames received      : 3
```

```
   Total error frames received: 0
   Total frames discarded     : 0
   Total discarded TLVs       : 0
   Total unrecognised TLVs    : 0
```

Customer Bridge

All configuration commands in the table below should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent customer-bridge`	Enter into the Customer Bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the port-description TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the system-name TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the system-capabilities TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the system-description TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the management-address TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the VLAN-id TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the VLAN-NAME TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the Protocol Identity TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the Management VID TLV to be transmitted

© 2026 IP Infusion Inc. Proprietary

	on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the Link Aggregation TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port.
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods.
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLD PDUs that are transmitted during a fast transmission period.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch:

```
#show #show running-config lldp
!
interface eth1
lldp-agent customer-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
  lldp tlv ieee-8021-org-specific mgmt-vid select
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6
!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 customer-bridge

Agent Mode                   : Customer-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 5
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Not Defined
 Traffic statistics          :
  Total frames transmitted   : 8
```

```
   Total entries aged         : 0
   Total frames received      : 7
   Total error frames received: 0
   Total frames discarded     : 0
   Total discarded TLVs       : 0
   Total unrecognised TLVs    : 0
```

Non-Tpmr-Bridge

The below configurations should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the Non tpmr Bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the port-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the system-name TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the system-capabilities TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the system-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the management-address TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the VLAN-id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the VLAN-NAME TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the Protocol Identity TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the VID Usage Digest TLV to be transmitted on the port

© 2026 IP Infusion Inc. Proprietary

`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the Management VID TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the Link Aggregation TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLD PDUs that are transmitted during a fast transmission period
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch:

```
#show running-config lldp
lldp-agent non-tpmr-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
  lldp tlv ieee-8021-org-specific mgmt-vid select
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6

!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 non-tmpr-bridge

Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 5
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : Not Defined
 Traffic statistics          :
  Total frames transmitted   : 17
```

```
    Total entries aged         : 0
    Total frames received      : 6
    Total error frames received: 0
    Total frames discarded     : 0
    Total discarded TLVs       : 0
    Total unrecognised TLVs    : 0
```

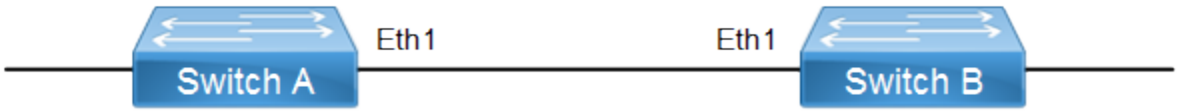
© 2026 IP Infusion Inc. Proprietary

Global Mode TLV

LLDPv2 TLVs can be configured globally, making it applicable for all interfaces where LLDP is enabled.

Topology

Figure 24. LLDP topology



SW1

`SW1#configure terminal`	Enter Configure mode
`SW1(config)#lldp tlv-select basic-mgmt port-description`	Enable LLDP port description TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-name`	Enable LLDP system name TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-capabilities`	Enable LLDP system capabilities TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-description`	Enable LLDP system description TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt management-address`	Enable LLDP port description TLV in global mode
`SW1(config)#interface eth1`	Enter interface mode
`SW1(config-if)#lldp-agent`	Enter LLDP interface mode
`SW1(if-lldp-agent)#set lldp enable txrx`	Enable LLDP TLV transmit and receive for the nearest bridge
`SW1(if-lldp-agent)#exit`	Exit LLDP mode
`SW1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#end`	Exit the configure mode

SW2

`SW2#configure terminal`	Enter Configure mode
`SW2(config)#lldp tlv-select basic-mgmt port-description`	Enable LLDP port description TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-name`	Enable LLDP system name TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-capabilities`	Enable LLDP system capabilities TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-description`	Enable LLDP system description TLV in global mode

© 2026 IP Infusion Inc. Proprietary

`SW2(config)#lldp tlv-select basic-mgmt management-address`	Enable LLDP management address TLV in global mode
`SW2(config)#interface eth1`	Enter interface mode
`SW2(config-if)#lldp-agent`	Enter LLDP interface mode
`SW2(if-lldp-agent)#set lldp enable txrx`	Enable LLDP TLV transmit and receive for the nearest bridge
`SW2(if-lldp-agent)#exit`	Exit LLDP mode
`SW2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#end`	Exit the configure mode

Validation

```
SW1#show running-config lldp
!
lldp tlv-select basic-mgmt port-description
lldp tlv-select basic-mgmt system-name
lldp tlv-select basic-mgmt system-capabilities
lldp tlv-select basic-mgmt system-description
lldp tlv-select basic-mgmt management-address
!
interface eth1
 lldp-agent
  set lldp enable txrx


SW1#show lldp neighbors

Loc PortID      Rem Host Name      Rem Chassis Id     Rem Port Id       Agent Mode

--------------------------------------------------------------------------------
Eth1           OcNOS              cc37.ab56.6d80     cc37.abbb.ed81   Nearest bridge


SW1#show lldp neighbors detail

--------------------------------------------------------------------------------

Nearest bridge Neighbors
Interface Name              : eth1
 Mandatory TLVs
 Chassis id type          : MAC address [cc37.ab56.6d80]
 Port id type             : MAC address [cc37.abbb.ed81]
 Time to live             : 121
 Basic Management TLVs
 System Name              : SW2
 System Description       : Hardware Model:EC_AS4610-54, Software version: Oc
NOS,1.3.6.241a
 Port Description          : eth1
 Remote System Capabilities : Bridge
                              Router
 Capabilities Enabled     : Router
 Management Address        : MAC Address [cc37.abbb.ed81]
 Interface Number subtype  : ifindex
 Interface Number          10046
 OID Number              : 0
 802.1 Org specific TLVs
 Port vlan id             : 0
```

```
  Port & Protocol vlan id   : 0
  Remote Configured VLANs   : None
  Remote Protocols Advertised: None
  Remote VID Usage Digest   : 0
  Remote Management Vlan    : 0
  Link Aggregation Capability: not capable of being aggregated
  Link Aggregation Status   : not currently in aggregation
  Link Aggregation Port ID  :
  802.3 Org specific TLVs
  AutoNego Support          : Not-Supported
  AutoNego Status           : Disabled
  AutoNego Capability       : 0
  Operational MAU Type      : 0 [unknown]
   Max Frame Size            :
SW1#
```

LLDP-MED

LLDP extensions and behavior requirements are described specifically in the areas of network Configuration and policy, device location (including for Emergency Call Service / E911), Power over Ethernet management, and inventory management.

Based on the device type, different TLVs are advertised by the Station.

LLDP-MED Network Connectivity Device

LLDP-MED Network Connectivity Devices, as defined in this Standard, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

- LAN Switch/Router
- IEEE 802.1 Bridge
- IEEE 802.3 Repeater (included for historical reasons)
- IEEE 802.11 Wireless Access Point
- Any device that supports the IEEE 802.1AB and MED extensions defined by this Standard and can relay IEEE 802 frames via any method.

Configuration Command

```
set lldp med-devtype net-connect
```

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services.

Configuration command:

```
set lldp med-devtype ep-class1
```

LLDP-MED Generic Endpoint (Class 2)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar

Configuration command:

```
set lldp med-devtype ep-class2
```

© 2026 IP Infusion Inc. Proprietary

LLDP-MED Generic Endpoint (Class 3)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Configuration command:

```
set lldp med-devtype ep-class3
```

Switch A

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(if-config-if)#lldp-agent customer-bridge`	Enter into the customer-bridge agent.
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the non-tpmr-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#set lldp med-devtype net-connect`	Configure the med device type
`(config-if)#exit`	Exit interface mode.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.

Switch B

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.

© 2026 IP Infusion Inc. Proprietary

`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent customer-bridge`	Enter into the customer-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the non-tpmr-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#set lldp med-devtype ep-class3`	Configure the med device type
`(config-if)#exit`	Exit interface mode.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.

Validation

1. Verify the LLDP configurations on Switch A:

```
#show running-config lldp
!
!
interface eth1
 lldp-agent
  set lldp enable txrx
 set lldp med-devtype net-connect
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
 lldp-agent customer-bridge
  set lldp enable txrx
!
```

2. Verify the LLDP port statistics on Switch A:

```
#show lldp interface eth1
Agent Mode                   : Customer-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 11
  Total entries aged         : 0
  Total frames received      : 10
  Total error frames received: 0
  Total frames discarded     : 0
```

© 2026 IP Infusion Inc. Proprietary

```
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 7
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Nearest bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 7
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0

#show lldp interface eth1 non-tpmr-bridge
Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 5
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Not Defined
 Traffic statistics          :
  Total frames transmitted   : 4
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
```

3. Verify the LLDP configurations for end device ep-class3 on Switch B:

```
#show running-config lldp
!
interface eth1
 set lldp med-devtype ep-class3
 lldp-agent
  set lldp enable txrx
  lldp tlv med network-policy select
lldp-agent non-TPMR-bridge
  set lldp enable txrx
  lldp tlv med network-policy select
lldp-agent customer-bridge
  set lldp enable txrx
  lldp tlv med network-policy select
!
```

4. Verify the LLDP port statistics on Switch B:

```
#show lldp interface eth1
Agent Mode                    : Customer-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : End Point Class-3
 Traffic statistics           :
  Total frames transmitted    : 124
  Total entries aged          : 0
  Total frames received       : 125
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
Agent Mode                    : Non-TPMR-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : End Point Class-3
 Traffic statistics           :
  Total frames transmitted    : 120
  Total entries aged          : 0
  Total frames received       : 0
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
Agent Mode                    : Nearest bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : End Point Class-3
 Traffic statistics           :
  Total frames transmitted    : 120
  Total entries aged          : 0
  Total frames received       : 0
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
#
```

Provider Bridging Configuration

Overview

This section contains sample provider bridging configurations.

A provider bridged network is a virtual bridged Local Area Network that comprises provider bridges (SVLAN bridges and provider edge bridges) and attached LANs, under the administrative control of a single service provider. Provider bridges interconnect the separate MACs of the IEEE 802 LANs that compose a provider bridged network, relaying frames to provide connectivity between all the LANs that provide customer interfaces for each service instance.

Single Provider Bridge Configuration

Topology

Following figure shows the single provider bridge configuration.

Figure 25. Single Provider Bridge Configuration

Configuration

SW1 (PEB)

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2 type customer bridge 1 state enable`	Create customer vlan VLAN 2
`SW1(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#cvlan registration table map1 bridge 1`	Create cvlan registration table map1
`SW1(config-cvlan-registration)#cvlan 2 svlan 200`	Map cvlan2 with svlan 200
`SW1(config-cvlan-registration)#exit`	Exit registration table
`SW1(config)#interface eth1`	Enter interface configuration mode for eth1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode customer-edge hybrid`	Configure switchport mode customer edge

© 2026 IP Infusion Inc. Proprietary

`SW1(config-if)#switchport customer-edge access vlan 2`	Associate customer vlan2 with interface
`SW1(config-if)#switchport customer-edge vlan registration map1`	Attach registration table map1 with interface
`SW1(config-if)#exit`	Exit interface mode
`SW1(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#commit`	Commit the configuration.
`SW1(config-if)#exit`	Exit interface configuration mode

SW2 (PB)

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface eth1`	Enter interface configuration mode for eth1
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#exit`	Exit interface configuration mode
`SW2(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#commit`	Commit the configuration.
`SW2(config-if)#exit`	Exit interface configuration mode

SW3 (PEB)

`SW3#configure terminal`	Enter configuration mode

SW3(config)#bridge 1 protocol provider-rstp edge	Create bridge
SW3(config)#vlan database	Enter VLAN configuration mode
SW3(config-vlan)#vlan 2 type customer bridge 1 state enable	Create customer vlan VLAN 2
SW3(config-vlan)#vlan 200 type service point-point bridge 1 state enable	Create service vlan VLAN200
SW3(config-vlan)#exit	Exit VLAN configuration mode
SW3(config)#cvlan registration table map1 bridge 1	Create cvlan registration table map1
SW3(config-cvlan-registration)#cvlan 2 svlan 200	Map cvlan2 with svlan 200
SW3(config-cvlan-registration)#exit	Exit registration table
SW3(config)#interface eth1	Enter interface configuration mode for eth1
SW3(config-if)#switchport	Configure switchport
SW3(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW3(config-if)#witchport mode customer-edge hybrid	Configure switchport mode customer edge
SW3(config-if)#switchport customer-edge access vlan 2	Associate customer vlan2 with interface
SW3(config-if)#switchport customer-edge vlan registration map1	Attach registration table map1 with interface
SW3(config-if)#exit	Exit interface mode
SW3(config-if)#interface eth2	Enter interface configuration mode for eth2
SW3(config-if)#switchport	Make interface as switchport
SW3(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW3(config-if)#switchport mode provider-network	Configure switchport pnp port
SW3(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW3(config-if)#commit	Commit the configuration.
SW3(config-if)#exit	Exit interface configuration mode

Validation

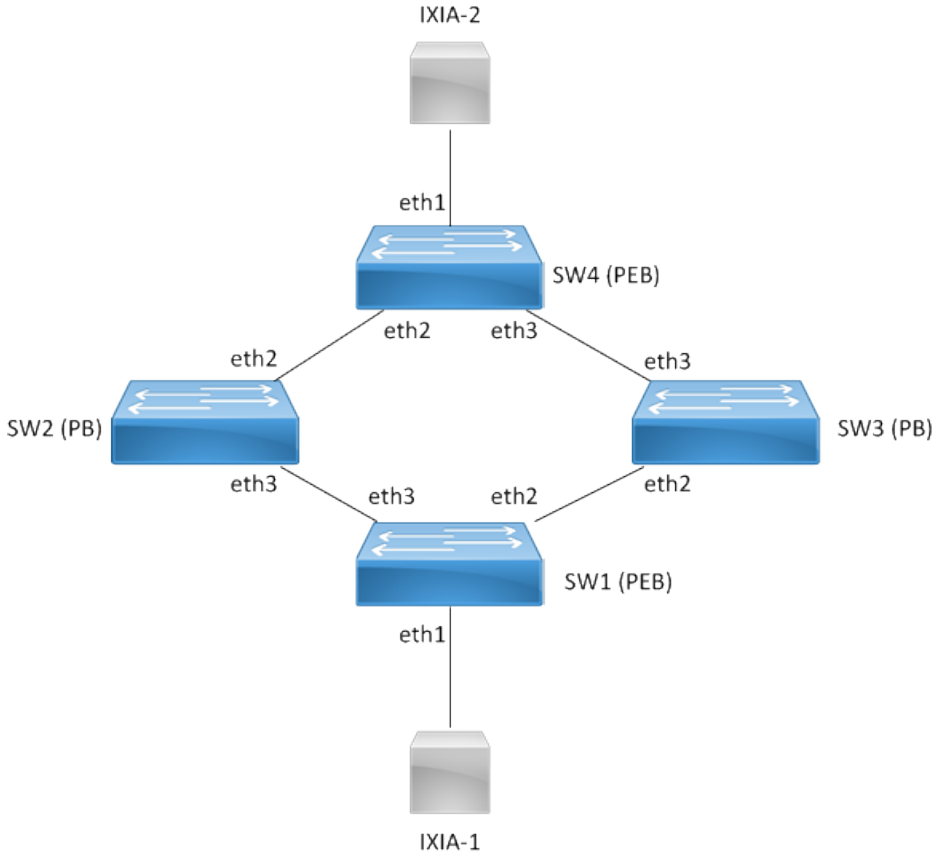
```
SW3#sh br
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1          2      200           eth1        0000.0000.0f00    1     300
 1          2      200           eth2        0001.0000.0800    1     300

SW1#sh br
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1          2      200           eth2        0000.0000.0f00    1     300
 1          2      200           eth1       0001.0000.0800    1     300

SW1#sh cvlan registration table
```

```
Bridge          Table Name       Port List

======          ==========       =========

1               map1             eth1

CVLAN ID        SVLAN ID
========        ========
2               200
```

Two Provider Bridge Configuration

Topology

Figure 26. Two provider bridge configuration



Configuration

SW1 (PEB)

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2 type customer bridge 1 state enable`	Create customer vlan VLAN 2

`SW1(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#cvlan registration table map1 bridge 1`	Create cvlan registration table map1
`SW1(config-cvlan-registration)#cvlan 2 svlan 200`	Map cvlan2 with svlan 200
`SW1(config-cvlan-registration)#exit`	Exit registration table
`SW1(config)#interface eth1`	Enter interface configuration mode for eth1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#witchport mode customer-edge hybrid`	Configure switchport mode customer edge
`SW1(config-if)#switchport customer-edge access vlan 2`	Associate customer vlan2 with interface
`SW1(config-if)#switchport customer-edge vlan registration map1`	Attach registration table map1 with interface
`SW1(config-if)#exit`	Exit interface mode
`SW1(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#interface eth3`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#commit`	Commit the configuration.
`SW1(config-if)#exit`	Exit interface configuration mode

SW2 (PB)

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface eth3`	Enter interface configuration mode for eth1
`SW2(config-if)#switchport`	Make interface as switchport

`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#exit`	Exit interface configuration mode
`SW2(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#commit`	Commit the configuration.
`SW2(config-if)#exit`	Exit interface configuration mode

SW3 (PB)

`SW3#configure terminal`	Enter configuration mode
`SW3(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW3(config)#vlan database`	Enter VLAN configuration mode
`SW3(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW3(config-vlan)#exit`	Exit VLAN configuration mode
`SW3(config)#interface eth3`	Enter interface configuration mode for eth1
`SW3(config-if)#switchport`	Make interface as switchport
`SW3(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW3(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW3(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW3(config-if)#exit`	Exit interface configuration mode
`SW3(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW3(config-if)#switchport`	Make interface as switchport
`SW3(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW3(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW3(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW3(config-if)#commit`	Commit the configuration.
`SW3(config-if)#exit`	Exit interface configuration mode

SW4 (PEB)

`SW4#configure terminal`	Enter configuration mode

SW4(config)#bridge 1 protocol provider-rstp edge	Create bridge
SW4(config)#vlan database	Enter VLAN configuration mode
SW4(config-vlan)#vlan 2 type customer bridge 1 state enable	Create customer vlan VLAN 2
SW4(config-vlan)#vlan 200 type service point-point bridge 1 state enable	Create service vlan VLAN200
SW4(config-vlan)#exit	Exit VLAN configuration mode
SW4(config)#cvlan registration table map1 bridge 1	Create cvlan registration table map1
SW4(config-cvlan-registration)#cvlan 2 svlan 200	Map cvlan2 with svlan 200
SW4(config-cvlan-registration)#exit	Exit registration table
SW4(config)#interface eth1	Enter interface configuration mode for eth1
SW4(config-if)#switchport	Configure switchport
SW4(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW4(config-if)#witchport mode customer-edge hybrid	Configure switchport mode customer edge
SW4(config-if)#switchport customer-edge access vlan 2	Associate customer vlan2 with interface
SW4(config-if)#switchport customer-edge vlan registration map1	Attach registration table map1 with interface
SW4(config-if)#exit	Exit interface mode
SW4(config-if)#interface eth2	Enter interface configuration mode for eth2
SW4(config-if)#switchport	Make interface as switchport
SW4(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW4(config-if)#switchport mode provider-network	Configure switchport pnp port
SW4(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW4(config-if)#interface eth3	Enter interface configuration mode for eth2
SW4(config-if)#switchport	Make interface as switchport
SW4(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW4(config-if)#switchport mode provider-network	Configure switchport pnp port
SW4(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW4(config-if)#commit	Commit the configuration.
SW4(config-if)#exit	Exit interface configuration mode

Validation

```
SW4#sh br
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1          2     200           eth1        0000.0000.0a00    1     300
 1          2     200           eth2        0001.0000.0b00    1     300

SW1#sh br
bridge 1 is running on provider-rstp edge
```

```
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1          2     200           eth1        0000.0000.0b00    1     300
 1          2     200           eth3        0001.0000.0a00    1     300

SW1#sh cvlan registration table
Bridge          Table Name       Port List

======          ==========       =========

1               map1             eth1

CVLAN ID        SVLAN ID
========        ========
2               200
```

Layer 2 Protocol Tunneling (L2PT/L2CP Tunneling)

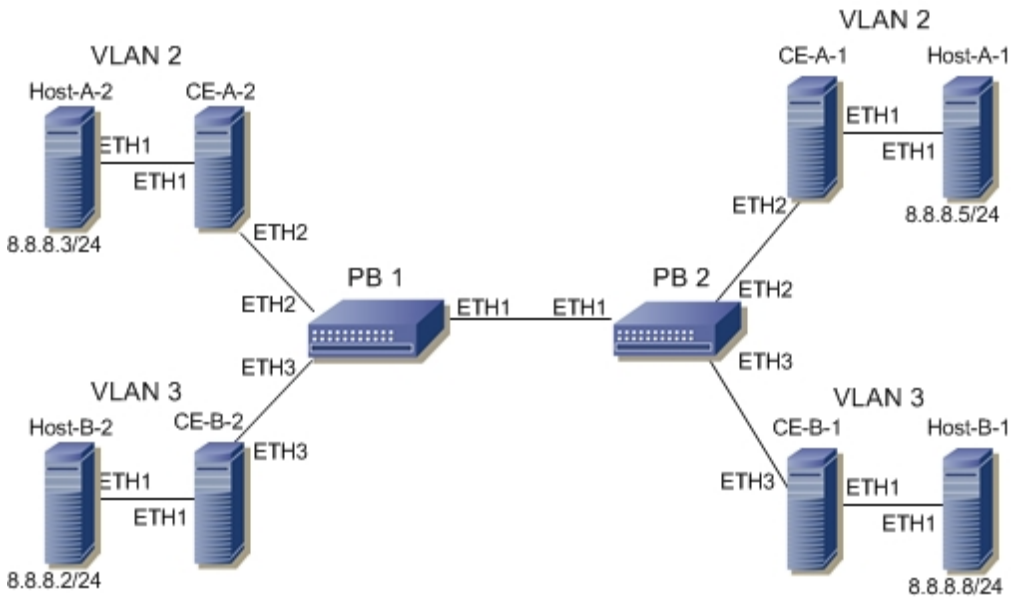
L2CP tunneling provides support for tunneling Control plane frames between CE nodes. When control frames received at CEP port of PE bridge, predefined multicast address (01-00-C2-CD-CD-D0) is used for tunneling the packets across service provider network. If control packets are customer vlan tagged or untagged, then PE bridge will append corresponding service vlan tag to the control packet as per registration table / vlan translation table mapped to the port and send it across the service provider as a data packet.

When tunneled control packet with multicast address (01-00-C2-CD-CD-D0) received on PNP port, the multicast address is replaced with corresponding control packet multicast address and cvlan/svlan removal or updating is done as per registration table / vlan translation table.

Topology

The following diagram displays a sample Provider Bridged topology with customer equipment.

Figure 27. Provider Bridging with Customer Equipment Topology



Configuring the L2PT Protocol on the Interface

The following L2PT protocols are supported:

- EFM: Ethernet first mile (Link OAM)
- ELMI: Ethernet Local Management Interface
- LACP: Link Aggregation Control Protocol
- LLDP: Link Layer Discovery Protocol
- STP: Spanning Tree Protocols

PB1

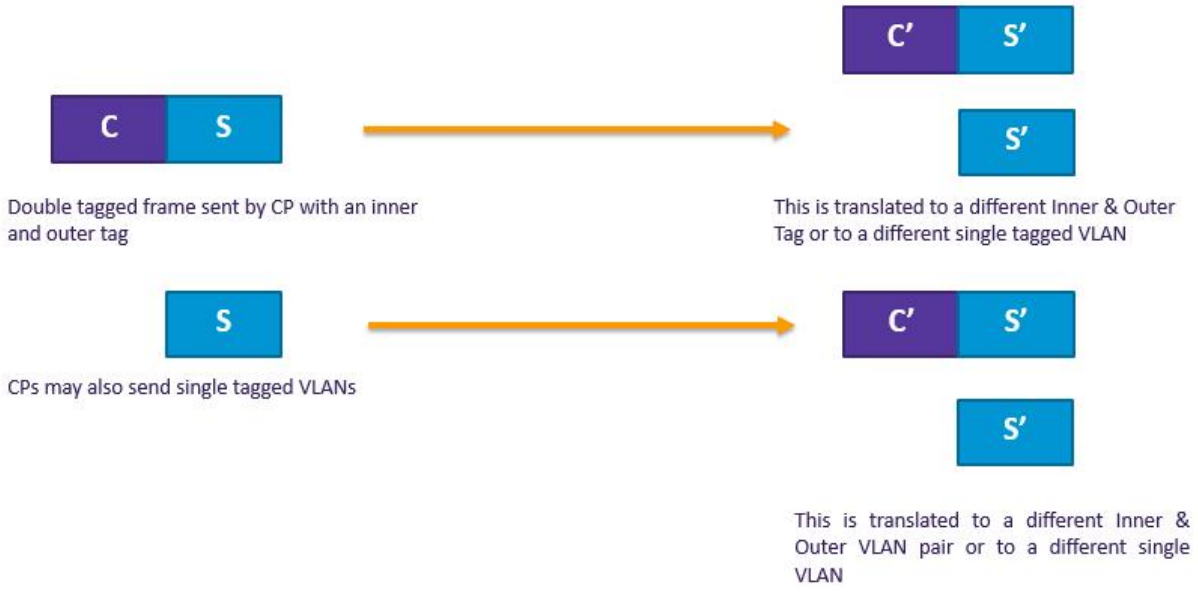
`PB1#configure terminal`	Enter Configure mode.
`PB1(config)#interface eth2`	Enter Interface mode
`PB1(config-if)#l2protocol stp peer`	Configure STP protocol as peer
`PB1(config-if)#l2protocol elmi tunnel`	Configure Elmi protocol as tunnel
`PB1(config-if)#l2protocol lldp tunnel`	Configure LLDP protocol as tunnel
`PB1(config-if)#l2protocol lacp discard`	Configure LACP protocol as discard
`PB1(config-if)#l2protocol efm discard`	Configure EFM protocol as discard
`PB1(config-if)#commit`	Commit the configuration.
`PB1(config-if)#exit`	Exit of the interface

Validation

```
PB1#show l2protocol processing interface eth2
Bridge    Interface Name                 Protocol       Processing Status
======    ==============                 ========       =================
1         eth2                           stp            Peer
1         eth2                           gmrp           Peer
1         eth2                           gvrp           Peer
1         eth2                           mmrp           Peer
1         eth2                           mvrp           Peer
1         eth2                           lacp           Discard
1         eth2                           lldp           Tunnel
1         eth2                           efm            Discard
1         eth2                           elmi           Tunnel
1         eth2                           ptp              Peer
```

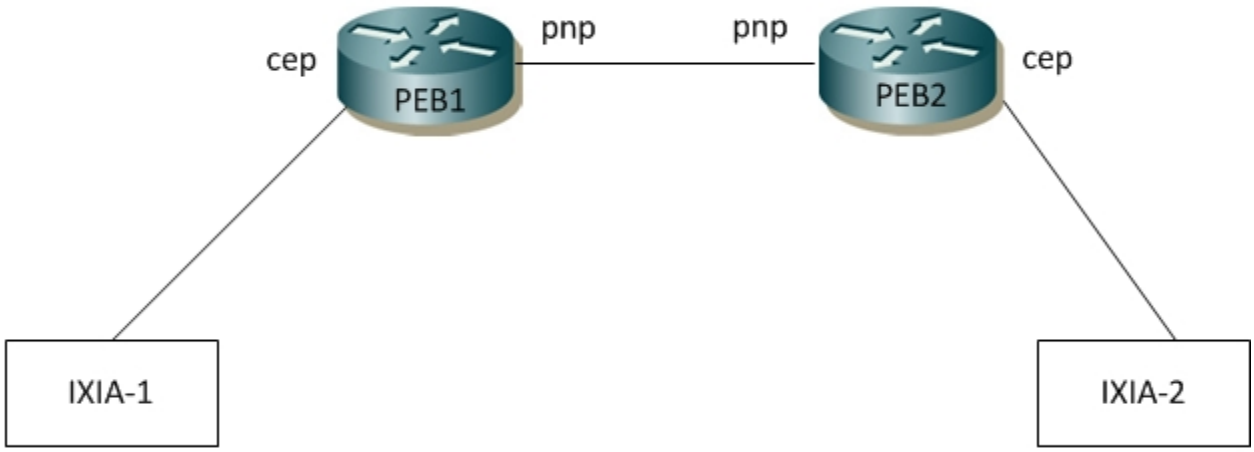
Provider Bridging with VLAN Translation

This is a sample configurations to verify functionality to support provider-bridging feature with extended SVLAN translation as below:



Topology

Figure 28. Provider Bridging with VLAN Traslation Topology



PEB1

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol provider-rstp edge`	Enter Configure bridge type as provider-RSTP edge bridge
`(config)#commit`	Commit the configuration.
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`(config-vlan)# vlan 2-500 type customer bridge 1 state enable`	Configure customer VLANs on bridge 1
`(config-vlan)#vlan 2-1005 type service point-point bridge 1 state enable`	Configure service VLANs on bridge 1
`(config-vlan)#commit`	Commit the configuration.
`(config-vlan)#end`	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode customer-edge hybrid`	Configure port as customer-edge hybrid port
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Add all VLANs configured above to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port

© 2026 IP Infusion Inc. Proprietary

(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

PEB2

Bridge Configuration

#configure terminal	Enter configure mode.
(config)# bridge 1 protocol provider-rstp edge	Enter configure bridge type as provider-RSTP edge bridge
(config-if)#commit	Commit the configuration.
(config)#exit	Exit configure mode.

VLAN Configuration

#configure terminal	Enter configure mode.
(config)#vlan database	Enter VLAN database
(config-vlan)#vlan 2-500 type customer bridge 1 state enable	Configure customer VLANs on bridge 1
(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable	Configure service VLANs on bridge 1
(config-if)#commit	Commit the configuration.
(config-vlan)#end	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

#configure terminal	Enter configure mode.
(config)#cvlan registration table map1 bridge 1	Configure CVLAN registration table as map1
(config-cvlan-registration)#cvlan 2 svlan 6	Map CVLAN to SVLAN
(config-cvlan-registration)#cvlan 3 svlan 7	Map CVLAN to SVLAN
(config-cvlan-registration)#commit	Commit the configuration.
(config-cvlan-registration)#end	End the CVLAN registration mode

CEP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode customer-edge hybrid	Configure port as customer-edge hybrid port
(config-if)#switchport customer-edge hybrid allowed vlan all	Add all VLANs configured above to this CEP port
(config-if)#switchport customer-edge vlan	Attach the Map1 to CEP port

© 2026 IP Infusion Inc. Proprietary

registration map1	
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge9	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Translation Cases

Case1 - (C S - C' S')

Configuration on PEB2

#configure terminal	Enter configure mode.
(config)#interface ge9	Enter the interface mode
(config-if)#switchport provider-network vlan translation cvlan 2 svlan 6 cvlan 3 svlan 7	Translate CVLAN and SVLAN to new CVLAN and new SVLAN on PNP port

Validation for Case 1

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with both CTAG and STAG entering provider network and gets translated to new CVLAN and SVLAN as per Case1.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address     FWD   Time-out
 ---------+------+------+------+-----------+----------------+-----+----------+
 1                1            ge27        1402.ec1c.3144    1     300
 1                6            ge9         6400.6a1e.d9a5    1     300
 1         3      7            ge9         0000.0500.0400    1     300
 1                7            ge9         6400.6a1e.d9a5    1     300
```

New SVLAN 7 is observed on PEB2 after translation. Also, captured packets on CEP show new CVLAN 3.

When tagged traffic for CVLAN 3 is sent from IXIA-2 to IXIA-1

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+----------------+-----+----------+
 1                1             ge9         74e6.e2af.598b    1     300
 1         2      6             ge3         0000.0500.0400    1     300
 1         2      6             ge9         0000.0500.0700    1     300
```

When traffic is reversed and traffic has both new CVLAN 3 and SVLAN 7 on provider network from IXIA-2, translation to old CVLAN 2 and SVLAN 6 happens. Also, captured packets have CVLAN as 2.

© 2026 IP Infusion Inc. Proprietary

Case2 - (C S - S')

Configuration on PEB2

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7 untagged-pep`	Map CVLAN to SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport customer-edge hybrid vlan 3`	Allow access VLAN 3 configured above to this CEP port
`(config-if)#switchport customer-edge hybrid allowed vlan add 2-3`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#no switchport provider-network vlan translation cvlan 2 svlan 6`	Unconfigure Translation Case1 from PNP port
`(config-if)#switchport provider-network vlan translation cvlan 2 svlan 6 svlan 7`	Configure Translation Case2 on PNP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

Validation for Case 2

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with both CTAG and STAG entering provider network and translated to new SVLAN as per Case2.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+----------+
 1                1            ge27        1402.ec1c.3144    1     300
 1                7            ge9         0000.0500.0400    1     300
```

New SVLAN 7 is observed on PEB2 after translation. At CEP port connected to IXIA-2, untagged traffic should be received.

When tagged traffic for CVLAN 3 is sent from IXIA-2 to IXIA-1.

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 --------+------+------+------+-----------+-----------------+-----+---------+
 1               1             ge9         74e6.e2af.598b    1     300
 1         2     6             ge3         0000.0500.0400    1     300
 1         2     6             ge9         0000.0500.0700    1     300
```

When traffic is reversed and traffic has both new CVLAN 3 and SVLAN 7 from IXIA-2, translatiom to old CVLAN 2 and SVLAN 6 happens. Also, captured packets have CVLAN as 2.

Case3 - (S - S')

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport customer-edge hybrid vlan 2`	Allow access VLAN 2 configured above to this CEP port
`(config-if)#switchport customer-edge hybrid allowed vlan add 2-3`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)

© 2026 IP Infusion Inc. Proprietary

(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge9	Enter the interface mode
(config-if)#no switchport provider-network vlan translation cvlan 2 svlan 6	Unconfigure Translation Case2 from PNP port
(config-if)#switchport provider-network vlan translation svlan 6 svlan 7	Configure Translation Case3 on PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Validation for Case 3

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with only STAG entering provider network and translation happens to new SVLAN as per Case3.

```
PEB2#show bridge
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1             ge27        1402.ec1c.3144    1     300
 1         2     6             ge9         0000.0500.0400    1     300
 1               6             ge9         6400.6a1e.d9a5    1     300
```

New SVLAN 7 is observed on PEB2 At PNP port connected to IXIA-2.

When double tagged traffic of CVLAN 2 and SVLAN 7 is sent from IXIA-2 to IXIA-1:

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1             ge9         74e6.e2af.598b    1     300
 1         3     7             ge3         0000.0500.0400    1     300
 1               6             ge9         0000.0500.0700    1     300
```

Here we get a tagged traffic of CVALN 2 when the captured at IXIA-1.

Case4 - (S - C' S')

Configuration on PEB1

CVLAN Registration Table Configuration

#configure terminal	Enter configure mode.
(config)#cvlan registration table map1 bridge 1	Configure CVLAN registration table as map1
(config-cvlan-registration)#cvlan 2 svlan 6 untagged-pep	Map CVLAN to SVLAN

(config-cvlan-registration)#cvlan 3 svlan 7	Map CVLAN to SVLAN
(config-cvlan-registration)#commit	Commit the configuration.
(config-cvlan-registration)#end	End the CVLAN registration mode

CEP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge3	Enter the interface mode
(config-if)#switchport customer-edge hybrid vlan 2	Allow access VLAN 2 configured above to this CEP port
(config-if)#switchport customer-edge hybrid allowed vlan add 2-3	Allow other VLANs configured to this CEP port
(config-if)#switchport customer-edge vlan registration map1	Attach the Map1 to CEP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

#configure terminal	Enter configure mode.
(config)#interface ge3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge9	Enter the interface mode
(config-if)#no switchport provider-network vlan translation svlan 6	Unconfigure Translation Case2 from PNP port
(config-if)#switchport provider-network vlan translation svlan 6 cvlan 3 svlan 7	Configure Translation Case3 on PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

© 2026 IP Infusion Inc. Proprietary

Validation for Case 4

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 enters provider network and translation happens to new CVLAN and new SVLAN as per Case4.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1             ge27        1402.ec1c.3144    1     300
 1         2     6             ge9         0000.0500.0400    1     300
 1               6             ge9         6400.6a1e.d9a5    1     300
```

When you observe the traffic received in IXIA-2, you can observe that new CVLAN 3 and SVLAN 7 tags can be seen. Here the VLAN 2 will be a data packet.

When tagged traffic for CVLAN 3 and SVLAN 7 is sent from IXIA-2 to IXIA-1:

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               6             ge3         0000.0500.0400    1     300
 1               7             ge9         0000.0500.0700    1     300
```

When you observe, in PEB1 the packets will be dropped at the CEP port since only a single S tagged packets is obtained in the PNP.

Case5 - (C - C' S')

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 cvlan3 svlan 4`	Map CVLAN to C'VLAN and SVLAN
`(config-cvlan-registration)#cvlan 5 cvlan 6 svlan 7`	Map CVLAN to C'VLAN and SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode customer-edge hybrid`	Configure port as customer-edge hybrid port
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port

© 2026 IP Infusion Inc. Proprietary

(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

#configure terminal	Enter configure mode.
(config)#interface ge3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge9	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Validation for Case 5

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with both CTAG and STAG entering provider network and gets translated to new CVLAN and SVLAN as per Case5.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1             ge27        1402.ec1c.3144    1     300
 1               4             ge9         0000.0500.0400    1     300
 1               7             ge9         6400.6a1e.d9a5    1     300
```

When the packet is captured at PNP port of PEB2 CVLAN of 3 and SVLAN of 4 is seen.

When tagged traffic for CVLAN 6 and SVLAN 7 is sent from IXIA-2 to IXIA-1:

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1             ge9         74e6.e2af.598b    1     300
```

```
  1               4             ge3         0000.0500.0400    1     300
  1        6      7             ge9         0000.0500.0700    1     300
```

When traffic is reversed and traffic has both new CVLAN 6 and SVLAN 7 on provider network from IXIA-2, translation to CVLAN 5 and SVLAN 7 happens. Also, captured packets have CVLAN as 2 based on the entry in the cvlan registration table.

Switchport ethertype

Bridge Configuration (for 0x88a8)

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 4`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port

© 2026 IP Infusion Inc. Proprietary

`(config-if)#dot1ad ethertype 0x88a8`	Change the TPID of the SVLAN to 0x88a8
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

Validation for Switchport ethertype

To validate, send tagged traffic of VLAN 2 from IXIA-1.

Now at eth9 of PB2, capture the packets through IXIA-2 and verify that the traffic is received with double tag.

If the 2 tags CVLAN tag 2 will have the TPID of 0x8100 and SVLAN tag 4 will have a TPID of 0x88a8.

Provider Bridging QoS Configuration

This section contains sample provider bridging configurations for QoS.

Scenario: 1 Traffic flow from CEP to PNP

Topology

Figure 29. Provider Bridging with QoS Topology

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol provider-rstp edge`	Enter configure bridge type as provider-RSTP edge bridge
`(config)#commit`	Commit the configuration.
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`(config-vlan)#vlan 2-500 type customer bridge 1 state enable`	Configure customer VLANs on bridge 1
`(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable`	Configure service VLANs on bridge 1

(config-vlan)#commit	Commit the configuration.
(config-vlan)#end	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

#configure terminal	Enter configure mode.
(config)#cvlan registration table map1 bridge 1	Configure CVLAN registration table as map1
(config-cvlan-registration)#cvlan 2 svlan 501	Map CVLAN to SVLAN
(config-cvlan-registration)#commit	Commit the configuration.
(config-cvlan-registration)#end	End the CVLAN registration mode

CEP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface xe2	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode customer-edge hybrid	Configure port as customer-edge hybrid port
(config-if)#switchport customer-edge hybrid allowed vlan all	Add all VLANs configured above to this CEP port
(config-if)#switchport customer-edge vlan registration map1	Attach the Map1 to CEP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface xe3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan add 501	Add all VLANs configured above to this PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

QoS Configurations

#configure terminal	Enter configure mode.
(config)#hardware-profile filter qos-ext enable	Enabling Ingress extended QoS group for QoS support with statistics

© 2026 IP Infusion Inc. Proprietary

`(config-if)#qos enable`	Enabling QoS
`(config-if)#qos statistics`	Enabling QoS statistics
`(config-if)#qos profile cos-to-queue cosq-cust1`	Configure QoS map profile
`config-ingress-cos-map)#cos 0 queue 1`	Configuring the cos value to be mapped to queue
`(config-ingress-cos-map)#exit`	Exit configure mode.
`(config)#qos profile queue-color-to-cos cosq-service1`	Configuring profile for queue color to cos map
`(config-egress-cos-map)#queue 1 cos 3`	Configuring the queue value to be cos remarked.
`(config-egress-cos-map)#exit`	Exit configure mode
`(config)#cvlan registration table map1 bridge 1`	Enter CVLAN registration mode
`(config-cvlan-registration)#cvlan 2 svlan 501 cos-to-queue cosq-cust1`	Map CVLAN to SVLAN with QoS map profile. Eg: when vlan 2 customer traffic with cos 0 value is received, queue will be assigned to 1 based on mapping.
`(config-cvlan-registration)#end`	End the CVLAN registration mode
`(config)#interface xe3`	Enter the interface mode
`(config-if)#qos map-profile queue-color-to-cos cosq-service1`	Map the profile to the PNP port. Eg: when traffic goes out of queue 1, cos value on service vlan header will be modified to 3 as remarking is enabled on the interface.
`(config-if)#qos remark cos enable`	Enabling Cos Remark on the Network Interface.
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

Validation for Scenario 1

```
#show cvlan registration table map1
Bridge          Table Name       Port List
======          ==========       =========
1               map1             xe2

CVLAN ID        T-CVLAN ID      SVLAN ID        Profile Name    Egress remark-Cos
========        ==========      ========        ============    =================
2               -               501             cosq-cust1      No

#show qos-profile interface xe2
profile name: default
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       2       green    |  2       1       2       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow
```

```
profile name: default
 profile type: queue-color-to-cos (Egress)
 Status: Inactive
mapping:
 ----------------+-------- | ----------------+-------- | ----------------+--------
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      | OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+--------
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+--------
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7

#show qos-profile interface xe3
profile name: default
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       2       green    |  2       1       2       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

profile name: cosq-service1
 profile type: queue-color-to-cos (Egress)
 Status: Active
mapping:
 ----------------+-------- | ----------------+-------- | ----------------+--------
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      | OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+--------
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+--------
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    3       |  1       yellow   3       |  1       red      3
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7
```

© 2026 IP Infusion Inc. Proprietary

Scenario: 2 Traffic flow from PNP to CEP

Topology

Figure 30. Provider Bridging with QoS Topology

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol provider-rstp edge`	Enter configure bridge type as provider-RSTP edge bridge
`(config)#commit`	Commit the configuration.
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`(config-vlan)#vlan 2-500 type customer bridge 1 state enable`	Configure customer VLANs on bridge 1
`(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable`	Configure service VLANs on bridge 1
`(config-vlan)#commit`	Commit the configuration.
`(config-vlan)#end`	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

© 2026 IP Infusion Inc. Proprietary

CEP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface xe2	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode customer-edge hybrid	Configure port as customer-edge hybrid port
(config-if)#switchport customer-edge hybrid allowed vlan all	Add all VLANs configured above to this CEP port
(config-if)#switchport customer-edge vlan registration map1	Attach the Map1 to CEP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface xe3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan add 501	Add all VLANs configured above to this PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

QoS Configurations

#configure terminal	Enter configure mode.
(config)#hardware-profile filter qos-ext enable	Enabling Ingress extended QoS group for QoS support with statistics
(config-if)#qos enable	Enabling QoS
(config-if)#qos statistics	Enabling QoS statistics
(config-if)#qos profile cos-to-queue cosq-cust1	Configure QoS map profile
config-ingress-cos-map)#cos 2 queue 5	Configuring the cos value to be mapped to queue. Eg: when double tagged traffic with cos 2 for outer vlan is received, queue will be assigned to 5 based on mapping.
(config-ingress-cos-map)#exit	Exit configure mode.
(config)#cvlan registration table map1 bridge 1	Enter CVLAN registration mode
(config-cvlan-registration)#cvlan 2 svlan 501 remark-cos	Map CVLAN to SVLAN with remark cos enabled. Eg: when double tagged traffic with cos 2 for outer

	vlan is received, queue will be assigned to 5 based on mapping and cos value will be changed to 5 when it goes out of cep port since remark cos is enabled.
`(config-cvlan-registration)#cvlan 3 svlan 501 remark-cos`	Map CVLAN to SVLAN without remark cos. Eg: when double tagged traffic with cos 2 for outer vlan is received, and cos value will be forwarded as it is when it goes out of cep port since remark cos is not enabled for customer2.
`(config-cvlan-registration)#end`	End the CVLAN registration mode
`(config)#configure terminal`	Enter configure mode
`(config)#interface xe3`	Enter the interface mode
`(config-if)#qos map-profile cos-to-queue cosq-service`	Map the profile to the PNP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode

Validation for Scenario 2

```
#show cvlan registration table map1
Bridge          Table Name       Port List
======          ==========       =========
1               map1             xe2

CVLAN ID        T-CVLAN ID      SVLAN ID        Profile Name    Egress remark-Cos
========        ==========      ========        ============    =================
2               -               501             N/A             Yes
3               -               501             N/A             No

#show qos-profile interface xe2
profile name: default
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       2       green    |  2       1       2       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

profile name: default
 profile type: queue-color-to-cos (Egress)
 Status: Inactive
mapping:
 ----------------+-------- | ----------------+-------- | ----------------+--------
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      | OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+--------
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+--------
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    2       |  2       yellow   2       |  2       red      2
```

```
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7

#show qos-profile interface xe3
profile name: cosq-service
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       5       green    |  2       1       5       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

profile name: default
 profile type: queue-color-to-cos (Egress)
 Status: Inactive
mapping:
 ----------------+-------- | ----------------+-------- | ----------------+--------
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      | OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+--------
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+--------
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7
```

Provider Bridging Untagged-pep Configuration

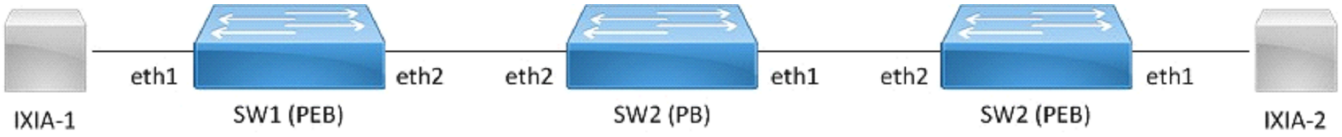
This is a sample configuration to verify functionality to support provider-bridging with untagged-pep feature.

For the below topology configuration,

1. While sending tagged traffic untagged-pep CVLAN 2, it should drop in provider edge bridge.
2. And while sending tagged traffic CVLAN 3 to the provider network, will egress with CVLAN 3 and SVLAN 12 tag and the same CVLAN and SVLAN tag from provider network, will egress with only CVLAN tag
3. And also for untagged traffic to the provider network, will egress with SVLAN 11 tag

Topology

Figure 31. Provider bridging untagged-pep configuration



Configuration

SW1 (PEB)

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2-10 type customer bridge 1 state enable`	Create customer vlan VLAN 2-10
`SW1(config-vlan)#vlan 11-15 type service point-point bridge 1 state enable`	Create service vlan VLAN 11-15
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#cvlan registration table map1 bridge 1`	Create cvlan registration table map1
`SW1(config-cvlan-registration)#cvlan 2 svlan 11 untagged-pep`	Map cvlan2 with svlan 11
`SW1(config-cvlan-registration)#cvlan 3 svlan 12`	Map cvlan3 with svlan 12
`SW1(config-cvlan-registration)#cvlan 4 svlan 14`	Map cvlan4 with svlan 14
`SW1(config-cvlan-registration)#exit`	Exit registration table
`SW1(config)#interface eth1`	Enter interface configuration mode for eth1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#witchport mode customer-edge hybrid`	Configure switchport mode customer edge
`SW1(config-if)#switchport customer-edge hybrid vlan 2`	Associate customer vlan2 with interface
`SW1(config-if)#switchport customer-edge hybrid allowed vlan all`	Associate all customer vlan with interface
`SW1(config-if)#switchport customer-edge vlan registration map1`	Attach registration table map1 with interface
`SW1(config-if)#exit`	Exit interface mode
`SW1(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider- network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#commit`	Apply the commit
`SW1(config-if)#exit`	Exit interface configuration mode
`SW1(config)#end`	Exit configuration mode

SW2 (PB)

`SW2#configure terminal`	Enter configuration mode

`SW2(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)# vlan 2-15 type service point-point bridge 1 state enable`	Create service vlan VLAN2-15
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface eth1`	Enter interface configuration mode for eth1
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider- network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#exit`	Exit interface configuration mode
`SW2(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider- network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#commit`	Apply the commit
`SW2(config-if)#exit`	Exit interface configuration mode
`SW2(config)#end`	Exit configuration mode

SW3 (PEB)

`SW3#configure terminal`	Enter configuration mode
`SW3(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW3(config)#vlan database`	Enter VLAN configuration mode
`SW3(config-vlan)#vlan 2-10 type customer bridge 1 state enable`	Create customer vlan VLAN 2-10
`SW3(config-vlan)#vlan 11-15 type service point-point bridge 1 state enable`	Create service vlan VLAN11-15
`SW3(config-vlan)#exit`	Exit VLAN configuration mode
`SW3(config)#cvlan registration table map1 bridge 1`	Create cvlan registration table map1
`SW3(config-cvlan-registration)#cvlan 2 svlan 11 untagged-pep`	Map cvlan2 with svlan 200
`SW3(config-cvlan-registration)#cvlan 3 svlan 12`	Map cvlan3 with svlan 12
`SW3(config-cvlan-registration)#cvlan 4 svlan 14`	Map cvlan4 with svlan 14
`SW3(config-cvlan-registration)#exit`	Exit registration table
`SW3(config)#interface eth1`	Enter interface configuration mode for eth1
`SW3(config-if)#switchport`	Configure switchport

© 2026 IP Infusion Inc. Proprietary

`SW3(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW3(config-if)#witchport mode customer-edge hybrid`	Configure switchport mode customer edge
`SW3(config-if)#switchport customer-edge hybrid vlan 2`	Associate customer vlan2 with interface
`SW3(config-if)#switchport customer-edge hybrid allowed vlan all`	Associate all customer vlan with interface
`SW3(config-if)#switchport customer-edge vlan registration map1`	Attach registration table map1 with interface
`SW3(config-if)#exit`	Exit interface mode
`SW3(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW3(config-if)#switchport`	Make interface as switchport
`SW3(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW3(config-if)#switchport mode provider- network`	Configure switchport pnp port
`SW3(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW3(config-if)#commit`	Apply the commit
`SW3(config-if)#exit`	Exit interface configuration mode
`SW3(config)#end`	Exit configuration mode

Validation

```
SW3#sh bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         4      14            eth1         0000.0100.0007    1     300

SW1#sh bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1                14            eth1       0000.0100.0007    1     300

SW1#sh cvlan registration table map1
Bridge          Table Name       Port List

======          ==========       =========

1               map1             eth2

CVLAN ID        T-CVLAN ID      SVLAN ID        CCOS  SCOS  CCFI  SCFI
========        ==========      ========        ====  ====  ====  ====
3               -               12
2               -               11
4               -               14
```

Provider Bridging Configuration (SVLAN)

This section contains sample provider bridging configurations for Customer-Network Port (CNP).

A provider bridged network is a virtual bridged Local Area Network that comprises provider bridges (SVLAN bridges and provider edge bridges) and attached LANs, under the administrative control of a single service provider. Provider bridges interconnect the separate MACs of the IEEE 802 LANs that compose a provider bridged network, relaying frames to provide connectivity between all the LANs that provide customer interfaces for each service instance.

Note: CVLAN information is not displayed in the output of `show bridge` CLI as it depends on the hardware learning.

Customer-Network Port (CNP)

In Q-in-Q, the customer network port is similar to provider network port, which can be present in provider-edge bridge (PEB) or provider bridge core (PB), where it can be directly connected to a dedicated customer network. Only SVLAN ids are configurable on Customer network port and learning and forwarding occurs based on SVLAN.

STAG-based Interface

In this case, the customer will be sending traffic with SVLAN, which will be learned and forwarded via provider network.

In this example, the xe1 interface allows S-TAG 100-200 and 400 traffic from customer.

```
(config)#interface xe1
(config-if)#switchport
(config-if)#dot1ad ethertype 0x88a8
(config-if)#bridge-group 1
(config-if)#switchport mode customer-network
(config-if)#switchport customer-network allowed vlan add 100-200,400
```

Port-based Interface

In this case, the customer traffic with C-VLAN/untagged, received on interface will be stacked with a customer-network SVLAN ID and will be forwarded via provider network. While egressing out of customer-network port for the default SVLAN, the outer SVLAN id will be stripped and the packet will be sent as C-TAG or untagged to customer device.

In this example, the xe1 interface allows C-TAG/untagged traffic from customers, adding an SVLAN ID 100 before forwarding to the provider network. While egressing out, the SVLAN ID100 will be stripped.

```
(config)#interface xe1
(config-if)#switchport
(config-if)#dot1ad ethertype 0x88a8
(config-if)#bridge-group 1
(config-if)#switchport mode customer-network
(config-if)#switchport customer-network allowed vlan add 100
(config-if)#switchport customer-network vlan 100
```

© 2026 IP Infusion Inc. Proprietary

Topology

Figure 32. Single provider bridge configuration

Configuration

SW1 (PEB)

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 100,200 type service point-point bridge 1 state enable`	Create service vlan VLAN 100, 200
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface eth1`	Enter interface configuration mode for eth1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#dot1ad ethertype 0x88a8`	Add Provider Bridging Service VLAN tag identifier
`SW1(config-if)#switchport mode customer-network`	Configure switchport mode for CNP(customer network port)
`SW1(config-if)#switchport customer-network allowed vlan add 200`	Associate vlan 200 with interface
`SW1(config-if)#switchport customer-network vlan 200`	Add vlan 200 as default SVLAN-ID for traffic with CVLAN/untagged
`SW1(config-if)#exit`	Exit interface mode
`SW1(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider- network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#commit`	Commit the configuration.
`SW1(config-if)#exit`	Exit interface configuration mode

© 2026 IP Infusion Inc. Proprietary

SW2 (PB)

SW2#configure terminal	Enter configuration mode
SW2(config)#bridge 1 protocol provider-rstp	Create provider bridge
SW2(config)#vlan database	Enter VLAN configuration mode
SW2(config-vlan)#vlan 200 type service point-point bridge 1 state enable	Create service vlan VLAN200
SW2(config-vlan)#exit	Exit VLAN configuration mode
SW2(config)#interface eth1	Enter interface configuration mode for eth1
SW2(config-if)#switchport	Make interface as switchport
SW2(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW2(config-if)#switchport mode provider- network	Configure switchport pnp port
SW2(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW2(config-if)#exit	Exit interface configuration mode
SW2(config-if)#interface eth2	Enter interface configuration mode for eth2
SW2(config-if)#switchport	Make interface as switchport
SW2(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW2(config-if)#switchport mode provider- network	Configure switchport pnp port
SW2(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW2(config-if)#commit	Commit the configuration.
SW2(config-if)#exit	Exit interface configuration mode

SW3 (PEB)

SW3#configure terminal	Enter configuration mode
SW3(config)#bridge 1 protocol provider-rstp edge	Create bridge
SW3(config)#vlan database	Enter VLAN configuration mode
SW3(config-vlan)#vlan 200 type service point-point bridge 1 state enable	Create service vlan VLAN200
SW3(config-vlan)#exit	Exit VLAN configuration mode
SW3(config)#interface eth1	Enter interface configuration mode for eth1
SW3(config-if)#switchport	Configure switchport
SW3(config-if)#dot1ad ethertype 0x88a8	Add Provider Bridging Service VLAN tag identifier
SW3(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW3(config-if)#switchport mode customer-network	Configure switchport CNP port
SW3(config-if)#switchport customer-network allowed vlan add 200	Associate vlan 200 with interface
SW3(config-if)#switchport customer-network vlan 200	Add vlan 200 as default SVLAN-ID for traffic with CVLAN/untagged

© 2026 IP Infusion Inc. Proprietary

SW3(config-if)#exit	Exit interface mode
SW3(config-if)#interface eth2	Enter interface configuration mode for eth2
SW3(config-if)#switchport	Make interface as switchport
SW3(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW3(config-if)#switchport mode provider- network	Configure switchport pnp port
SW3(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW3(config-if)#commit	Commit the configuration.
SW3(config-if)#exit	Exit interface configuration mode

Validation

```
SW3#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected here also
Bridge    CVLAN  SVLAN  BVLAN     Port       MAC Address    FWD   Time-out
---------+------+------+------+-----------+----------------+-----+------+
     1             200            eth1      0000.0000.0f00    1     300
     1             200            eth2      0001.0000.0800    1     300

SW1#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected here also
Bridge    CVLAN  SVLAN  BVLAN     Port       MAC Address    FWD   Time-out
---------+------+------+------+-----------+----------------+-----+------+
     1             200            eth2      0000.0000.0f00    1     300
     1             200            eth1      0001.0000.0800    1     300
```

Traffic Mirroring Configuration

This section contains a sample local and remote switched port analyzer feature configuration.

SPAN Overview

Switched Port Analyzer (SPAN) refers to selecting network traffic for analysis by a network analyzer. SPAN feature is introduced on switches as the switch forwards traffic that is destined for a MAC address directly to the corresponding port leaving no scope to analyze the traffic.

SPAN monitors the traffic on source port and sends a copy of the traffic to a destination port. The network analyzer, which is attached to the destination port, analyzes the received traffic. Source port can be a single port or multiple ports. A replication of the packets is sent to the destination port for analysis

SPAN is originally referred to port mirroring or port monitoring where all the network traffic on the source port is mirrored to destination port. Port mirroring has three subdivisions.

- Ingress mirroring: Traffic received on the source port will be monitored
- Egress mirroring: Traffic transmitted from the source port will be monitored
- Ingress and egress mirroring: Both received and transmitted traffic on the source port will be monitored.

With enhancements to SPAN, mirroring can be classified into three categories.

Port Mirroring

In port mirroring, source will be a port which could be a physical interface or a port channel. All the traffic on the source port will be mirrored to destination port. Either traffic received on the source port or traffic transmitted from the source port or both can be monitored.

Notes:

- If monitor session configured with two or more source interfaces in the Egress direction (tx) then the destination mirror port will receive only one copy of the non-unicast packet.
- The Service VLAN (dot1ad) TPID for mirrored traffic is set to 0x8100 only when the egress packet is mirrored.
- When ingress traffic is mirrored, the TPID is maintained as 0x88a8.

VLAN Mirroring

In VLAN mirroring, the source is a VLAN identifier and the traffic received on all ports with the VLAN identifier matching source VLAN identifier are mirrored to destination port.

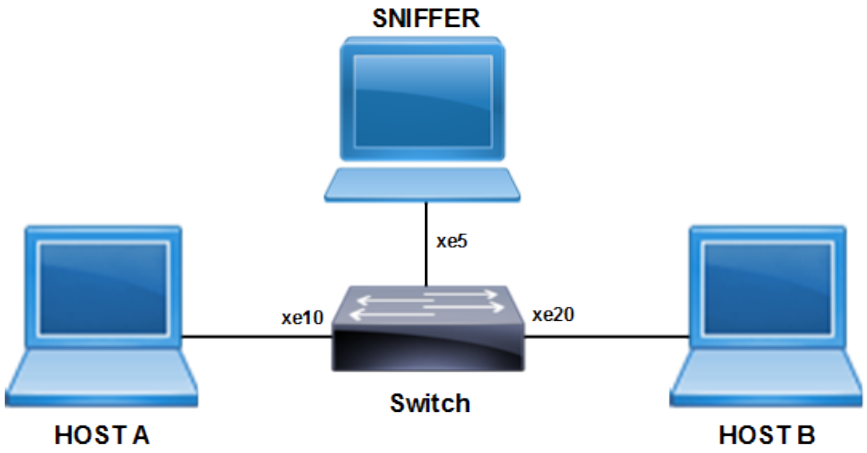
Rule Based Mirroring

In rule based mirroring, there is a set of matching criteria for the ingress traffic such as matching destination MAC address, matching frame type, and so on. The traffic matching the rules is mirrored to the destination port

© 2026 IP Infusion Inc. Proprietary

Topology

Figure 33. SPAN Topology



Port Mirroring Configuration

This example shows detailed configuration of port mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe5`	Enter interface mode.

© 2026 IP Infusion Inc. Proprietary

(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1	Enter monitor session configuration mode
(config-monitor)# destination interface xe5	Configure the interface as destination port
(config-monitor)# source interface xe10 both	Configure the source interface to mirror ingress as well as egress direction traffic
(config-monitor)# no shut	Activate monitor session
(config-monitor)#end	Exit monitor session configuration mode

Validation

Enter the below commands to confirm the configurations.

```
#show running-config monitor
!
monitor session 1
 source interface xe10 both
 destination interface xe5
 no shut

#show monitor session all
   session 1
---------------
type              : local
state             : up
source intf       :
    tx            : xe10
    rx            : xe10
    both          : xe10
source VLANs      :
    rx            :
destination ports : xe5
filter count      :

Legend: f = forwarding enabled, l = learning enabled
```

If monitor session configured with two source interface as egress direction (tx) then the destination port will receive only one copy of the egressed packet.

#configure terminal	Enter configure mode.
(config)# bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)# vlan 101-110 bridge 1 state enable	Configure VLANs.
(config)#interface xe10	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.

© 2026 IP Infusion Inc. Proprietary

(config)#interface xe20	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe30	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1	Enter monitor session configuration mode
(config-monitor)# destination interface xe5	Configure the interface as destination port
(config-monitor)# source interface xe10 tx	Configure the source interface to mirror egress direction traffic
(config-monitor)# source interface xe30 tx	Configure the source interface to mirror egress direction traffic
(config-monitor)# no shut	Activate monitor session
(config-monitor)#end	Exit monitor session configuration mode

Validation

```
#show running-config monitor
!
monitor session 1
source interface xe10 tx
source interface xe30 tx
destination interface xe5
no shut

#show monitor session all
       session 1
    ---------------
Type                : local
State               : up
source intf         :
        tx          : xe10  xe30
        rx          :
        both        :
```

```
source VLANs        :
        rx          :
destination ports   : xe5
filter count        :
Legend: f = forwarding enabled, l = learning enable
```

If you send 10 frames from xe20 packets egress via xe10 and xe30, then on mirror destination port only 10 packets are received.

VLAN and Rule Based Mirroring

This example shows detailed configuration of VLAN with rule based mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe5`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)#exit`	Exit interface mode.
`(config)# monitor session 1`	Enter monitor session configuration mode
`(config-monitor)# destination interface xe5`	Configure the interface as destination port
`(config-monitor)# source vlan 101`	Configure source VLAN to be mirrored
`(config-monitor)# filter src-mac host 0000.0000.0005`	Configure the rule to match the source MAC
`(config-monitor)# no shut`	Activate monitor session
`(config-monitor)#end`	Exit monitor session configuration mode

© 2026 IP Infusion Inc. Proprietary

Validation

Enter the below commands to confirm the configurations.

```
#show running-config monitor
!
monitor session 1
 source vlan 101
 destination interface xe5
 10 filter src-mac host 0000.0000.0005
 no shut


#show monitor session all
   session 1
---------------
type              : local
state             : up
source intf       :
    tx            :
    rx            :
    both          :
source VLANs      :
    rx            : 101
destination ports : xe5
filter count      : 1

Legend: f = forwarding enabled, l = learning enabled


#show monitor session 1 filter
   session 1
---------------
filter count      : 1

  ---------------
  match set 1
  ---------------
  source mac address : 0000.0000.0005 (host)
```

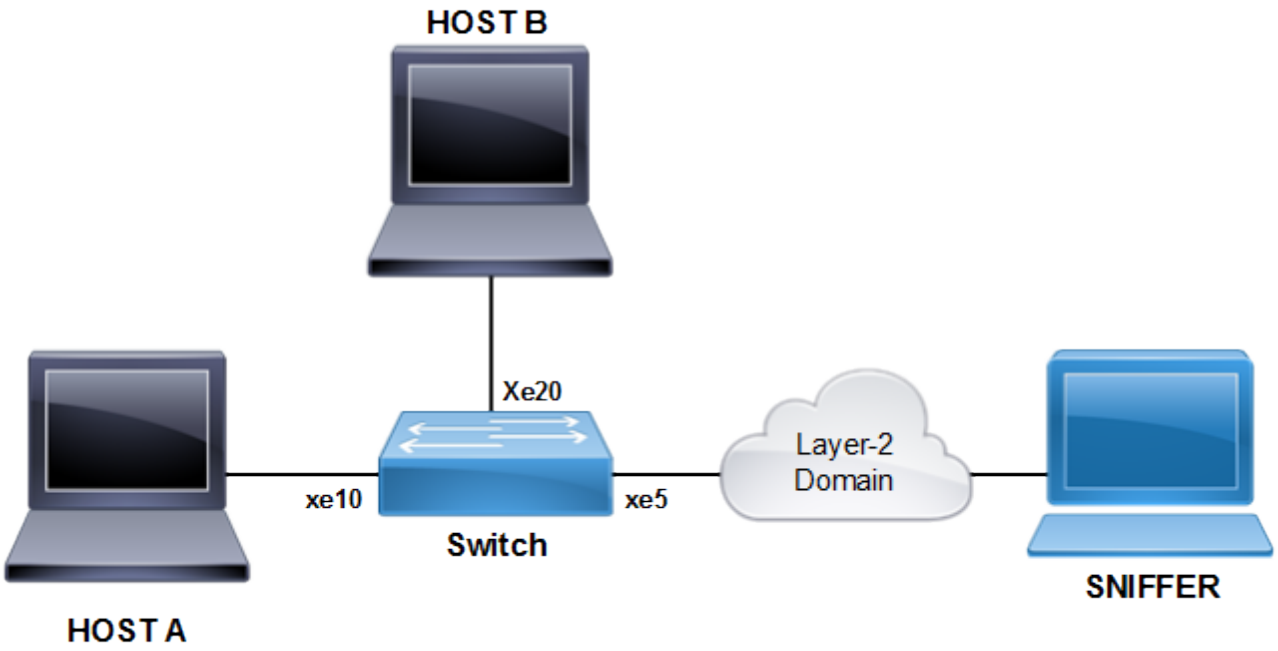
RSPAN Overview

When several switches need to be analyzed with a single centralized sniffer, remote switched port analyzer (RSPAN) is used. In RSPAN, all the mirrored traffic will be tagged with a RSPAN VLAN ID and forwarded to remote destination via a port called reflector port. Reflector port will have the same characteristics of a local destination port. RSPAN VLAN ID will be a dedicated VLAN for the monitoring purpose and will not participate in bridging. RSPAN destination switch will strip the RSPAN VLAN tag and send it the sniffer for analysis. RSPAN will have the same sub-categories as SPAN except that the mirrored traffic will be tagged with RSPAN VLAN header and forwarded to destination switch for analysis.

© 2026 IP Infusion Inc. Proprietary

Topology

Figure 34. RSPAN Topology



Port Mirroring Configuration

This example shows detailed configuration of port mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.

© 2026 IP Infusion Inc. Proprietary

(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1 type remote	Enter monitor session configuration mode.
(config-monitor)# destination remote vlan 100 reflector-port xe5	Configure the interface as remote destination port
(config-monitor)# source interface xe10 both	Configure the source interface to mirror ingress as well as egress direction traffic.
(config-monitor)# no shut	Activate monitor session.
(config-monitor)#end	Exit monitor session configuration mode.

Validation

Enter the commands below to confirm the configurations

```
#show running-config monitor
!
monitor session 1 type remote
 source interface xe10 both
 destination remote vlan 100 reflector-port xe5
 no shut


#show monitor session all
   session 1
---------------
type               : remote
state              : up
source intf        :
    tx             : xe10
    rx             : xe10
    both           : xe10
source VLANs       :
    rx             :
rspan VLAN         : 100
reflector ports    : xe5
filter count       :

Legend: f = forwarding enabled, l = learning enabled
```

VLAN and Rule Based Mirroring Configuration

This example shows detailed configuration of VLAN with rule based mirroring.

#configure terminal	Enter configure mode.
(config)# bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)# vlan 101-110 bridge 1 state enable	Configure VLANs.
(config)#interface xe10	Enter interface mode.

(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe20	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1 type remote	Enter monitor session configuration mode.
(config-monitor)# destination remote vlan 100 reflector-port xe5	Configure the interface as remote destination port.
(config-monitor)# source vlan 101	Configure source VLAN to be mirrored.
(config-monitor)# filter src-mac host 0000.0000.0005	Configure the rule to match the source MAC.
(config-monitor)# no shut	Activate monitor session.
(config-monitor)#end	Exit monitor session configuration mode.

Validation

Enter the commands below to confirm the configuration.

```
#show running-config monitor
!
monitor session 1 type remote
 source vlan 101
 destination remote vlan 100 reflector-port xe5
 10 filter src-mac host 0000.0000.0005
 no shut


#show monitor session all
   session 1
---------------
type              : remote
state             : up
source intf       :
    tx            :
    rx            :
    both          :
```

```
source VLANs      :
    rx            : 101
rspan VLAN        : 100
reflector ports   : xe5
filter count      : 1

Legend: f = forwarding enabled, l = learning enabled


#show monitor session 1 filter
   session 1
---------------
filter count      : 1

  ---------------
  match set 1
  ---------------
  source mac address : 0000.0000.0005 (host)
```

VLAN Mirroring Using VLAN Ranges Configuration

The Switch Port Analyzer (SPAN) monitors the traffic on source port and sends a copy of the traffic to a destination port. The network analyzer, which is attached to the destination port, analyzes the received traffic. The source port can either be a single port or multiple ports. A replication of the packets is sent to the destination port for analysis.

The SPAN is also referred to as port mirroring or port monitoring. It is installed in Layer 2 Access Control List (ACL) group by default. It is used for monitoring Ingress MAC ACL or VLAN group. Any packet received can be monitored based on source port including Physical or MAC or VLAN port.

This is an existing VLAN monitor session feature in the OcNOS DC, enhanced in current release to support VLAN ranges.

The following two CLIs are updated to support the VLAN ranges:

- hardware-profile filter (XGS)
- filter

Feature Characteristics

The VLAN range is supported only for ingress traffic.

LIMITATIONS

The ingress port mirroring is not supported for sub-interface and Switched Virtual Interface (SVI) interface.

Benefits

Users can apply port monitoring rules for multiple source ports, multiple VLANs, and a combination of port and VLAN ranges.

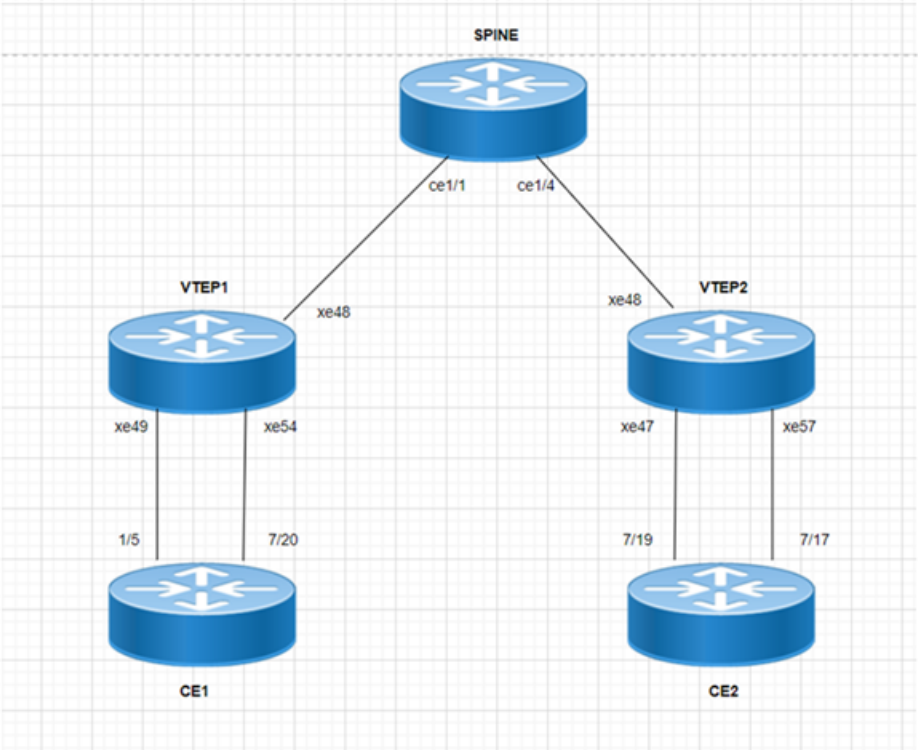
Configuration

To configure an ingress VLAN monitor session using VLAN ranges, perform the following configurations:

© 2026 IP Infusion Inc. Proprietary

Topology

Figure 35. SPAN Topology



VTEP1

`VTEP1#configure terminal`	Enter configure mode.
`VTEP1(config)#hardware-profile filter ingress-mirror enable`	Enable hardware profile igress mirror.
`VTEP1(config)#nvo vxlan enable`	Enable vxlan.
`VTEP1(config)#evpn esi hold-time 60`	Configure esi hold timer.
`VTEP1(config)#evpn vxlan multihoming enable`	Enable VxLAN multihoming.
`VTEP1(config)#mac vrf VRF1`	Configure MAC VRF as VRF1.
`VTEP1(config-vrf)#rd 1.1.1.1:11`	Configure route distinguisher value.
`VTEP1(config-vrf)#route-target both 9.9.9.9:100`	Configure route-target import and export.
`VTEP1(config)#mac vrf VRF2`	Configure MAC VRF as VRF2.
`VTEP1(config-vrf)#rd 1.1.1.1:21`	Configure route distinguisher value.
`VTEP1(config-vrf)#route-target both 90.90.90.90:100`	Configure route-target import and export.
`VTEP1(config)#mac vrf VRF3`	Configure MAC VRF as VRF3.
`VTEP1(config-vrf)#rd 1.1.1.1:22`	Configure route distinguisher value.
`VTEP1(config-vrf)#route-target both 90.90.90.90:101`	Configure route-target import and export.

© 2026 IP Infusion Inc. Proprietary

`VTEP1(config)#mac vrf VRF4`	Configure MAC VRF as VRF4.
`VTEP1(config-vrf)#rd 1.1.1.1:23`	Configure route distinguisher value.
`VTEP1(config-vrf)#route-target both 10.10.10.10:100`	Configure route-target import and export.
`VTEP1(config)#mac vrf VRF5`	Configure MAC VRF as VRF5.
`VTEP1(config-vrf)#rd 1.1.1.1:24`	Configure route distinguisher value.
`VTEP1(config-vrf)#route-target both 20.20.20.20:100`	Configure route-target import and export.
`VTEP1(config)#mac vrf VRF6`	Configure MAC VRF as VRF6.
`VTEP1(config-vrf)#rd 1.1.1.1:25`	Configure route distinguisher value.
`VTEP1(config-vrf)#route-target both 30.30.30.30:100`	Configure route-target import and export.
`VTEP1(config)#mac vrf VRF7`	Configure MAC VRF as VRF7.
`VTEP1(config-vrf)#rd 1.1.1.1:26`	Configure route distinguisher value.
`VTEP1(config-vrf)#route-target both 40.40.40.40:100`	Configure route-target import and export.
`VTEP1(config-vrf)#exit`	Exit from VRF mode
`VTEP1(config)#mac vrf VRF8`	Configure MAC VRF as VRF8
`VTEP1(config-vrf)#rd 1.1.1.1:27`	Configure route distinguisher value.
`VTEP1(config-vrf)#route-target both 50.50.50.50:100`	Configure route-target import and export.
`VTEP1(config-vrf)#exit`	Exit from VRF mode.
`VTEP1(config)#mac vrf VRF9`	Configure MAC VRF as VRF2.
`VTEP1(config-vrf)#rd 1.1.1.1:28`	Configure route distinguisher value.
`VTEP1(config-vrf)#route-target both 60.60.60.60:100`	Configure route-target import and export.
`VTEP1(config-vrf)#exit`	Exit from VRF mode.
`VTEP1(config)#mac vrf VRF10`	Configure MAC VRF as VRF2.
`VTEP1(config-vrf)#rd 1.1.1.1:29`	Configure route distinguisher value.
`VTEP1(config-vrf)#route-target both 70.70.70.70:100`	Configure route-target import and export.
`VTEP1(config-vrf)#exit`	Exit from VRF mode.
`VTEP1(config)#nvo vxlan vtep-ip-global 1.1.1.1`	Enable VxLAN Source VTEP IPp address global configuration.
`VTEP1(config)#nvo vxlan id 10 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP1(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF1`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP1(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP1(config)#nvo vxlan id 20 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.

© 2026 IP Infusion Inc. Proprietary

`VTEP1(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF2`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP1(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP1(config)#nvo vxlan id 21 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP1(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF3`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP1(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP1(config)#nvo vxlan id 23 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP1(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF4`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP1(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP1(config)#nvo vxlan id 24 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP1(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF5`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP1(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP1(config)#nvo vxlan id 25 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP1(config-nvo)#VxLAN host-reachability-protocol evpn-bgp VRF6`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP1(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP1(config)#nvo VxLAN id 26 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP1(config-nvo)#VxLAN host-reachability-protocol evpn-bgp VRF7`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP1(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP1(config)#nvo VxLAN id 27 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP1(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF8`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP1(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP1(config)#nvo vxlan id 28 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP1(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF9`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP1(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP1(config)#nvo vxlan id 29 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.

© 2026 IP Infusion Inc. Proprietary

`VTEP1(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF10`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP1(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP1(config)#qos enable`	Enable QoS.
`VTEP1(config)#hostname VTEP1`	Configure system's network name as VTEP1
`VTEP1(config)#interface lo`	Enter loopback interface mode.
`VTEP1(config-if)#ip address 1.1.1.1/32 secondary`	Configure the secondary IP address of the- loopback interface
`VTEP1(config)#interface xe48`	Enter interface mode.
`VTEP1(config-if)#load-interval 30`	Configure load interval.
`VTEP1(config-if)#ip address 10.10.10.1/24`	Configure the IP address of the interface.
`VTEP1(config-if)#exit`	Exit from interface mode.
`VTEP1(config)#interface xe49`	Enter interface mode.
`VTEP1(config-if)#switchport`	Enter the switchport mode.
`VTEP1(config-if)#load-interval 30`	Configure load interval.
`VTEP1(config-if)#exit`	Exit from interface mode.
`VTEP1(config)#interface xe54`	Enter interface mode.
`VTEP1(config-if)#switchport`	Enter the switchport mode.
`VTEP1(config-if)#load-interval 30`	Configure load interval.
`VTEP1(config-if)#exit`	Exit from interface mode.
`VTEP1(config)#router ospf 100`	Configure router ospf process ID.
`VTEP1(config-router)#ospf router-id 1.1.1.1`	Configure OSPF router id
`VTEP1(config-router)#bfd all-interfaces`	Enable BFD all interfaces
`VTEP1(config-router)#network 1.1.1.1/32 area 0.0.0.0`	Configure network and area as 0
`VTEP1(config-router)#network 10.10.10.0/24 area 0.0.0.0`	Configure network and area as 0
`VTEP1(config-router)#exit`	Exit from router ospf mode
`VTEP1(config)#router bgp 500`	Configure router bgp AS number
`VTEP1(config-router)#bgp router-id 1.1.1.1`	Configure BGP router ID.
`VTEP1(config-router)#neighbor 2.2.2.2 remote-as 500`	Configure a neighbor router and Peer AS Specify AS number of BGP neighbor.
`VTEP1(config-router)#neighbor 2.2.2.2 update-source lo`	Configure a neighbor router and Source of routing updates as loopbacl
`VTEP1(config-router)#neighbor 2.2.2.2 advertisement-interval 0`	Configure a neighbor router and minimum interval between sending BGP routing updates
`VTEP1(config-router)#address-family ipv4 unicast`	Enter Address Family command mode

`VTEP1(config-router-af)#network 1.1.1.1/32`	Configure a network to announce via BGP
`VTEP1(config-router-af)#neighbor 2.2.2.2 activate`	Activate the neighbor
`VTEP1(config-router-af)#exit-address-family`	Exit from address family mode
`VTEP1(config-router)#address-family l2vpn evpn`	Enter Address Family with l2vpn evpn Identifier
`VTEP1(config-router-af)#neighbor 2.2.2.2 activate`	Activate the neighbor
`VTEP1(config-router-af)#exit-address-family`	Exit from address family mode
`VTEP1(config-router)#exit`	Exit from router bgp mode
`VTEP1(config)#monitor session 1`	Configure Ethernet SPAN session with preferences
`VTEP1(config-monitor)#source interface xe49 rx`	Configure source interface as Ingress
`VTEP1(config-monitor)#destination interface xe54`	Configure destination interface.
`VTEP1(config-monitor)#10 filter vlan 2-6`	Configure sequence number with filter option and specify the vlan ranges.
`VTEP1(config-monitor)#no shut`	Unshut a monitor session.
`VTEP1(config-monitor)#exit`	Exit from monitor session.
`VTEP1(config)#nvo vxlan max-cache-disable 2500`	Configure vxlan Max number of ARP/ND cache disable allowed for port-vlan
`VTEP1(config)#nvo vxlan access-if port-vlan xe49 2`	Configure VxLAN access-if single tagged interface name with VLAN id
`VTEP1(config-nvo-acc-if)#map vnid 22`	Map access port attribute with VxLAN Identifier.
`VTEP1(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP1(config)#nvo vxlan access-if port-vlan xe49 3`	Configure VxLAN access-if single tagged interface name with VLAN id
`VTEP1(config-nvo-acc-if)#map vnid 23`	Map access port attribute with VxLAN Identifier.
`VTEP1(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP1(config)#nvo vxlan access-if port-vlan xe49 4`	Configure VxLAN access-if single tagged interface name with VLAN id
`VTEP1(config-nvo-acc-if)#map vnid 24`	Map access port attribute with VxLAN Identifier.
`VTEP1(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP1(config)#nvo vxlan access-if port-vlan xe49 5`	Configure VxLAN access-if single tagged interface name with VLAN id
`VTEP1(config-nvo-acc-if)#map vnid 25`	Map access port attribute with VxLAN Identifier.
`VTEP1(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP1(config)#nvo vxlan access-if port-vlan xe49 6`	Configure VxLAN access-if single tagged interface name with VLAN id
`VTEP1(config-nvo-acc-if)#map vnid 26`	Map access port attribute with VxLAN Identifier.

© 2026 IP Infusion Inc. Proprietary

`VTEP1(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP1(config)#nvo vxlan access-if port-vlan xe49 7`	Configure VxLAN access-if single tagged interface name with VLAN id
`VTEP1(config-nvo-acc-if)#map vnid 27`	Map access port attribute with VxLAN Identifier.
`VTEP1(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP1(config)#nvo vxlan access-if port-vlan xe49 8`	Configure VxLAN access-if single tagged interface name with VLAN id
`VTEP1(config-nvo-acc-if)#map vnid 28`	Map access port attribute with VxLAN Identifier.
`VTEP1(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP1(config)#nvo vxlan access-if port-vlan xe49 9`	Configure VxLAN access-if single tagged interface name with VLAN id
`VTEP1(config-nvo-acc-if)#map vnid 29`	Map access port attribute with VxLAN Identifier.
`VTEP1(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP1(config)#nvo vxlan access-if port-vlan xe49 10`	Configure VxLAN access-if single tagged interface name with VLAN id.
`VTEP1(config-nvo-acc-if)#map vnid 10`	Map access port attribute with VxLAN Identifier.
`VTEP1(config)#nvo vxlan access-if port-vlan xe49 11`	Configure VxLAN access-if single tagged interface name with VLAN id.
`VTEP1(config-nvo-acc-if)#map vnid 21`	Map access port attribute with VxLAN Identifier.
`VTEP1(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP1(config)#nvo vxlan access-if port-vlan xe49 12`	Configure VxLAN access-if single tagged interface name with VLAN id.
`VTEP1(config-nvo-acc-if)#map vnid 20`	Map access port attribute with VxLAN Identifier.
`VTEP1(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP1(config)#commit`	Commit the candidate configuration to the running configuration.

VTEP2

`VTEP2#configure terminal`	Enter configure mode.
`VTEP2(config)#hardware-profile filter ingress-mirror enable`	Enable hardware profile igress mirror
`VTEP2(config)#nvo vxlan enable`	Enable vxlan
`VTEP2(config)#evpn esi hold-time 60`	Config esi hold timer
`VTEP2(config)#evpn vxlan multihoming enable`	Enable vxlan multihoming
`VTEP2(config)#mac vrf VRF1`	Configure mac vrf as VRF1
`VTEP2(config-vrf)#rd 2.2.2.2:11`	Configure route distinguisher value.
`VTEP2(config-vrf)#route-target both 9.9.9.9:100`	Configure route-target import and export
`VTEP2(config-vrf)#exit`	Exit from vrf mode

© 2026 IP Infusion Inc. Proprietary

`VTEP2(config)#mac vrf VRF2`	Configure mac vrf as VRF2
`VTEP2(config-vrf)#rd 2.2.2.2:21`	Configure route distinguisher value.
`VTEP2(config-vrf)#route-target both 90.90.90.90:100`	Configure route-target import and export
`VTEP2(config-vrf)#exit`	Exit from vrf mode
`VTEP2(config)#mac vrf VRF3`	Configure mac vrf as VRF3
`VTEP2(config-vrf)#rd 2.2.2.2:22`	Configure route distinguisher value.
`VTEP2(config-vrf)#route-target both 90.90.90.90:101`	Configure route-target import and export
`VTEP2(config-vrf)#exit`	Exit from vrf mode
`VTEP2(config)#mac vrf VRF4`	Configure mac vrf as VRF4
`VTEP2(config-vrf)#rd 2.2.2.2:23`	Configure route distinguisher value.
`VTEP2(config-vrf)#route-target both 10.10.10.10:100`	Configure route-target import and export
`VTEP2(config-vrf)#exit`	Exit from vrf mode
`VTEP2(config)#mac vrf VRF5`	Configure mac vrf as VRF5
`VTEP2(config-vrf)#rd 2.2.2.2:24`	Configure route distinguisher value.
`VTEP2(config-vrf)#route-target both 20.20.20.20:100`	Configure route-target import and export
`VTEP2(config-vrf)#exit`	Exit from vrf mode
`VTEP2(config)#mac vrf VRF6`	Configure mac vrf as VRF6
`VTEP2(config-vrf)#rd 2.2.2.2:25`	Configure route distinguisher value.
`VTEP2(config-vrf)#route-target both 30.30.30.30:100`	Configure route-target import and export
`VTEP2(config-vrf)#exit`	Exit from vrf mode
`VTEP2(config)#mac vrf VRF7`	Configure mac vrf as VRF7
`VTEP2(config-vrf)#rd 2.2.2.2:26`	Configure route distinguisher value.
`VTEP2(config-vrf)#route-target both 40.40.40.40:100`	Configure route-target import and export
`VTEP2(config-vrf)#exit`	Exit from vrf mode
`VTEP2(config)#mac vrf VRF8`	Configure mac vrf as VRF8
`VTEP2(config-vrf)#rd 2.2.2.2:27`	Configure route distinguisher value.
`VTEP2(config-vrf)#route-target both 50.50.50.50:100`	Configure route-target import and export
`VTEP2(config-vrf)#exi` t	Exit from vrf mode
`VTEP2(config)#mac vrf VRF9`	Configure mac vrf as VRF9
`VTEP2(config-vrf)#rd 2.2.2.2:28`	Configure route distinguisher value.
`VTEP2(config-vrf)#route-target both 60.60.60.60:100`	Configure route-target import and export

`VTEP2(config-vrf)#exit`	Exit from vrf mode
`VTEP2(config)#mac vrf VRF10`	Configure mac vrf as VRF10
`VTEP2(config-vrf)#rd 2.2.2.2:29`	Configure route distinguisher value.
`VTEP2(config-vrf)#route-target both 70.70.70.70:100`	Configure route-target import and export
`VTEP2(config-vrf)#exit`	Exit from vrf mode
`VTEP2(config)#nvo vxlan vtep-ip-global 2.2.2.2`	Enable vxlan Source Vtep Ip address global configuration
`VTEP2(config)#nvo vxlan id 10 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF1`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP2(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP2(config)#nvo vxlan id 20 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF2`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP2(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP2(config)#nvo vxlan id 21 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF3`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP2(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP2(config)#nvo vxlan id 22 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF3`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP2(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP2(config)#nvo vxlan id 23 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF4`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP2(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP2(config)#nvo vxlan id 24 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF5`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP2(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP2(config)#nvo vxlan id 25 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.

© 2026 IP Infusion Inc. Proprietary

`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF6`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP2(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP2(config)#nvo vxlan id 26 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF7`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP2(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP2(config)#nvo vxlan id 27 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF8`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP2(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP2(config)#nvo vxlan id 28 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF9`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP2(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP2(config)#nvo vxlan id 29 ingress-replication`	Enable VxLAN Network Identifier Head End Replication tenant type.
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF10`	Host reachability protocol multiprotocol BGP VRF to carry EVPN routes.
`VTEP2(config-nvo)#exit`	Exit from the VxLAN mode.
`VTEP2(config)#qos enable`	Enable QoS.
`VTEP2(config)#hostname VTEP2`	Configure system's network name as VTEP2.
`VTEP2(config)#interface lo`	Enter loopback interface mode.
`VTEP2(config-if)#ip address 2.2.2.2/32 secondary`	Configure the secondary IP address of the loopback interface.
`VTEP2(config-if)#exit`	Exit from interface mode.
`VTEP2(config)#interface xe47`	Enter interface mode.
`VTEP2(config-if)#switchport`	Enter the switchport mode.
`VTEP2(config-if)#load-interval 30`	Configure load interval.
`VTEP2(config-if)#exit`	Exit from interface mode.
`VTEP2(config)#interface xe48`	Enter interface mode.
`VTEP2(config-if)#ip address 30.30.30.1/24`	Configure the IP address of the interface.
`VTEP2(config-if)#exit`	Enter interface mode.
`VTEP2(config)#interface xe57`	Enter interface mode.
`VTEP2(config-if)#switchport`	Enter the switchport mode.

© 2026 IP Infusion Inc. Proprietary

`VTEP2(config-if)#load-interval 30`	Configure load interval.
`VTEP2(config-if)#exit`	Exit from interface mode.
`VTEP2(config)#router ospf 100`	Configure router ospf process ID.
`VTEP2(config-router)#ospf router-id 2.2.2.2`	Configure OSPF router ID.
`VTEP2(config-router)#bfd all-interfaces`	Enable BFD all interfaces.
`VTEP2(config-router)#network 2.2.2.2/32 area 0.0.0.0`	Configure network and area as 0.
`VTEP2(config-router)#network 30.30.30.0/24 area 0.0.0.0`	Configure network and area as 0.
`VTEP2(config-router)#exit`	Exit from router OSPF mode.
`VTEP2(config)#router bgp 500`	Configure router BGP AS number.
`VTEP2(config-router)#bgp router-id 2.2.2.2`	Configure BGP router ID.
`VTEP2(config-router)#neighbor 1.1.1.1 remote-as 500`	Configure a neighbor router and Peer AS Specify AS number of BGP neighbor.
`VTEP2(config-router)#neighbor 1.1.1.1 update-source lo`	Configure a neighbor router and Source of routing updates as loopback.
`VTEP2(config-router)#neighbor 1.1.1.1 advertisement-interval 0`	Configure a neighbor router and minimum interval between sending BGP routing updates.
`VTEP2(config-router)#address-family ipv4 unicast`	Enter Address Family command mode.
`VTEP2(config-router-af)#network 2.2.2.2/32`	Configure a network to announce via BGP.
`VTEP2(config-router-af)#neighbor 1.1.1.1 activate`	Activate the neighbor.
`VTEP2(config-router-af)#exit-address-family`	Exit from address family mode.
`VTEP2(config-router)#address-family l2vpn evpn`	Enter Address Family with l2vpn evpn Identifier.
`VTEP2(config-router-af)#neighbor 1.1.1.1 activate`	Activate the neighbor.
`VTEP2(config-router-af)#exit-address-family`	Exit from address family mode.
`VTEP2(config-router)#exit`	Exit from router bgp mode.
`VTEP2(config)#nvo vxlan max-cache-disable 2500`	Configure vxlan Max number of ARP/ND cache disable allowed for port-vlan.
`VTEP2(config)#nvo vxlan access-if port-vlan xe47 2`	Configure VxLAN access-if single tagged interface name with VLAN id.
`VTEP2(config-nvo-acc-if)#map vnid 22`	Map access port attribute with VxLAN Identifier.
`VTEP2(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP2(config)#nvo vxlan access-if port-vlan xe47 3`	Configure VxLAN access-if single tagged interface name with VLAN id.
`VTEP2(config-nvo-acc-if)#map vnid 23`	Map access port attribute with VxLAN Identifier.
`VTEP2(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP2(config)#nvo vxlan access-if port-vlan`	Configure VxLAN access-if single tagged interface name with

© 2026 IP Infusion Inc. Proprietary

`xe47 4`	VLAN id.
`VTEP2(config-nvo-acc-if)#map vnid 24`	Map access port attribute with VxLAN Identifier.
`VTEP2(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP2(config)#nvo vxlan access-if port-vlan xe47 5`	Configure VxLAN access-if single tagged interface name with VLAN id.
`VTEP2(config-nvo-acc-if)#map vnid 25`	Map access port attribute with VxLAN Identifier.
`VTEP2(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP2(config)#nvo vxlan access-if port-vlan xe47 6`	Configure VxLAN access-if single tagged interface name with VLAN id.
`VTEP2(config-nvo-acc-if)#map vnid 26`	Map access port attribute with VxLAN Identifier.
`VTEP2(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP2(config)#nvo vxlan access-if port-vlan xe47 7`	Configure VxLAN access-if single tagged interface name with VLAN id.
`VTEP2(config-nvo-acc-if)#map vnid 27`	Map access port attribute with VxLAN Identifier.
`VTEP2(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP2(config)#nvo vxlan access-if port-vlan xe47 8`	Configure VxLAN access-if single tagged interface name with VLAN id.
`VTEP2(config-nvo-acc-if)#map vnid 28`	Map access port attribute with VxLAN Identifier.
`VTEP2(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP2(config)#nvo vxlan access-if port-vlan xe47 9`	Configure VxLAN access-if single tagged interface name with VLAN id.
`VTEP2(config-nvo-acc-if)#map vnid 29`	Map access port attribute with VxLAN Identifier.
`VTEP2(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP2(config)#nvo vxlan access-if port-vlan xe47 10`	Configure VxLAN access-if single tagged interface name with VLAN id.
`VTEP2(config-nvo-acc-if)#map vnid 10`	Map access port attribute with VxLAN Identifier.
`VTEP2(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP2(config)#nvo vxlan access-if port-vlan xe47 11`	Configure VxLAN access-if single tagged interface name with VLAN id
`VTEP2(config-nvo-acc-if)#map vnid 21`	Map access port attribute with VxLAN Identifier.
`VTEP2(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP2(config)#nvo vxlan access-if port-vlan xe47 12`	Configure VxLAN access-if single tagged interface name with VLAN id
`VTEP2(config-nvo-acc-if)#map vnid 20`	Map access port attribute with VxLAN Identifier.
`VTEP2(config-nvo-acc-if)#exit`	Exit from access-if mode.
`VTEP2(config)#commit`	Commit the candidate configuration to the running configuration.

Validation

Verify OSPF neighbors

```
VTEP1#show ip ospf  neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface           Instance ID
11.11.11.11       1   Full/DR         00:00:29    10.10.10.2      xe48                    0
VTEP1#
```

Checking the IP Routes

```
VTEP1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            1.1.1.1/32 is directly connected, lo, 01:21:26
O            2.2.2.2/32 [110/3] via 10.10.10.2, xe48, 01:15:25
C            10.10.10.0/24 is directly connected, xe48, 01:16:11
O            11.11.11.11/32 [110/2] via 10.10.10.2, xe48, 01:15:25
C            20.20.20.0/24 is directly connected, xe52, 01:20:42
O            30.30.30.0/24 [110/2] via 10.10.10.2, xe48, 01:15:25
C            127.0.0.0/8 is directly connected, lo, 01:21:26

Gateway of last resort is not set
VTEP1#
VTEP1#
VTEP1
```

Verify the BGP neighbors

```
VTEP1#show ip bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 500, local AS 500, internal link, peer index: 12
  BGP version 4, local router ID 1.1.1.1, remote router ID 2.2.2.2
  BGP state = Established, up for 01:15:26
  Last read 00:00:18, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family L2VPN EVPN: advertised and received
  Received 527 messages, 0 notifications, 0 in queue
  Sent 502 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 0 seconds
  Update source is lo

For address family: IPv4 Unicast  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  AIGP is enabled
  Community attribute sent to this neighbor (both)
  Large Community attribute sent to this neighbor
  1 accepted prefixes
  1 announced prefixes


For address family: L2VPN EVPN  BGP table version 96, neighbor version 95
```

```
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)

.skipping 1 line
  31 accepted prefixes
  Accepted AD:0 MACIP:20 MCAST:11 ESI:0 PREFIX:0
  21 announced prefixes

Connections established 1; dropped 0
Local host: 1.1.1.1, Local port: 179
Foreign host: 2.2.2.2, Foreign port: 38227
TCP MSS: (0), Advertise TCP MSS: (1460), Send TCP MSS: (1460),  Receive TCP MSS: (1460)
Sock FD : (22)
Nexthop: 1.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

Verify the VxLAN access-if

```
VTEP1#show nvo vxlan access-if brief

                Inner                       Admin   Link
Interface  Vlan  vlan  Ifindex    Vnid      status  status
-----------------------------------------------------------
xe49       2     ---   0x7a120    22        up      up
xe49       3     ---   0x7a121    23        up      up
xe49       4     ---   0x7a122    24        up      up
xe49       5     ---   0x7a123    25        up      up
xe49       6     ---   0x7a124    26        up      up
xe49       7     ---   0x7a125    27        up      up
xe49       8     ---   0x7a126    28        up      up
xe49       9     ---   0x7a127    29        up      up
xe49       10    ---   0x7a128    10        up      up
xe49       11    ---   0x7a129    21        up      up
xe49       12    ---   0x7a12a    20        up      up

Total number of entries are 11

Refer sub-interface config for VLAN information.
```

Verify the VxLAN tunnel

```
VTEP1#
VTEP1#
VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status        Up/Down       Update
=========================================================================
1.1.1.1          2.2.2.2          Installed     01:15:37      01:15:37

Total number of entries are 1
VTEP1#
```

Verify the VxLAN

```
VTEP1#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface ESI                           VLAN      DF-Status Src-
Addr         Dst-Addr
```

```
_____________________________________________________________________________________________________________
_____________________________
10       ----         L2       NW   ----      ----                          ----      ----
      1.1.1.1          2.2.2.2
10       ----         --       AC   xe49      --- Single Homed Port ---     10        ----      ----
            ----
20       ----         L2       NW   ----      ----                          ----      ----
      1.1.1.1          2.2.2.2
20       ----         --       AC   xe49      --- Single Homed Port ---     12        ----      ----
            ----
21       ----         L2       NW   ----      ----                          ----      ----
      1.1.1.1          2.2.2.2
21       ----         --       AC   xe49      --- Single Homed Port ---     11        ----      ----
            ----
22       ----         L2       NW   ----      ----                          ----      ----
      1.1.1.1          2.2.2.2
22       ----         --       AC   xe49      --- Single Homed Port ---     2         ----      ----
            ----
23       ----         L2       NW   ----      ----                          ----      ----
      1.1.1.1          2.2.2.2
23       ----         --       AC   xe49      --- Single Homed Port ---     3         ----      ----
            ----
24       ----         L2       NW   ----      ----                          ----      ----
      1.1.1.1          2.2.2.2
24       ----         --       AC   xe49      --- Single Homed Port ---     4         ----      ----
            ----
25       ----         L2       NW   ----      ----                          ----      ----
      1.1.1.1          2.2.2.2
25       ----         --       AC   xe49      --- Single Homed Port ---     5         ----      ----
            ----
26       ----         L2       NW   ----      ----                          ----      ----
      1.1.1.1          2.2.2.2
26       ----         --       AC   xe49      --- Single Homed Port ---     6         ----      ----
            ----
27       ----         L2       NW   ----      ----                          ----      ----
      1.1.1.1          2.2.2.2
27       ----         --       AC   xe49      --- Single Homed Port ---     7         ----      ----
            ----
28       ----         L2       NW   ----      ----                          ----      ----
      1.1.1.1          2.2.2.2
28       ----         --       AC   xe49      --- Single Homed Port ---     8         ----      ----
            ----
29       ----         L2       NW   ----      ----                          ----      ----
      1.1.1.1          2.2.2.2
29       ----         --       AC   xe49      --- Single Homed Port ---     9         ----      ----
            ----

Total number of entries are 22
```

Note: Refer sub-interface config for VLAN information.

Verify the interface counters

```
VTEP1#

VTEP1#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe48                 42.73          30012         14.25          10011
 xe49                 41.60          40625         10.24          10000
 xe54                 0.00           0             20.80          20312
VTEP1#
```

Validation for Port Mirroring

Verify the monitor

```
VTEP1#show monitor
Session  State        Reason                  Description
-------  -----------  ----------------------  --------------------------------
1        up           The session is up
VTEP1#

Verify the monitor session

VTEP1#show monitor session 1
   session 1
---------------
type              : local
state             : up
source intf       :
    tx            :
    rx            : xe49
    both          :
source VLANs      :
    rx            :
destination ports : xe54
filter count      : 1

Legend: f = forwarding enabled, l = learning enabled

VTEP1#

VTEP1#show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
    tx            :
    rx            : xe49
    both          :
destination ports : xe54
filter count      : 1

VTEP1#

VTEP1#show monitor session 1 filter
   session 1
---------------
filter count      : 1

  ---------------
  match set 1
  ---------------
Sequence number : 10 vlan : 2-6

VTEP1#

END
```

Revised CLI Commands

hardware-profile filter (XGS)

The existing hardware-profile filter CLI syntax is updated as follows:

hardware-profile filter port-isolation (ingress-ipv4|ingress-ipv6|egress-ipv6|ingress-arp|bfd-group) (enable|disable)

to

hardware-profile filter port-isolation (ingress-mirror|ingress-ipv4|ingress-ipv6|egress-ipv6|ingress-arp|bfd-group) (enable|disable)

Refer to hardware-profile filter (XGS) (page 281) CLI section for more details.

Use the new filter ingress-mirror profile for port mirroring when monitor session is installed with filters. when the specified filter profile is not enabled, port mirror uses default L2 group.

filter

The existing filter CLI syntax is updated as follows:

filter {vlan <2-4094> | cos <0-7> ...

(<1-268435453>/<1-4294967294> |) filter {vlan <2-4094>| cos <0-7> | dest-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX XXXX.XXXX.XXXX) | src-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX XXXX.XXXX.XXXX) | frame-type (ETHTYPE | arp (req | resp|) (sender-ip A.B.C.D|) (target-ip A.B.C.D|) | ipv4 (src-ip (A.B.C.D | A.B.C.D/M)|) (dest-ip (A.B.C.D | A.B.C.D/M)|) | ipv6 (src-ip X:X::X:X/M |) (dest-ip X:X::X:X/M |))}

to

(<1-268435453>/<1-4294967294> |) filter {vlan VLAN_RANGE|inner-vlan VLAN_RANGE| cos <0-7> | dest-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX XXXX.XXXX.XXXX) | src-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX XXXX.XXXX.XXXX) | frame-type (ETHTYPE | arp (req | resp|) (sender-ip A.B.C.D|) (target-ip A.B.C.D|) | ipv4 (src-ip (A.B.C.D | A.B.C.D/M)|) (dest-ip (A.B.C.D | A.B.C.D/M)|) | ipv6 (src-ip X:X::X:X/M |) (dest-ip X:X::X:X/M |))}

Refer to filter CLI section for more details.

Abbreviations

Acronym	Expansion
ACL	Access Control List
MAC	Media Access Control
SPAN	Switch Port Analyzer
VLAN	Virtual LAN
VxLAN	Virtual eXtensible Local Area Network

© 2026 IP Infusion Inc. Proprietary

Traffic Mirroring using ERSPAN

Overview

Encapsulated Remote Switched Port Analyzer (ERSPAN) is a function used for monitoring network traffic. Using ERSPAN, you can mirror traffic from one or more ports or VLANs on a network switch and send the mirrored traffic to a remote monitoring device for analysis.

ERSPAN encapsulates mirrored traffic with Generic Routing Encapsulation (GRE) and, in addition, ERSPAN headers to send over an IP network.

Traffic mirroring protocols such as Switched Port Analyzer (SPAN) and Remote Switched Port Analyzer (RSPAN) in OcNOS allow traffic analysis within the same domain. ERSPAN aims to overcome this limitation by routing the traffic to any destination on the network.

Feature Characteristics

The main characteristics of ERSPAN are as follows:

- Transports mirrored traffic from the source to the destination over Layer 3 IP network.
- Monitors ingress, egress, or both ingress and egress traffic.
- Sends mirrored traffic to remote monitoring device for analysis without being restricted by Layer 2 boundaries.
- Supports filters on ingress traffic providing capability to filter the traffic to be mirrored.
- Supports Type 1 and Type 3 ERSPAN, with Type 1 as the default.

Supported Hardware

- XGS platforms - Trident 3 (TR3), Trident 4 (TR4), Tomahawk (TH/TH2) and Tomahawk 4 (TH4).

Supported scenarios

Trident 3

ERSPAN type	ERSPAN over IPv4 Ingress traffic	ERSPAN over IPv4 Egress traffic	ERSPAN over IPv6 Ingress traffic	ERSPAN over IPv6 Egress traffic
Type 1	Yes	Yes	Yes	No
Type 3	Yes	No	No	No

Trident 4

ERSPAN type	ERSPAN over IPv4 Ingress traffic	ERSPAN over IPv4 Egress traffic	ERSPAN over IPv6 Ingress traffic	ERSPAN over IPv6 Egress traffic
Type 1	Yes	Yes	Yes	Yes
Type 3	Yes	No	Yes	No

Tomahawk/Tomahawk 2

© 2026 IP Infusion Inc. Proprietary

ERSPAN type	ERSPAN over IPv4 Ingress traffic	ERSPAN over IPv4 Egress traffic	ERSPAN over IPv6 Ingress traffic	ERSPAN over IPv6 Egress traffic
Type 1	Yes	Yes	No	No
Type 3	No	No	No	No

Tomahawk 4

ERSPAN type	ERSPAN over IPv4 Ingress traffic	ERSPAN over IPv4 Egress traffic	ERSPAN over IPv6 Ingress traffic	ERSPAN over IPv6 Egress traffic
Type 1	Yes	Yes	Yes	Yes
Type 3	No	No	No	No

Prerequisites

Before configuration, ensure the IP address is available for:

- Destination of the ERSPAN tunnel.
- Origin of the ERSPAN tunnel.

Configuration

The following configuration enables a sender session to send packets to the destination over ERSPAN tunnels.

Topology

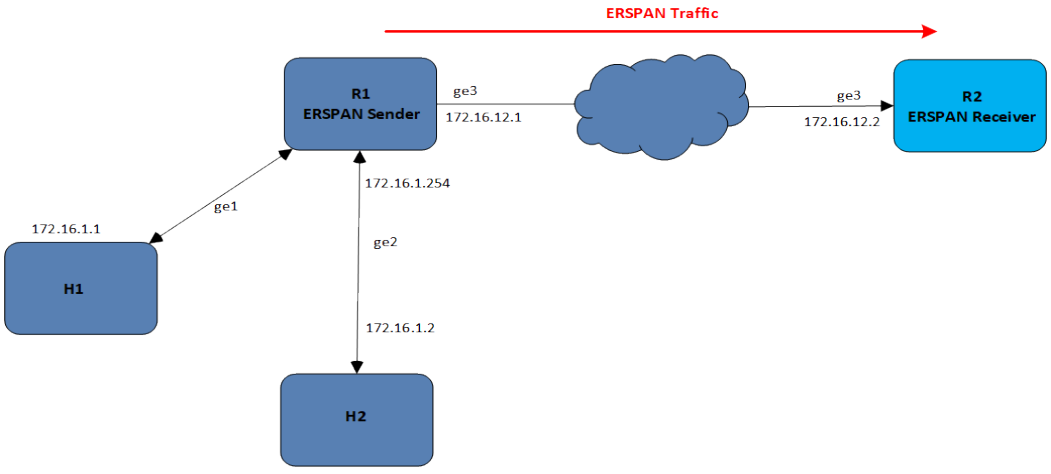
The topology shown here consists of Host 1, Host 2, a Sender node R1, and a Receiver node R2.

The sender node forwards ERSPAN traffic to the receiver node. An ERSPAN tunnel is created between R1 and R2 over interface ge3.

R1 collects the traffic received or sent over one or more interfaces (such as ge1 and/or ge2), mirrors the collected traffic, encapsulates the packets inside ERSPAN and sends them to the IP address on R2.

R2 is configured to receive ERSPAN encapsulated packets.

Figure 36. ERSPAN Topology



The configuration is done in two stages:

a. *Configure ERSPAN destination (page 285)*

b. *Configure ERSPAN sender session (page 286)* using the ERSPAN destination

Configure ERSPAN destination

1. Enter configure mode and set a name for the ERSPAN destination.

```
R1(config-router)#monitor destination erspan erspan_dest_1
R1(config-erspan-dst)#
```

2. Configure the destination IPv4/IPv6 where the ERSPAN packets will be forwarded.

```
R1(config-erspan-dst)#dest-ip 172.16.12.2
```

3. Set the origin IPv4/IPv6 of the ERSPAN tunnel.

```
R1(config-erspan-dst)#origin-ip 172.16.12.1
```

4. The below parameters are optional. If not specified, the default values are used for each parameter.

   - Set the VRF where the ERSPAN tunnel will be created. If not specified, value `default` will be used.

```
R1(config-erspan-dst)#vrf default
```

   - Set the TTL value to be used at the outer IP layer. If not specified, value 255 will be used.

```
R1(config-erspan-dst)#ttl 50
```

   - Set the DSCP value to be used at the outer IP layer. If not specified, value 0 will be used.

```
R1(config-erspan-dst)#dscp 50
```

   - Enable the packet truncation when mirroring to the ERSPAN destination. When this flag is set, the original packet is truncated to 192 bytes and then encapsulated in ERSPAN. By default, truncation is not enabled.

```
R1(config-erspan-dst)#enable-truncate
```

Note: Packet truncation is not supported on TH and TH2 platforms.

   - Set the ERSPAN tunnel to Type 1 or Type 3. If not specified, value 1 will be used.

```
R1(config-erspan-dst)#erspan-type 1
```

   - Set the ERSPAN ID to be used in the ERSPAN session. This is relevant for type 3 only. If not specified, value 0 is used.

```
R1(config-erspan-dst)#erspan-id 100
```

   - Set a Hardware ID value between 0 to 63. This parameter is relevant for type 3 only. If not specified, value 0 is used.

```
R1(config-erspan-dst)#hardware-id 45
```

   - Set a Switch ID value between 0 to 511. This parameter is relevant for type 3 only. If not specified, value 0 is used.

```
R1(config-erspan-dst)#switch-id 110
```

   - Commit the changes.

```
R1(config-erspan-dst)#commit
```

© 2026 IP Infusion Inc. Proprietary

Configure ERSPAN sender session

1. Enter configure mode and create a sender session with ID 1. Optionally, you can enter a description for the session (containing a maximum of 32 characters).

```
R1(config)#monitor session 1 type erspan-sender
R1(config-monitor)#description R1 ERSPAN sender
```

2. Configure the ERSPAN destination for the session using the name of the destination that has been created previously.

```
R1(config-monitor)#destination erspan erspan_dest_1
```

3. Optionally, add sources such as `source VLAN` and/or `source interface` to the sessions. For example, the command `source interface` configures the monitored source interface and the direction of the traffic to be monitored. If not specified, both ingress and egress traffic are monitored.

```
R1(config-monitor)#source interface ce51 rx
```

4. Enable the configured session on the interface.

```
no shut
```

Running Configuration

To verify the configuration and view the overall commands, use the `show running-config monitor` command.

```
R1#show running-config monitor
monitor destination erspan erspan_dest_1
  dest-ip 23.1.1.2
  vrf default
  origin-ip 69.69.69.69
  ttl 211
  dscp 50
  enable-truncate
  erspan-type 1
!
monitor session 1 type erspan-sender
 description R1 ERSPAN sender
 source interface ce51 rx
 destination erspan erspan_dest_1
 no shut
```

Validation

To verify the ERSPAN configuration, check the output of the show monitor session 1 command.

```
#show monitor session 1
session 1
---------------
description : R1 ERSPAN sender
type : ERSPAN Sender
state : up
source intf :
tx :
rx : ge1
both :
source VLANs :
rx :
destination ERSPAN: erspan_dest_1
ERSPAN Type : 1
Dest IP addr : 172.16.12.2
Origin IP addr: 172.16.12.1
Dest VRF : default
ERSPAN ID : 0
```

© 2026 IP Infusion Inc. Proprietary

```
DSCP : 50
TTL : 211
pkt truncate : Enabled
NextHop addr : 172.16.12.2
NextHop intf : ge3
filter count :
Legend: f = forwarding enabled, l = learning enabled
Sender#
```

CLI Commands

The ERSPAN feature introduces the following configuration commands.

destination erspn

Use this command to configure the ERSPAN destination for an ERSPAN sender session. The destination must be already created using the command `monitor destination erspan`.

Use `no` form of this command to remove the ERSPAN destination from the session.

Command Syntax

```
destination erspan NAME
no destination erspan
```

Parameters

NAME

ERSPAN destination name mentioned in the command `monitor destination erspan`.

Default

No default value is specified

Command Mode

ERSPAN destination mode

Applicability

This command was introduced in OcNOS version 6.6.0.

Example

The following sequence of commands is used to configure the ERSPAN destination.

```
(config)#monitor destination erspan erspan_dest_1
(config-erspan-dst)#dest-ip 172.16.12.2
(config-erspan-dst)#origin-ip 172.16.12.1
(config-erspan-dst)#exit
(config)#monitor session 1 type erspan-sender
(config-monitor)#destination erspan erspan_dest_1
(config-monitor)#no destination erspan
```

origin-ip

Use this command to set the origin IPv4/IPv6 of the ERSPAN tunnel.

Use `no` form of this command to unset the origin IPv4/IPv6 of the ERSPAN tunnel.

© 2026 IP Infusion Inc. Proprietary

Command Syntax

```
origin-ip A.B.C.D|X:X::X:X
no origin-ip
```

Parameters

A.B.C.D|X:X::X:X
Origin IPv4/IPv6 address of the ERSPAN tunnel

Default

Disabled

Command Mode

ERSPAN destination mode

Applicability

This command was introduced in OcNOS version 6.6.0.

Example

The following sequence of commands is used to set the origin IPv4/IPv6 of the ERSPAN tunnel.

```
(config)#monitor destination erspan erspan_dest_1
(config-erspan-dst)#origin-ip 172.16.12.1
(config-erspan-dst)#commit
(config-erspan-dst)#no origin-ip
(config-erspan-dst)#commit
```

destination-ip

Use this command to set the destination IPv4/IPv6 of the ERSPAN tunnel.

Use `no` form of this command to unset the destination IPv4/IPv6 of the ERSPAN tunnel.

Command Syntax

```
dest-ip A.B.C.D|X:X::X:X
no dest-ip
```

Parameters

A.B.C.D|X:X::X:X
Destination IPv4/IPv6 address of the ERSPAN tunnel

Default

Disabled

Command Mode

ERSPAN destination mode

Applicability

This command was introduced in OcNOS version 6.6.0.

© 2026 IP Infusion Inc. Proprietary

Example

The following sequence of commands is used to set the destination IPv4/IPv6 of the ERSPAN tunnel.

```
(config)#monitor destination erspan erspan_dest_1
(config-erspan-dst)#dest-ip 172.16.12.1
(config-erspan-dst)#commit

(config-erspan-dst)#no dest-ip
(config-erspan-dst)#commit
```

vrf

Use this command to set the VRF where the ERSPAN tunnel will be created.

Use `no` form of this command to reset the VRF to default.

Command Syntax

```
vrf VRF_NAME
no vrf
```

Parameters

VRF_NAME
VRF name where the ERSPAN tunnel will be created

Default

Default

Command Mode

ERSPAN destination mode

Applicability

This command was introduced in OcNOS version 6.6.0.

Example

The following sequence of commands is used to set the VRF where the ERSPAN tunnel will be created.

```
(config)#monitor destination erspan erspan_dest_1
(config-erspan-dst)#vrf custom_vrf_1
(config-erspan-dst)#commit

(config-erspan-dst)#no vrf
(config-erspan-dst)#commit
```

ttl

Use this command to set the Time To Live (TTL) value to use at the outer IP layer. This is an optional parameter that uses TTL value 255, if not specified.

Use `no` form of this command to reset the TTL value to 255.

Command Syntax

```
ttl <1-255>
```

```
no ttl
```

Parameters

<1-255>
TTL value to be used

Default

Value 255

Command Mode

ERSPAN destination mode

Applicability

This command was introduced in OcNOS version 6.6.0.

Example

The following sequence of commands is used to set the TTL value to use at the outer IP layer.

```
(config)#monitor destination erspan erspan_dest_1
(config-erspan-dst)#ttl 25
(config-erspan-dst)#commit

(config-erspan-dst)#no ttl
(config-erspan-dst)#commit
```

dscp

Use this command to set the Differentiated Services Code Point (DSCP) value to use at the outer IP layer. This is an optional parameter that uses DSCP value 0, if not specified.

Use `no` form of this command to reset the DSCP value to 0.

Command Syntax

```
dscp <0-63>
no dscp
```

Parameters

<0-63>
DSCP value to be used

Default

Value 0

Command Mode

ERSPAN destination mode

Applicability

This command was introduced in OcNOS version 6.6.0.

© 2026 IP Infusion Inc. Proprietary

Example

The following sequence of commands is used to set the DSCP value to use at the outer IP layer.

```
(config)#monitor destination erspan erspan_dest_1
(config-erspan-dst)#dscp 42
(config-erspan-dst)#commit

(config-erspan-dst)#no dscp
(config-erspan-dst)#commit
```

enable-truncate

Use this command to enable packet truncation when mirroring to the ERSPAN destination. When this flag is set, the original packet is truncated to 192 bytes and then encapsulated in ERSPAN.

Use `no` form of this command to disable packet truncate.

Command Syntax

```
enable-truncate
no enable-truncate
```

Parameters

None

Default

Disabled

Command Mode

ERSPAN destination mode

Applicability

This command was introduced in OcNOS version 6.6.0.

Example

The following sequence of commands is used to enable the packet truncation.

```
(config)#monitor destination erspan erspan_dest_1
(config-erspan-dst)#enable-truncate
(config-erspan-dst)#commit

(config-erspan-dst)#no enable-truncate
(config-erspan-dst)#commit
```

erspan-type

Use this command to set the ERSPAN tunnel to Type 1 or Type 3. Note that ERSPAN Type 2 is not supported on XGS TR3 and TH/TH2 boards.

Use `no` form of this command to reset the ERSPAN type to the default value.

Command Syntax

```
erspan-type (1|3)
```

© 2026 IP Infusion Inc. Proprietary

```
no erspan-type
```

Parameters

1
Use ERSPAN Type 1

3
Use ERSPAN Type 3

Default

Type 1

Command Mode

ERSPAN destination mode

Applicability

This command was introduced in OcNOS version 6.6.0.

Example

The following sequence of commands is used to set the ERSPAN tunnel.

```
(config)#monitor destination erspan erspan_dest_1
(config-erspan-dst)#erspan-type 3
(config-erspan-dst)#commit

(config-erspan-dst)#no erspan-type
(config-erspan-dst)#commit
```

erspn-id

Use this command to set the ERSPAN ID to be used in the ERSPAN session. This is only relevant for ERSPAN Type 3. This is an optional parameter and the ERSPAN ID 0 is used, if not specified.

Use `no` form of this command to reset the value to 0.

Command Syntax

```
erspan-id (1-1023)
no erspan-id
```

Parameters

<1-1023>
ERSPAN ID to be used

Default

Value 0

Command Mode

ERSPAN destination mode

Applicability

This command was introduced in OcNOS version 6.6.0.

Example

The following sequence of commands is used to set the ERSPAN ID.

```
(config)#monitor destination erspan erspan_dest_1
(config-erspan-dst)#erspan-id 33
(config-erspan-dst)#commit

(config-erspan-dst)#no erspan-id
(config-erspan-dst)#commit
```

hardware-id

Use this command to set the Hardware ID to be used. This is only relevant for ERSPAN Type 3.

Use `no` form of this command to reset the value to 0.

Command Syntax

```
hardware-id (0-63)
no hardware-id
```

Parameters

<1-63>
Hardware ID to be used

Default

Value 0

Command Mode

ERSPAN destination mode

Applicability

This command was introduced in OcNOS version 6.6.0.

Example

The following sequence of commands is used to set the Hardware ID.

```
(config)#monitor destination erspan erspan_dest_1
(config-erspan-dst)#hardware-id 12
(config-erspan-dst)#commit

(config-erspan-dst)#no hardware-id
(config-erspan-dst)#commit
```

switch-id

Use this command to set value for the Switch ID to be used. This is only relevant for ERSPAN Type 3.

Use `no` form of this command to reset the value to 0.

© 2026 IP Infusion Inc. Proprietary

Command Syntax

```
switch-id (0-1023)
no switch-id
```

Parameters

<1-1023>
Switch ID to be used

Default

Value 0

Command Mode

ERSPAN destination mode

Applicability

This command was introduced in OcNOS version 6.6.0.

Example

The following sequence of commands is used to set the Switch ID.

```
(config)#monitor destination erspan erspan_dest_1
(config-erspan-dst)#switch-id 112
(config-erspan-dst)#commit

(config-erspan-dst)#no switch-id
(config-erspan-dst)#commit
```

Revised Command

The below commands have been revised for ERSPAN. For more details, refer to the *Traffic Mirroring Commands (page 542)* section.

- Command syntax in monitor session (page 547)
- Example section in show monitor session (page 554)

Glossary

The following table provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
Switched Port Analyzer (SPAN)	A protocol that monitors the traffic on source port and sends a copy of the traffic to a destination port.
Remote Switched Port Analyzer (RSPAN)	A protocol that monitors the traffic distributed over multiple switches from the source ports.
Time to Live (TTL)	A limit on how long a piece of information can exist before it should be discarded.

© 2026 IP Infusion Inc. Proprietary

Differentiated Services Code Point (DSCP)	A six-bit field in an IP header that enables allocation of resources on a per-packet basis.
Virtual Routing and Forwarding (VRF)	A technology that allows multiple data structures to co-exist within the same router at the same time.

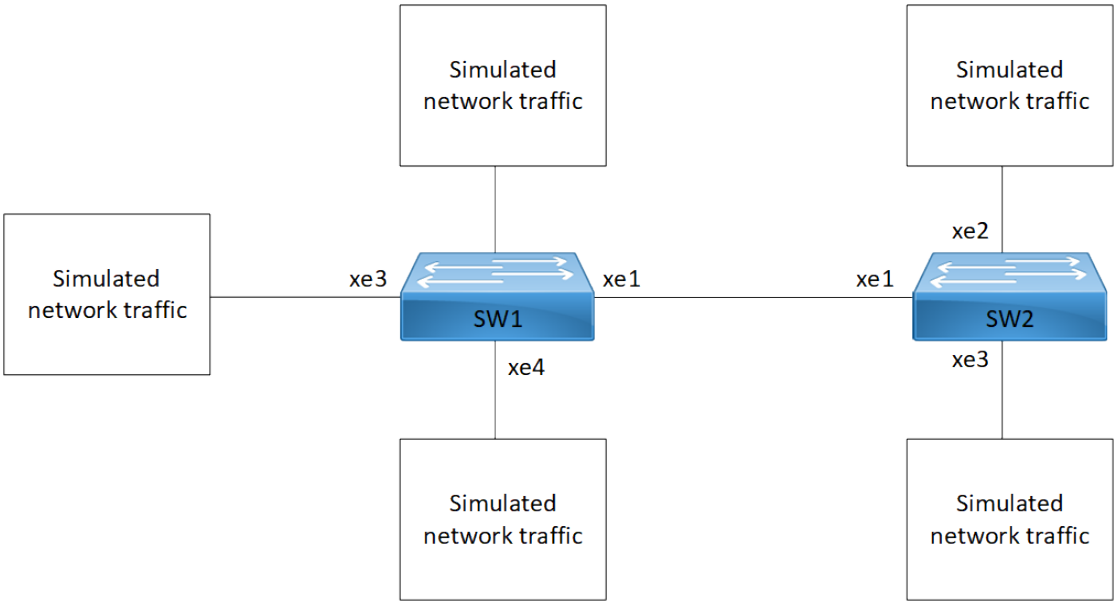
© 2026 IP Infusion Inc. Proprietary

Private VLAN Configuration

A private VLANs (PVLAN) splits a primary VLAN domain into multiple isolated broadcast sub-domains. PVLAN, also known as port isolation, is a technique where a VLAN contains switch ports that are restricted such that they can only communicate with a given uplink.

Topology

Figure 37. PVLAN configuration



Configure PVLAN Trunk and Promiscuous Trunk Port

SW1

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol ieee vlan- bridge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 10 bridge 1 state enable`	Create VLAN 10
`SW1(config-vlan)#vlan 20 bridge 1 state enable`	Create VLAN 20
`SW1(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100
`SW1(config-vlan)#private-vlan 10 isolated bridge 1`	Configure VLAN 10 as isolated VLAN
`SW1(config-vlan)#private-vlan 20 community bridge 1`	Configure VLAN 20 as community VLAN
`SW1(config-vlan)#private-vlan 100 primary bridge 1`	Configure VLAN 100 as primary VLAN
`SW1(config-vlan)#private-vlan 100 association add 10 bridge 1`	Associate secondary isolated VLAN 10 with primary VLAN 100

© 2026 IP Infusion Inc. Proprietary

`SW1(config-vlan)#private-vlan 100association add 20 bridge 1`	Associate secondary community VLAN 20 with primary VLAN 100
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface xe1`	Enter interface configuration mode for xe1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW1(config-if)#switchport trunk allowed vlan add 10,20,100`	Configure VLAN 10,20,100 (primary, secondary VLANs)
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe3`	Enter interface configuration mode for xe3
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW1(config-if)#switchport mode private-vlan promiscuous`	Configure the interface as promiscuous port for private-vlan
`SW1(config-if)#switchport trunk allowed vlan add 100`	Configure VLAN 100 (primary VLAN)
`SW1(config-if)#switchport private-vlan mapping 100 add 10`	Associate port with primary and secondary VLAN of private- vlan
`SW1(config-if)#switchport private-vlan mapping 100 add 20`	Associate port with primary and secondary VLAN of private- vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe4`	Enter interface configuration mode for xe4
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW1(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW1(config-if)#switchport access vlan 20`	Configure VLAN 20 (community VLAN)
`SW1(config-if)#switchport private-vlan host-association 100 add 20`	Associate port with primary and secondary VLAN of private- vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe2`	Enter interface configuration mode for xe2
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access

© 2026 IP Infusion Inc. Proprietary

`SW1(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW1(config-if)#switchport access vlan 10`	Configure VLAN 10 (isolated VLAN)
`SW1(config-if)#switchport private-vlan host-association 100 add 10`	Associate port with primary and secondary VLAN of private- vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#commit`	Commit the configure on the node.
`SW1(config)#exit`	Exit configuration mode

SW2

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol ieee vlan- bridge`	Create bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 10 bridge 1 state enable`	Create VLAN 10
`SW2(config-vlan)#vlan 20 bridge 1 state enable`	Create VLAN 20
`SW2(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100
`SW2(config-vlan)#private-vlan 10 isolated bridge 1`	Configure VLAN 10 as isolated VLAN
`SW2(config-vlan)#private-vlan 20 community bridge 1`	Configure VLAN 20 as community VLAN
`SW2(config-vlan)#private-vlan 100 primary bridge 1`	Configure VLAN 100 as primary VLAN
`SW1(config-vlan)#private-vlan 100 association add 10 bridge 1`	Associate secondary isolated VLAN 10 with primary VLAN 100
`SW1(config-vlan)#private-vlan 100 association add 20 bridge 1`	Associate secondary community VLAN 20 with primary VLAN 100
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface xe1`	Enter interface configuration mode for xe1
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW2(config-if)#switchport trunk allowed vlan add 10,20,100`	Configure VLAN 10,20,100 (primary, secondary VLANs)
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#interface xe2`	Enter interface configuration mode for xe2
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW2(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW2(config-if)#switchport access vlan 10`	Configure VLAN 10 (isolated VLAN)

© 2026 IP Infusion Inc. Proprietary

`SW2(config-if)#switchport private-vlan host-association 100 add 10`	Associate port with primary and secondary VLAN of private- vlan
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#interface xe3`	Enter interface configuration mode for xe3
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW2(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW2(config-if)#switchport access vlan 20`	Configure VLAN 20 (community VLAN)
`SW2(config-if)#switchport private-vlan host-association 100 add 20`	Associate port with primary and secondary VLAN of private- vlan
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#commit`	Commit the configure on the node.
`SW2(config)#exit`	Exit configuration mode

Validation

```
SW1#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      xe1,xe2,
     100              20         community      xe1,xe4,
SW1#
SW2#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      xe1,xe2,
     100              20         community      xe1,xe3,
SW2#
```

Configure PVLAN Trunk and Promiscuous Access Port

SW1

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 10 bridge 1 state enable`	Create VLAN 10
`SW1(config-vlan)#vlan 20 bridge 1 state enable`	Create VLAN 20
`SW1(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100
`SW1(config-vlan)#private-vlan 10 isolated bridge 1`	Configure VLAN 10 as isolated VLAN
`SW1(config-vlan)#private-vlan 20 community bridge 1`	Configure VLAN 20 as community VLAN
`SW1(config-vlan)#private-vlan 100 primary bridge 1`	Configure VLAN 100 as primary VLAN

© 2026 IP Infusion Inc. Proprietary

`SW1(config-vlan)#private-vlan 100 association add 10 bridge 1`	Associate secondary isolated VLAN 10 with primary VLAN 100
`SW1(config-vlan)#private-vlan 100 association add 20 bridge 1`	Associate secondary community VLAN 20 with primary VLAN 100
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface xe1`	Enter interface configuration mode for xe1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW1(config-if)#switchport trunk allowed vlan add 10,20,100`	Configure VLAN 10,20,100 (primary, secondary VLANs)
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe3`	Enter interface configuration mode for xe3
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW1(config-if)#switchport mode private-vlan promiscuous`	Configure the interface as promiscuous port for private-vlan
`SW1(config-if)#switchport access vlan 100`	Configure VLAN 100 (primary VLAN)
`SW1(config-if)#switchport private-vlan mapping 100 add 10`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#switchport private-vlan mapping 100 add 20`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe4`	Enter interface configuration mode for xe4
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW1(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW1(config-if)#switchport access vlan 20`	Configure VLAN 20 (community VLAN)
`SW1(config-if)#switchport private-vlan host-association 100 add 20`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe2`	Enter interface configuration mode for xe2
`SW1(config-if)#switchport`	Configure switchport

© 2026 IP Infusion Inc. Proprietary

`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW1(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW1(config-if)#switchport access vlan 10`	Configure VLAN 10 (isolated VLAN)
`SW1(config-if)#switchport private-vlan host-association 100 add 10`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#commit`	Commit the configure on the node.
`SW1(config)#exit`	Exit configuration mode

SW2

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 10 bridge 1 state enable`	Create VLAN 10
`SW2(config-vlan)#vlan 20 bridge 1 state enable`	Create VLAN 20
`SW2(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100
`SW2(config-vlan)#private-vlan 10 isolated bridge 1`	Configure VLAN 10 as isolated VLAN
`SW2(config-vlan)#private-vlan 20 community bridge 1`	Configure VLAN 20 as community VLAN
`SW2(config-vlan)#private-vlan 100 primary bridge 1`	Configure VLAN 100 as primary VLAN
`SW1(config-vlan)#private-vlan 100 association add 10 bridge 1`	Associate secondary isolated VLAN 10 with primary VLAN 100
`SW1(config-vlan)#private-vlan 100 association add 20 bridge 1`	Associate secondary community VLAN 20 with primary VLAN 100
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface xe1`	Enter interface configuration mode for xe1
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW2(config-if)#switchport trunk allowed vlan add 10,20,100`	Configure VLAN 10,20,100 (primary, secondary VLANs)
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#interface xe2`	Enter interface configuration mode for xe2
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode access`	Set the switching characteristics of this interface as

© 2026 IP Infusion Inc. Proprietary

	access
SW2(config-if)#switchport mode private-vlan host	Configure the interface as host port for private-vlan
SW2(config-if)#switchport access vlan 10	Configure VLAN 10 (isolated VLAN)
SW2(config-if)#switchport private-vlan host-association 100 add 10	Associate port with primary and secondary VLAN of private-vlan
SW2(config-if)#exit	Exit interface mode
SW2(config)#interface xe3	Enter interface configuration mode for xe3
SW2(config-if)#switchport	Configure switchport
SW2(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW2(config-if)#switchport mode access	Set the switching characteristics of this interface as access
SW2(config-if)#switchport mode private-vlan host	Configure the interface as host port for private-vlan
SW2(config-if)#switchport access vlan 20	Configure VLAN 20 (community VLAN)
SW2(config-if)#switchport private-vlan host-association 100 add 20	Associate port with primary and secondary VLAN of private-vlan
SW2(config-if)#exit	Exit interface mode
SW2(config)#commit	Commit the configure on the node.
SW2(config)#exit	Exit configuration mode

Validation

```
SW1#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      xe1,xe2,
     100              20         community      xe1,xe4,

SW2#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      xe1,xe2,
     100              20         community      xe1,xe3,
SW2#
```

Traffic Validation

Configure Host trunk and promiscuous trunk configurations on SW1 and SW2

1. Send untagged traffic from SW1 xe3 (promiscuous port), traffic should forward to interfaces xe1,xe2, and xe4. On SW2, traffic should receive from xe1 and forward through xe2 and xe3.

```
SW1#show interface counters rate mbps
+------------------+--------------+-------------+--------------+-------------+
|     Interface    |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+------------------+--------------+-------------+--------------+-------------+
 xe1                0.00           0             86.49          84462
 xe2                0.00           0             86.49          84462
 xe3                86.49          84462         0.00           0
 xe4                0.00           0             86.49          84462

SW2#show interface counters rate mbps
+------------------+--------------+-------------+--------------+-------------+
```

```
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1                 86.49          84462         0.00           0
 xe2                 0.00           0             86.49          84462
 xe3                 0.00           0             86.49          84462
```

2. Send untagged traffic from SW1 xe2 (isolated port), traffic should forward to interfaces xe3 and xe1. On SW2, traffic should receive from xe1 and remaining ports should be 0.

```
SW1#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1                 0.00           0             86.49          84462
 xe2                 86.49          84462         0.00           0
 xe3                 0.00           0             86.49          84462
 xe4                 0.00           0             0.00           0

SW2#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1                 86.49          84462         0.00           0
 xe2                 0.00           0             0.00           0
 xe3                 0.00           0             0.00           0
```

3. Send untagged traffic from SW1 xe4 (community port), traffic should forward through interfaces xe3 and xe1. On SW2, traffic should receive from xe1 and forward to xe3.

```
SW1#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1                 0.00           0             86.49          84462
 xe2                 0.00           0             0.00           0
 xe3                 0.00           0             86.49          84462
 xe4                 86.49          84462         0.00           0

SW2#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1                 86.49          84462         0.00           0
 xe2                 0.00           0             0.00           0
 xe3                 0.00           0             86.49          84462
```

Spanning Tree Protocol Configuration

This section contains a complete sample Spanning Tree Protocol (STP) configuration.

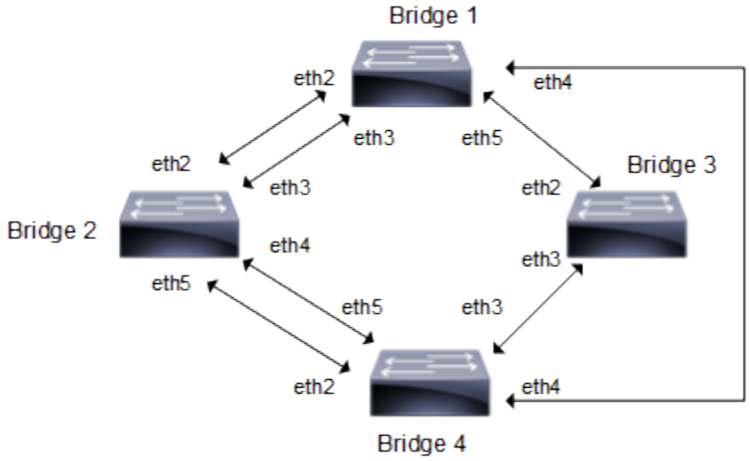
Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops. Spanning tree also allows a network design to include redundant links to provide automatic backup paths if an active link fails, thus, eliminating the need to manually enable or disable the backup links.

Configurations

Topology

The following example is a simple multi-bridge topology.

Figure 38. STP Topology



Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol ieee`	Add a bridge `(1)` to the spanning tree table
`Bridge1(config)#interface eth2`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.

`Bridge1(config)#interface eth3`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter interface mode
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol ieee`	Add a bridge (`2`) to the spanning tree table
`Bridge2(config)#interface eth2`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth4`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.

© 2026 IP Infusion Inc. Proprietary

`Bridge2(config)#interface eth5`	Enter interface mode
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol ieee`	Add a bridge (`4`) to the spanning tree table
`Bridge4(config)#interface eth2`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol ieee`	Add a bridge `(3)` to the spanning tree table

© 2026 IP Infusion Inc. Proprietary

`Bridge3(config)#interface eth2`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit interface mode.

Validation

Bridge 1

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 0
% 1: Root Id 80005254000be278
% 1: Bridge Id 80005254000be278
% 1: 15 topology changes - last topology change Sat Jul 10 09:44:56 2021
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8003 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 250 - designated cost 0
%   eth2: Designated Port Id 0x8004 - state Forwarding -Priority 128
%   eth2: Designated root 80005254000be278
%   eth2: Designated Bridge 80005254000be278
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 250 - designated cost 0
%   eth3: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth3: Designated root 80005254000be278
%   eth3: Designated Bridge 80005254000be278
```

```
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: Restricted-role OFF
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - path cost 250 - designated cost 0
%   eth4: Designated Port Id 0x8006 - state Forwarding -Priority 128
%   eth4: Designated root 80005254000be278
%   eth4: Designated Bridge 80005254000be278
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: Restricted-role OFF
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00 1970


% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
```

```
#show spanning-tree  interface eth1
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 0
% 1: Root Id 80005254000be278
% 1: Bridge Id 80005254000be278
% 1: 15 topology changes - last topology change Sat Jul 10 09:44:56 2021
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8003 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
```

Bridge 2

```
#show spanning-tree
% 2: Bridge up - Spanning Tree Enabled
% 2: Root Path Cost 250 - Priority 32768
% 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 2: Root Id 80005254000be278
% 2: Bridge Id 8000525400b210cd
```

```
% 2: 5 topology changes - last topology change Sat Jul 10 09:44:30 2021
% 2: portfast bpdu-filter disabled
% 2: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8003 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 250 - designated cost 0
%   eth2: Designated Port Id 0x8004 - state Blocked -Priority 128
%   eth2: Designated root 80005254000be278
%   eth2: Designated Bridge 80005254000be278
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 17 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 0
%   eth2: Restricted-role OFF
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 250 - designated cost 250
%   eth3: Designated Port Id 0x8005 - state Blocked -Priority 128
%   eth3: Designated root 80005254000be278
%   eth3: Designated Bridge 800052540047dc01
%   eth3: Message Age 3 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 13 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: Restricted-role OFF
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - path cost 250 - designated cost 250
%   eth4: Designated Port Id 0x8006 - state Blocked -Priority 128
%   eth4: Designated root 80005254000be278
%   eth4: Designated Bridge 800052540047dc01
%   eth4: Message Age 3 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 13 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: Restricted-role OFF
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00 1970
```

```
% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
```

```
#show spanning-tree interface eth1
% 2: Bridge up - Spanning Tree Enabled
% 2: Root Path Cost 250 - Priority 32768
% 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 2: Root Id 80005254000be278
% 2: Bridge Id 8000525400b210cd
% 2: 5 topology changes - last topology change Sat Jul 10 09:44:30 2021
% 2: portfast bpdu-filter disabled
% 2: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8003 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 17 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
```

Bridge 3

```
#sho spanning-tree
% 3: Bridge up - Spanning Tree Enabled
% 3: Root Path Cost 250 - Priority 32768
% 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 3: Root Id 80005254000be278
% 3: Bridge Id 8000525400686eb9
% 3: 2 topology changes - last topology change Sat Jul 10 09:37:36 2021
% 3: portfast bpdu-filter disabled
% 3: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 250 - designated cost 250
%   eth2: Designated Port Id 0x8004 - state Forwarding -Priority 128
%   eth2: Designated root 80005254000be278
%   eth2: Designated Bridge 8000525400686eb9
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
```

```
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Sat Jul 10 09:37:04 2021
% Default: 1 topology change(s)  - last topology change Sat Jul 10 09:37:04 2021


% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
```

```
#  show spanning-tree interface eth1
% 3: Bridge up - Spanning Tree Enabled
% 3: Root Path Cost 250 - Priority 32768
% 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 3: Root Id 80005254000be278
% 3: Bridge Id 8000525400686eb9
% 3: 2 topology changes - last topology change Sat Jul 10 09:37:36 2021
% 3: portfast bpdu-filter disabled
% 3: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 17 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
```

Bridge 4

```
#show spanning-tree
% 4: Bridge up - Spanning Tree Enabled
% 4: Root Path Cost 250 - Priority 32768
% 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 4: Root Id 80005254000be278
% 4: Bridge Id 800052540047dc01
% 4: 4 topology changes - last topology change Sat Jul 10 09:44:56 2021
% 4: portfast bpdu-filter disabled
% 4: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8006 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 17 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 250 - designated cost 250
%   eth2: Designated Port Id 0x8004 - state Forwarding -Priority 128
%   eth2: Designated root 80005254000be278
%   eth2: Designated Bridge 800052540047dc01
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
```

```
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 250 - designated cost 250
%   eth3: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth3: Designated root 80005254000be278
%   eth3: Designated Bridge 800052540047dc01
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: Restricted-role OFF
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - path cost 250 - designated cost 250
%   eth4: Designated Port Id 0x8006 - state Forwarding -Priority 128
%   eth4: Designated root 80005254000be278
%   eth4: Designated Bridge 800052540047dc01
%   eth4: Message Age 1 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: Restricted-role OFF
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%
```

```
#  show spanning-tree interface eth1
% 4: Bridge up - Spanning Tree Enabled
% 4: Root Path Cost 250 - Priority 32768
% 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 4: Root Id 80005254000be278
% 4: Bridge Id 800052540047dc01
% 4: 4 topology changes - last topology change Sat Jul 10 09:44:56 2021
% 4: portfast bpdu-filter disabled
% 4: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8006 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%
%
```

MLAG with Provider Bridging Configuration

This section contains sample MLAG with Provider bridging configuration.

A provider bridged network is a virtual bridged Local Area Network that comprises provider bridges (SVLAN bridges and provider edge bridges) and attached LANs, under the administrative control of a single service provider. Provider bridges interconnect the separate MACs of the IEEE 802 LANs that compose a provider bridged network, relaying frames to provide connectivity between all the LANs that provide customer interfaces for each service instance.

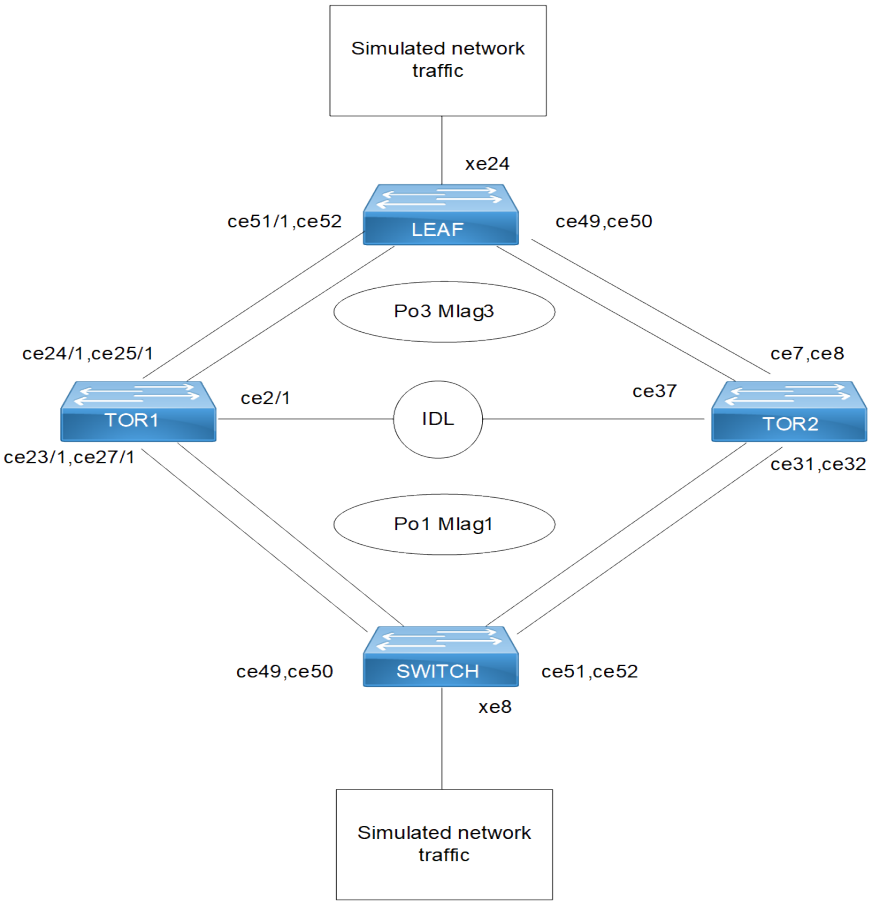
MLAG (also called DRNI, Distributed Resilient Network Interconnect) expands the concept of link aggregation so that it provides node-level redundancy by allowing two or more nodes to share a common LAG endpoint. MLAG emulates multiple nodes to represent as a single logical node to the remote node running link aggregation. As a result, even if one of the nodes is down there exists a path to reach the destination through the other nodes.

Note: For MLAG with PB, use provider rstp edge bridge on TOR (PEB) nodes and LEAF (PB) node.

Configuration

Topology

Figure 39. MLAG with Provider Bridging



Switch

`SWITCH#configure terminal`	Enter configuration mode
`SWITCH(config)#bridge 1 protocol rstp vlan-bridge`	Configure the rstp vlan bridge
`SWITCH(config)#vlan database`	Enter VLAN configuration mode
`SWITCH(config-vlan)#vlan 2-2000 bridge 1 state enable`	Create vlan for bridge
`SWITCH(config-vlan)#exit`	Exit VLAN configuration mode
`SWITCH(config)#interface po1`	Enter interface configuration mode for po1
`SWITCH(config-if)#switchport`	Configure switchport
`SWITCH(config-if)#bridge-group 1 spanning-tree disable`	Associate interface with bridge-group 1 by disblaing spanning tree
`SWITCH(config-if)#switchport mode trunk`	Configure switchport mode as trunk
`SWITCH(config-if)#switchport trunk allowed vlan all`	Associate created vlans to po1 interface
`SWITCH(config-if)#exit`	Exit from interface mode
`SWITCH(config)#interface xe8`	Enter interface configuration mode for xe8
`SWITCH(config-if)#switchport`	Configure switchport
`SWITCH(config-if)#bridge-group 1 spanning-tree disable`	Associate interface with bridge-group 1 by disblaing spanning tree
`SWITCH(config-if)#switchport mode trunk`	Configure switchport mode as trunk
`SWITCH(config-if)#switchport trunk allowed vlan all`	Associate created vlans to xe8 interface
`SWITCH(config-if)#exit`	Exit from interface mode
`SWITCH(config)#interface ce49`	Enter interface configuration mode for ce49
`SWITCH(config-if)# channel-group 1 mode active`	Configure interface as member port for po1- port channel
`SWITCH(config-if)#exit`	Exit from interface mode
`SWITCH(config)#interface ce50`	Enter interface configuration mode for ce49
`SWITCH(config-if)#channel-group 1 mode active`	Configure interface as member port for po1- port channel
`SWITCH(config-if)#exit`	Exit from interface mode
`SWITCH(config)#interface ce51`	Enter interface configuration mode for ce49
`SWITCH(config-if)#channel-group 1 mode active`	Configure interface as member port for po1- port channel
`SWITCH(config-if)#exit`	Exit from interface mode
`SWITCH(config)#interface ce52`	Enter interface configuration mode for ce49
`SWITCH(config-if)#channel-group 1 mode active`	Configure interface as member port for po1- port channel
`SWITCH(config-if)#exit`	Exit from interface mode
`SWITCH(config)#commit`	Commit the candidate configuration to the running

© 2026 IP Infusion Inc. Proprietary

	configuration.
SWITCH(config)#exit	Exit from config mode

TOR1 (PEB)

TOR1#configure terminal	Enter configuration mode
TOR1(config)#bridge 1 protocol provider-rstp edge	Create provider rstp edge bridge
TOR1(config)#vlan database	Enter VLAN configuration mode
TOR1(config-vlan)#vlan 2-500 type customer bridge 1 state enable	Create customer vlan VLAN 2-500
TOR1(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable	Create service vlan VLAN 501-1005
TOR1(config-vlan)#exit	Exit VLAN configuration mode
TOR1(config)#cvlan registration table cvlan100 bridge 1	Create cvlan registration table with name cvlan100
TOR1(config-cvlan-registration)#cvlan 100 svlan 1000	Map cvlan100 with svlan 1000
TOR1(config-cvlan-registration)#exit	Exit registration table
TOR1(config)#hardware-profile filter egress-l2 enable	Enable the hardware-profile filter for egress l2.
TOR1(config)#interface mlag1	Enter interface configuration mode for mlag1
TOR1(config-if)#switchport	Configure switchport
TOR1(config-if)#bridge-group 1 spanning-tree disable	Associate interface with bridge-group 1 and disable spanning-tree
TOR1(config-if)#switchport mode customer-edge trunk	Configure switchport mode customer edge
TOR1(config-if)# switchport customer-edge trunk allowed vlan add 100	Associate customer vlan100 to interface
TOR1(config-if)#switchport customer-edge vlan registration cvlan100	Attach registration table cvlan100 to interface
TOR1(config-if)#mode active-active	Configure mlag mode as active-active
TOR1(config-if)#exit	Exit interface mode
TOR1(config)#interface mlag3	Enter interface configuration mode for mlag3
TOR1(config-if)#switchport	Make interface as switchport
TOR1(config-if)# bridge-group 1 spanning-tree disable	Associate interface with bridge-group 1 and disable spanning-tree
TOR1(config-if)#switchport mode provider- network	Configure switchport pnp port
TOR1(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
TOR1(config-if)#mode active-active	Configure mlag mode as active-active
TOR1(config-if)#exit	Exit interface configuration mode
TOR1(config)#interface po1	Enter interface configuration mode for po1
TOR1(config-if)#switchport	Make interface as switchport

© 2026 IP Infusion Inc. Proprietary

`TOR1(config-if)#mlag 1`	Associate mlag1 interfacce to po1
`TOR1(config-if)#exit`	Exit interface configuration mode
`TOR1(config)#interface po3`	Enter interface configuration mode for po3
`TOR1(config-if)#switchport`	Make interface as switchport
`TOR1(config-if)#dot1ad ethertype 0x88a8`	Configure TPID with 88a8 to send and receive double tag (Q in Q)
`TOR1(config-if)#mlag 3`	Associate mlag3 interfacce to po3
`TOR1(config-if)#exit`	Exit interface configuration mode
`TOR1(config)#interface ce2/1`	Enter interface configuration mode for ce2/1 which is an IDL link
`TOR1(config-if)#switchport`	Make interface as switchport
`TOR1(config-if)#exit`	Exit interface configuration mode
`TOR1(config)#interface ce24/1`	Enter interface configuration mode for ce24/1
`TOR1(config-if)#channel-group 3 mode active`	Configure interface as member port for po3- port channel
`TOR1(config-if)#exit`	Exit interface configuration mode
`TOR1(config)# interface ce25/1`	Enter interface configuration mode for ce25/1
`TOR1(config-if)#channel-group 3 mode active`	Configure interface as member port for po3- port channel
`TOR1(config-if)#exit`	Exit interface configuration mode
`TOR1(config)#interface ce23/1`	Enter interface configuration mode for ce23/1
`TOR1(config-if)#channel-group 1 mode active`	Configure interface as member port for po1- port channel
`TOR1(config-if)#exit`	Exit interface configuration mode
`TOR1(config)#interface ce27/1`	Enter interface configuration mode for ce2471
`TOR1(config-if)#channel-group 1 mode active`	Configure interface as member port for po1- port channel
`TOR1(config-if)#exit`	Exit interface configuration mode
`TOR1(config)#mcec domain configuration`	Enter mcec domain configuration mode
`TOR1(config-mcec-domain)#domain-address 2222.3333.4444`	Configure domain address for mlag domain
`TOR1(config-mcec-domain)#domain-system-number 1`	Configure domain number to identify node in a domain
`TOR1(config-mcec-domain)#intra-domain-link ce2/1`	Configure intra domain link between tor nodes mlag domain
`TOR1(config-mcec-domain)#exit`	Exit from mcec domain mode
`TOR1(config)#commit`	Commit the candidate configuration to the running configuration.
`TOR1(config)#exit`	Exit from config mode

© 2026 IP Infusion Inc. Proprietary

TOR2 (PEB)

`TOR2#configure terminal`	Enter configuration mode
`TOR2(config)#bridge 1 protocol provider-rstp edge`	Create provider rstp edge bridge
`TOR2(config)#vlan database`	Enter VLAN configuration mode
`TOR2(config-vlan)#vlan 2-500 type customer bridge 1 state enable`	Create customer vlan VLAN 2-500
`TOR2(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable`	Create service vlan VLAN 501-1005
`TOR2(config-vlan)#exit`	Exit VLAN configuration mode
`TOR2(config)#cvlan registration table cvlan100 bridge 1`	Create cvlan registration table with name cvlan100
`TOR2(config-cvlan-registration)#cvlan 100 svlan 1000`	Map cvlan100 with svlan 1000
`TOR2(config-cvlan-registration)#exit`	Exit registration table
`TOR2(config)#hardware-profile filter egress-l2 enable`	Enable the hardware-profile filter for egress l2.
`TOR2(config)#interface mlag1`	Enter interface configuration mode for mlag1
`TOR2(config-if)#switchport`	Configure switchport
`TOR2(config-if)#bridge-group 1 spanning-tree disable`	Associate interface with bridge-group 1 and disable spanning-tree
`TOR2(config-if)#switchport mode customer-edge trunk`	Configure switchport mode customer edge
`TOR2(config-if)# switchport customer-edge trunk allowed vlan add 100`	Associate customer vlan 100 to interface
`TOR2(config-if)#switchport customer-edge vlan registration cvlan100`	Attach registration table cvlan100 to interface
`TOR2(config-if)#mode active-active`	Configure mlag mode as active-active
`TOR2(config-if)#exit`	Exit interface mode
`TOR2(config)#interface mlag3`	Enter interface configuration mode for mlag3
`TOR2(config-if)#switchport`	Make interface as switchport
`TOR2(config-if)# bridge-group 1 spanning-tree disable`	Associate interface with bridge-group 1 and disable spanning-tree
`TOR2(config-if)#switchport mode provider- network`	Configure switchport pnp port
`TOR2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`TOR2(config-if)#mode active-active`	Configure mlag mode as active-active
`TOR2(config-if)#exit`	Exit interface configuration mode
`TOR2(config)#interface po1`	Enter interface configuration mode for po1
`TOR2(config-if)#switchport`	Make interface as switchport
`TOR2(config-if)#mlag 1`	Associate mlag1 interfacce to po1
`TOR2(config-if)#exit`	Exit interface configuration mode

© 2026 IP Infusion Inc. Proprietary

`TOR2(config)#interface po3`	Enter interface configuration mode for po3
`TOR2(config-if)#switchport`	Make interface as switchport
`TOR2(config-if)#dot1ad ethertype 0x88a8`	Configure TPID with 88a8 to send and receive double tag (Q in Q)
`TOR2(config-if)#mlag 3`	Associate mlag1 interfacce to po3
`TOR2(config-if)#exit`	Exit interface configuration mode
`TOR2(config)#interface ce37`	Enter interface configuration mode for ce2/1 which is an IDL link
`TOR2(config-if)#switchport`	Make interface as switchport
`TOR2(config-if)#exit`	Exit interface configuration mode
`TOR2(config)#interface ce7`	Enter interface configuration mode for ce7
`TOR2(config-if)#channel-group 3 mode active`	Configure interface as member port for po3- port channel
`TOR2(config-if)#exit`	Exit interface configuration mode
`TOR2(config)# interface ce8`	Enter interface configuration mode for ce8
`TOR2(config-if)#channel-group 3 mode active`	Configure interface as member port for po3- port channel
`TOR2(config-if)#exit`	Exit interface configuration mode
`TOR2(config)#interface ce31`	Enter interface configuration mode for ce31
`TOR2(config-if)#channel-group 1 mode active`	Configure interface as member port for po1- port channel
`TOR2(config-if)#exit`	Exit interface configuration mode
`TOR2(config)#interface ce32`	Enter interface configuration mode for ce32
`TOR2(config-if)#channel-group 1 mode active`	Configure interface as member port for po1- port channel
`TOR2(config-if)#exit`	Exit interface configuration mode
`TOR2(config)#mcec domain configuration`	Enter mcec domain configuration mode
`TOR2(config-mcec-domain)#domain-address 2222.3333.4444`	Configure domain address for mlag domain
`TOR2(config-mcec-domain)#domain-system-number 2`	Configure domain number to identify node in a domain
`TOR2(config-mcec-domain)#intra-domain-link ce37`	Configure intra domain link between tor nodes mlag domain
`TOR2(config-mcec-domain)#exit`	Exit interface configuration mode
`TOR2(config)#commit`	Commit the candidate configuration to the running configuration.
`TOR2(config)#exit`	Exit interface configuration mode

LEAF(PB)

`LEAF#configure terminal`	Enter configuration mode
`LEAF(config)# bridge 1 protocol provider-rstp edge`	Create provider rstp edge bridge
`LEAF(config)#vlan database`	Enter VLAN configuration mode
`LEAF(config-vlan)#vlan 2-500 type customer bridge 1 state enable`	Create customer vlan VLAN 2-500
`LEAF(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable`	Create service vlan VLAN 501-1005
`LEAF(config-vlan)#exit`	Exit VLAN configuration mode
`LEAF(config)#interface po3`	Enter interface configuration mode for po3
`LEAF(config-if)#switchport`	Make interface as switchport
`LEAF(config-if)#dot1ad ethertype 0x88a8`	Configure TPID with 88a8 to send and receive double tag (Q in Q)
`LEAF(config-if)#bridge-group 1 spanning-tree disable`	Associate interface with bridge-group 1 and disable spanning-tree
`LEAF(config-if)#switchport mode provider-network`	Configure switchport pnp port
`LEAF(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`LEAF(config-if)#exit`	Exit interface configuration mode
`LEAF(config)#interface xe24`	Enter interface configuration mode for xe24
`LEAF(config-if)#switchport`	Make interface as switchport
`LEAF(config-if)#dot1ad ethertype 0x88a8`	Configure TPID with 88a8 to send and receive double tag (Q in Q)
`LEAF(config-if)#bridge-group 1 spanning-tree disable`	Associate interface with bridge-group 1 and disable spanning-tree
`LEAF(config-if)#switchport mode provider-network`	Configure switchport pnp port
`LEAF(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`LEAF(config-if)#exit`	Exit interface configuration mode
`LEAF(config)#interface ce49`	Enter interface configuration mode for ce49
`LEAF(config-if)# channel-group 3 mode active`	Configure interface as member port for po3- port channel
`LEAF(config-if)#exit`	Exit interface configuration mode
`LEAF(config)#interface ce50`	Enter interface configuration mode for ce50
`LEAF(config-if)# channel-group 3 mode active`	Configure interface as member port for po3- port channel
`LEAF(config-if)#exit`	Exit interface configuration mode

© 2026 IP Infusion Inc. Proprietary

`LEAF(config)#interface ce51`	Enter interface configuration mode for ce51
`LEAF(config-if)# channel-group 3 mode active`	Configure interface as member port for po3- port channel
`LEAF(config-if)#exit`	Exit interface configuration mode
`LEAF(config)#interface ce52`	Enter interface configuration mode for ce52
`LEAF(config-if)# channel-group 3 mode active`	Configure interface as member port for po3- port channel
`LEAF(config-if)#exit`	Exit interface configuration mode
`LEAF(config)#commit`	Commit the candidate configuration to the running configuration.
`LEAF(config)#exit`	Exit from config mode

Validation

Validation commands are : `show mlag domain summary , show mlag domain details, show ether-channel summary, show bridge, Show mac address-table bridge <bridge-id>, show cvlan registration table bridge <bridge-id>`

For below show mac table output sending cvlan 100 traffic from SWITCH to LEAF, for which TOR nodes add svlan 1000 and egress same to LEAF and LEAF ixia also receives double tag.

```
TOR1#show mlag domain details

------------------------------------
Domain Configuration
------------------------------------

Domain System Number           : 1
Domain Address                 : 2222.3333.4444
Domain Priority                : 32768
Intra Domain Interface         : ce2/1

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP
Domain Sync via                : Intra-domain-interface

------------------------------------
MLAG Configuration
------------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Admin Key                    : 16385
  Oper Key                     : 16385
  Physical status              : 1
  Physical properties Digest   : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2

  Neigh Admin Key              : 32769
  Neigh Physical status        : 1
  Neigh Physical Digest        : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Active
```

```
  Current Mlag state           : Active

MLAG-3
  Mapped Aggregator            : po3
  Admin Key                    : 16387
  Oper Key                     : 16387
  Physical status              : 1
  Physical properties Digest   : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93

  Neigh Admin Key              : 32771
  Neigh Physical status        : 1
  Neigh Physical Digest        : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Active
  Current Mlag state           : Active

TOR1#

TOR1#show mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 2222.3333.4444
Domain Priority                 : 32768
Intra Domain Interface          : ce2/1
Domain Adjacency                : UP
Domain Sync via                 : Intra-domain-interface
-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Physical properties Digest   : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2
  Total Bandwidth              : 400g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Active
  Current Mlag state           : Active


MLAG-3
  Mapped Aggregator            : po3
  Physical properties Digest   : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93
  Total Bandwidth              : 400g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Active
  Current Mlag state           : Active


TOR1#

TOR1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 16385 - Oper Key 16385
     Link: ce23/1 (5001) sync: 1 (Mlag-active-link)
     Link: ce27/1 (5029) sync: 1 (Mlag-active-link)
-------------------------------------
  Aggregator po3 100003
  Aggregator Type: Layer2
  Admin Key: 16387 - Oper Key 16387
     Link: ce25/1 (5005) sync: 1 (Mlag-active-link)
     Link: ce24/1 (5117) sync: 1 (Mlag-active-link)
```

```
TOR1#

TOR2#show mlag domain details

------------------------------------
Domain Configuration
------------------------------------

Domain System Number           : 2
Domain Address                 : 2222.3333.4444
Domain Priority                : 32768
Intra Domain Interface         : ce37

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP
Domain Sync via                : Intra-domain-interface

------------------------------------
MLAG Configuration
------------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Admin Key                    : 32769
  Oper Key                     : 16385
  Physical status              : 1
  Physical properties Digest   : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2

  Neigh Admin Key              : 16385
  Neigh Physical status        : 1
  Neigh Physical Digest        : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Active
  Current Mlag state           : Active

MLAG-3
  Mapped Aggregator            : po3
  Admin Key                    : 32771
  Oper Key                     : 16387
  Physical status              : 1
  Physical properties Digest   : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93

  Neigh Admin Key              : 16387
  Neigh Physical status        : 1
  Neigh Physical Digest        : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Active
  Current Mlag state           : Active

TOR2#  show mlag domain summary

------------------------------------
Domain Configuration
------------------------------------

Domain System Number            : 2
Domain Address                  : 2222.3333.4444
Domain Priority                 : 32768
Intra Domain Interface          : ce37
Domain Adjacency                : UP
Domain Sync via                 : Intra-domain-interface
```

```
-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Physical properties Digest   : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2
  Total Bandwidth              : 400g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Active
  Current Mlag state           : Active


MLAG-3
  Mapped Aggregator            : po3
  Physical properties Digest   : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93
  Total Bandwidth              : 400g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Active
  Current Mlag state           : Active
TOR2#

TOR2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 32769 - Oper Key 16385
     Link: ce31 (5062) sync: 1 (Mlag-active-link)
     Link: ce32 (5064) sync: 1 (Mlag-active-link)
-------------------------------------
  Aggregator po3 100003
  Aggregator Type: Layer2
  Admin Key: 32771 - Oper Key 16387
     Link: ce7 (5029) sync: 1 (Mlag-active-link)
     Link: ce8 (5031) sync: 1 (Mlag-active-link)
TOR2#

SWITCH2#show bridge
bridge 1 is running on rstp vlan-bridge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
  1         100                 xe8         0000.2223.2425    1     300
SWITCH2#
SWITCH2#
SWITCH2#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
  100          0000.2223.2425  dynamic   xe8       Disable
SWITCH2#


TOR1# show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
1               1000          mlag1       0000.2223.2425    1     300
TOR1#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   mlag1     Disable
TOR1#


TOR2#show bridge
bridge 1 is running on provider-rstp edge
```

```
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
  1               1000          mlag1       0000.2223.2425    1     300
TOR2#

TOR2#
TOR2#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   mlag1     Disable
TOR2#
```

```
LEAF#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   po3       Disable
LEAF#
```

```
LEAF#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1000          po3         0000.2223.2425    1     300
LEAF#
```

Now send traffic with svlan-1000 and c-vlan 100 from LEAF to SWITCH,Tor removes svlan and send only cvlan to SWITCH

```
LEAF#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1000          po3         0000.2223.2425    1     300
 1               1000          xe24        0000.2425.2627    1     300
LEAF#

LEAF#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   po3       Disable
       1000   0000.2425.2627  dynamic   xe24      Disable
LEAF#
```

```
TOR1#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1000          mlag1       0000.2223.2425    1     300
 1               1000          mlag3       0000.2425.2627    1     300
TOR1#
```

```
TOR1#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   mlag1     Disable
       1000   0000.2425.2627  dynamic   mlag3     Disable
TOR1#


TOR2#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1                1000          mlag1       0000.2223.2425    1     300
 1                1000          mlag3       0000.2425.2627    1     300
TOR2#

TOR2#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   mlag1     Disable
       1000   0000.2425.2627  dynamic   mlag3     Disable
TOR2#


SWITCH2#show bridge
bridge 1 is running on rstp vlan-bridge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         100                 xe8         0000.2223.2425    1     300
 1         100                 po1         0000.2425.2627    1     300
SWITCH2#

SWITCH2#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
 100          0000.2223.2425  dynamic   xe8       Disable
 100          0000.2425.2627  dynamic   po1       Disable
SWITCH2#
```

RPVST+ Configuration

This section contains a complete example of an RPVST+ configuration.

Topology

Figure 40. RPVST+ configuration

Configuration

Switch 2

`#configure terminal`	Enter configure mode for the switch.
`(config)#bridge 1 protocol rpvst+`	Configure bridge 1 as an RPVST+ bridge.
`(config)#vlan 2-3 bridge 1`	Configure VLAN 2 and 3 and associate it to bridge 1.
`(config)#spanning-tree rpvst+ configuration`	Enter Rapid Per-VLAN Spanning Tree configuration mode.
`(config-rpvst+)#bridge 1 vlan 2`	Associate a configured VLAN with bridge 1.
`(config-rpvst+)#bridge 1 vlan 3`	Associate a configured VLAN with bridge 1,.
`(config-rvpst+)#exit`	Exit RPVST+ configuration mode.
`(config)#interface eth1`	Enter interface mode for eth1.
`(config-if)#switchport`	Configure eth1 as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface.
`(config-if)#switchport mode trunk`	Configure port as trunk.
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#bridge-group 1 vlan 2`	Configure bridge group to interface with VLAN 2.
`(config-if)#bridge-group 1 vlan 3`	Configure bridge group to interface with VLAN 3.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for eth2.
`(config-if)#switchport`	Configure eth2 as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface/
`(config-if)#switchport mode trunk`	Configure port as trunk
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#bridge-group 1 vlan 2`	Configure bridge group to interface with VLAN 2.

© 2026 IP Infusion Inc. Proprietary

`(config-if)#bridge-group 1 vlan 3`	Configure bridge group to interface with VLAN3.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode.

Switch 1

`#configure terminal`	Enter configure mode for the switch.
`(config)#bridge 1 protocol rpvst+`	Configure bridge 1 as an rpvst+ bridge.
`(config)#vlan 2-3 bridge 1`	Configure VLAN 2 and 3 and associate it to bridge 1.
`(config)#spanning-tree rpvst+ configuration`	Enter Rapid Per-VLAN Spanning Tree configuration mode.
`(config-rpvst+)#bridge 1 vlan 2`	Associate a configured VLAN with bridge 1.
`(config-rpvst+)#bridge 1 vlan 3`	Associate a configured VLAN with bridge 1.
`(config-rvpst+)#exit`	Exit RPVST+ configuration mode.
`(config)#interface eth1`	Enter interface mode for eth1.
`(config-if)#switchport`	Configure eth1 as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface.
`(config-if)#switchport mode trunk`	Configure port as trunk.
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#bridge-group 1 vlan 2`	Configure bridge group to interface with VLAN 2.
`(config-if)#bridge-group 1 vlan 3`	Configure bridge group to interface with VLAN3.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode.

Switch 3

`#configure terminal`	Enter configure mode for the switch.
`(config)#bridge 1 protocol rpvst+`	Configure bridge 1 as an rpvst+ bridge
`(config)#vlan 2-3 bridge 1`	Configure VLAN 2 and 3 and associate it to bridge 1.
`(config)#interface eth1`	Enter interface mode for eth1.
`(config-if)#switchport`	Configure eth1 as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface.
`(config-if)#switchport mode trunk`	Configure port as trunk.
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode.

© 2026 IP Infusion Inc. Proprietary

Validation

Switch2

```
#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b7bfa7
% 1: Bridge Id 8002525400b7bfa7
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b7bfa7
%   eth1: Designated Bridge 8002525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128
%   eth2: Configured External Priority 128
%   eth2: Designated Root 8002525400b7bfa7
%   eth2: Designated Bridge 8002525400b7bfa7
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%

#show spanning-tree rpvst+ interface eth1
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80015254000be278
% 1: Bridge Id 80015254000be278
% 1: last topology change Tue Jul  6 10:51:37 2021
% 1: 6 topology change(s)  - last topology change Tue Jul  6 10:51:37 2021

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 20000000  - Add type Explicit ref count 3
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 80015254000be278
%   eth1: Designated Bridge 80015254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth1: forward-transitions 2
%   eth1: Restricted-role OFF
%   eth1: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%
```

```
%
%   Instance        VLAN
%   0:              1
%   1:              2
%   2:              3
#


#show spanning-tree rpvst+ detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80015254008e6259
% 1: Bridge Id 80015254008e6259
% 1: last topology change Fri Aug 19 07:49:51 2022
% 1: 2 topology change(s)  - last topology change Fri Aug 19 07:49:51 2022

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 3
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 80015254008e6259
%   eth1: Designated Bridge 80015254008e6259
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 0
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 3
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 80015254008e6259
%   eth2: Designated Bridge 80015254008e6259
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%

% Instance  1:  Vlans: 2
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003 (Priority 0x80 Port Number
0x03)
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 80025254008e6259 (Priority 0x8002 Address 52:54:00:8e:62:59)
%   eth1: Designated Bridge 80025254008e6259 (Priority 0x8002 Address 52:54:00:8e:62:59)
```

```
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0


% Instance  1:  Vlans: 2
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004 (Priority 0x80 Port Number
0x04)
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128
%   eth2: Configured External Priority 128
%   eth2: Designated Root 80025254008e6259 (Priority 0x8002 Address 52:54:00:8e:62:59)
%   eth2: Designated Bridge 80025254008e6259 (Priority 0x8002 Address 52:54:00:8e:62:59)
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1


% Instance  2:  Vlans: 3
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003 (Priority 0x80 Port Number
0x03)
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 80035254008e6259 (Priority 0x8003 Address 52:54:00:8e:62:59)
%   eth1: Designated Bridge 80035254008e6259 (Priority 0x8003 Address 52:54:00:8e:62:59)
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0


% Instance  2:  Vlans: 3
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004 (Priority 0x80 Port Number
0x04)
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128
%   eth2: Configured External Priority 128
%   eth2: Designated Root 80035254008e6259 (Priority 0x8003 Address 52:54:00:8e:62:59)
%   eth2: Designated Bridge 80035254008e6259 (Priority 0x8003 Address 52:54:00:8e:62:59)
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

#
```

© 2026 IP Infusion Inc. Proprietary

RSTP Configuration

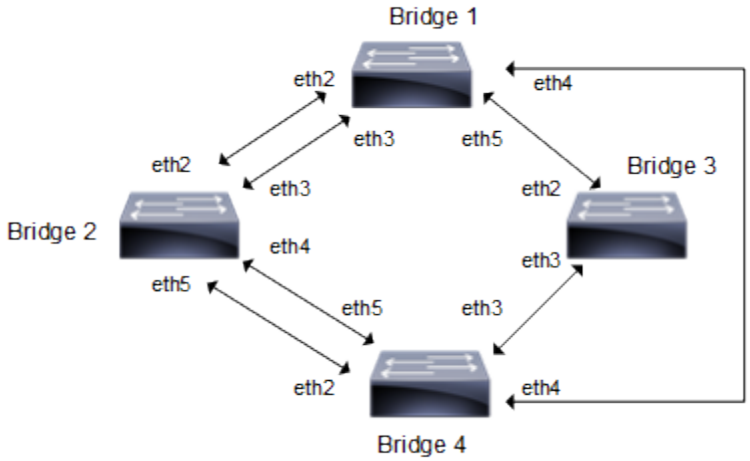
This section contains a complete sample Rapid Spanning Tree Protocol (RSTP) configuration. RSTP provides rapid convergence of a spanning tree. It speeds up the reconfiguration of the tree after a change by using alternate ports.

Configuration

Topology

The following example is a simple multi-bridge topology.

Figure 41. RSTP Topology



Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol rstp`	Add a bridge (`1`) to the rapid spanning tree table
`Bridge1(config)#interface eth2`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode.

`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter interface mode
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#commit`	Commit the configure on the node.
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol rstp`	Add a bridge (`2`) to the rapid spanning tree table
`Bridge2(config)#interface eth2`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth4`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#commit`	Commit the configure on the node.
`Bridge2(config-if)#exit`	Exit interface mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol rstp`	Add a bridge `(3)` to the rapid spanning tree table
`Bridge3(config)#interface eth2`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.

© 2026 IP Infusion Inc. Proprietary

`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#commit`	Commit the configure on the node.
`Bridge3(config-if)#exit`	Exit interface mode.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol rstp`	Add a bridge `(4)` to the rapid spanning tree table
`Bridge4(config)#interface eth2`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#commit`	Commit the configure on the node.
`Bridge4(config-if)#exit`	Exit interface mode.

Validation

show spanning-tree, show spanning-tree interface <if-name>

Bridge 1

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 200000 - Root Port 6 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 800052540046f549
% 1: Bridge Id 80005254009cb7e6
% 1: last topology change Tue Aug 11 02:25:01 2020
% 1: 30 topology change(s)  - last topology change Tue Aug 11 02:25:01 2020

% 1: portfast bpdu-filter disabled
```

```
% 1: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State Discarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 8000525400751db5
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 2
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State Discarding
%   eth3: Designated Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 8000525400751db5
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 3
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State Forwarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8006 - Priority 128  -
%   eth4: Root 800052540046f549
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 6
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State Discarding
%   eth5: Designated Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8004 - Priority 128  -
%   eth5: Root 800052540046f549
%   eth5: Designated Bridge 800052540065fd8c
%   eth5: Message Age 1 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change timer 0
%   eth5: forward-transitions 4
```

```
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00 1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
```

Bridge 2

```
#show spanning-tree
% 2: Bridge up - Spanning Tree Enabled  - topology change detected
% 2: Root Path Cost 200000 - Root Port 7 -  Bridge Priority 32768
% 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 2: Root Id 800052540046f549
% 2: Bridge Id 8000525400751db5
% 2: last topology change Tue Aug 11 02:25:00 2020
% 2: 22 topology change(s)  - last topology change Tue Aug 11 02:25:00 2020

% 2: portfast bpdu-filter disabled
% 2: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State Forwarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 8000525400751db5
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 3
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State Forwarding
%   eth3: Designated Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 8000525400751db5
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 3
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
```

```
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Alternate - State Discarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8007 - Priority 128  -
%   eth4: Root 800052540046f549
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 3
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Rootport - State Forwarding
%   eth5: Designated Path Cost 0
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8004 - Priority 128  -
%   eth5: Root 800052540046f549
%   eth5: Designated Bridge 800052540046f549
%   eth5: Message Age 0 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0
%   eth5: forward-transitions 2
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00 1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
```

Bridge 3

```
#show spanning-tree
% 3: Bridge up - Spanning Tree Enabled  - topology change detected
% 3: Root Path Cost 200000 - Root Port 5 -  Bridge Priority 32768
% 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 3: Root Id 800052540046f549
% 3: Bridge Id 800052540065fd8c
% 3: last topology change Tue Aug 11 02:25:00 2020
% 3: 16 topology change(s)  - last topology change Tue Aug 11 02:25:00 2020

% 3: portfast bpdu-filter disabled
% 3: portfast bpdu-guard disabled
```

```
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State Forwarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 800052540065fd8c
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth2: forward-transitions 2
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Rootport - State Forwarding
%   eth3: Designated Path Cost 0
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 800052540046f549
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 2
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00 1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
```

Bridge 4

```
#show spanning-tree
% 4: Bridge up - Spanning Tree Enabled  - topology change detected
% 4: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 4: Root Id 800052540046f549
% 4: Bridge Id 800052540046f549
% 4: last topology change Tue Aug 11 02:24:58 2020
% 4: 6 topology change(s)  - last topology change Tue Aug 11 02:24:58 2020

% 4: portfast bpdu-filter disabled
% 4: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State Forwarding
%   eth2: Designated Path Cost 0
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 800052540046f549
```

```
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State Forwarding
%   eth3: Designated Path Cost 0
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 800052540046f549
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State Forwarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8006 - Priority 128  -
%   eth4: Root 800052540046f549
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State Forwarding
%   eth5: Designated Path Cost 0
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8007 - Priority 128  -
%   eth5: Root 800052540046f549
%   eth5: Designated Bridge 800052540046f549
%   eth5: Message Age 0 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth5: forward-transitions 1
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
```

```
%   eth5: No auto-edge configured - Current port Auto Edge off
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00 1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
```

VLAN Configuration

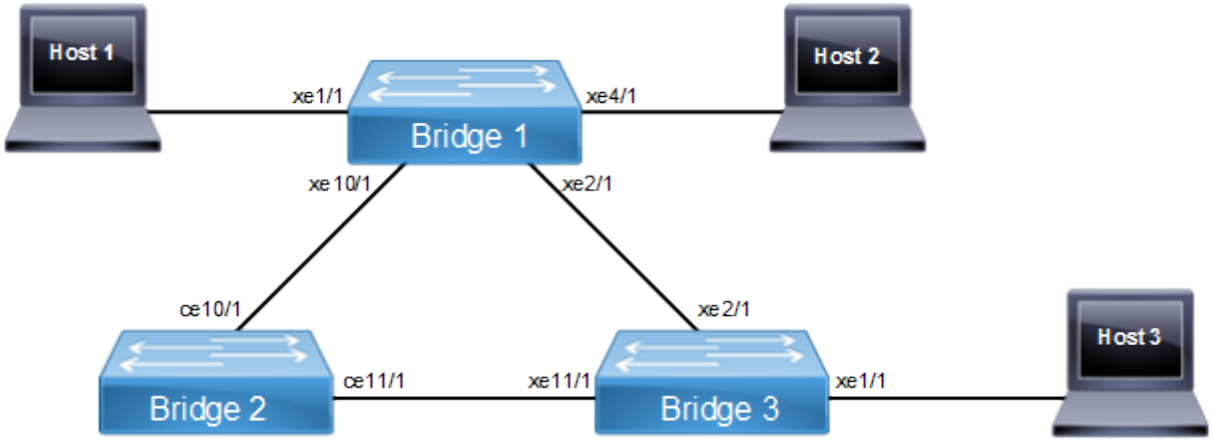
This section contains an example for VLAN configuration on trunk port.

Configuration

Topology

This shows configuring a VLAN bridge with VLAN tags on forwarding frames. Link between Bridge 2 and Bridge 3 is configured with VLAN 5 and VLAN 10. Link between Bridge 2 and Bridge 1 is configured as VLAN 5 and link between Bridge 3 and Bridge 1 is configured as VLAN 10.

Figure 42. VLAN Topology



Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

`Bridge1#configure terminal`	Enter configuration mode
`Bridge1(config)#bridge 1 protocol ieee vlan-bridge`	Specify VLAN for bridge 1.
`Bridge1(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge1(config-vlan)#vlan 5 bridge 1 state enable`	Enable VLAN (5) on bridge 1.Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge1(config-vlan)#vlan 10 bridge 1 state enable`	Enable VLAN (10) on bridge 1. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge1(config-vlan)#commit`	Commit the candidate configuration to the running configuration.

© 2026 IP Infusion Inc. Proprietary

`Bridge1(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge1(config)#interface xe1/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge1(config-if)#switchport access vlan 5`	Enable VLAN ID 5 on this port.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe2/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge1(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe4/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge1(config-if)#switchport access vlan 10`	Enable VLAN ID 10 on this port.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe10/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge1(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol ieee vlan-bridge`	Specify VLAN for bridge 2.
`Bridge2(config)#vlan database`	
`Bridge2(config-vlan)#vlan 5 bridge 2 state enable`	Enable VLAN (5) on bridge 2. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge2(config-vlan)#vlan 10 bridge 2 state enable`	Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge2(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge2(config)#interface ce10/1`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure port as L2.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge2(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge2(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge2(config)#interface ce11/1`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure port as L2.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge2(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge2(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit from the interface mode and go config mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.

`Bridge3(config)#bridge 3 protocol ieee vlan-bridge`	Specify VLAN for bridge 3.
`Bridge3(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge3(config-vlan)#vlan 5 bridge 3 state enable`	Enable VLAN (5) on bridge 3. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge3(config-vlan)#vlan 10 bridge 3 state enable`	Enable VLAN (10) on bridge 3. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge3(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge3(config)#interface xe1/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge3(config-if)#switchport access vlan 10`	Enable VLAN ID 10 on this port.
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge3(config)#interface xe2/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge3(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge3(config)#interface xe11/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge3(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.

© 2026 IP Infusion Inc. Proprietary

Validation

Bridge 1

```
Bridge1#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 1 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 909
% 1: Root Id 8000001823304db6
% 1: Bridge Id 8000001823305244
% 1: 6 topology changes - last topology change Fri Apr 19 12:32:26 2019
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   xe1/1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 - designated cost 1
%   xe1/1: Designated Port Id 0x8389 - state Forwarding -Priority 128
%   xe1/1: Designated root 8000001823304db6
%   xe1/1: Designated Bridge 8000001823305244
%   xe1/1: Message Age 1 - Max Age 20
%   xe1/1: Hello Time 2 - Forward Delay 15
%   xe1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   xe1/1: forward-transitions 1
%   xe1/1: No portfast configured - Current  portfast off
%   xe1/1: bpdu-guard  default  - Current bpdu-guard off
%   xe1/1: bpdu-filter default  - Current bpdu-filter off
%   xe1/1: no root guard configured     - Current root guard off
%
%   xe2/1: Port Number 909 - Ifindex 5005 - Port Id 0x838d - path cost 1 - designated cost 0
%   xe2/1: Designated Port Id 0x838d - state Forwarding -Priority 128
%   xe2/1: Designated root 8000001823304db6
%   xe2/1: Designated Bridge 8000001823304db6
%   xe2/1: Message Age 0 - Max Age 20
%   xe2/1: Hello Time 2 - Forward Delay 15
%   xe2/1: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 0 - topo change timer 0
%   xe2/1: forward-transitions 2
%   xe2/1: No portfast configured - Current  portfast off
%   xe2/1: bpdu-guard  default  - Current bpdu-guard off
%   xe2/1: bpdu-filter default  - Current bpdu-filter off
%   xe2/1: no root guard configured     - Current root guard off
%
%   xe4/1: Port Number 917 - Ifindex 5013 - Port Id 0x8395 - path cost 4 - designated cost 1
%   xe4/1: Designated Port Id 0x8395 - state Forwarding -Priority 128
%   xe4/1: Designated root 8000001823304db6
%   xe4/1: Designated Bridge 8000001823305244
%   xe4/1: Message Age 1 - Max Age 20
%   xe4/1: Hello Time 2 - Forward Delay 15
%   xe4/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   xe4/1: forward-transitions 1
%   xe4/1: No portfast configured - Current  portfast off
%   xe4/1: bpdu-guard  default  - Current bpdu-guard off
%   xe4/1: bpdu-filter default  - Current bpdu-filter off
%   xe4/1: no root guard configured     - Current root guard off
%
%   xe10/1: Port Number 941 - Ifindex 5037 - Port Id 0x83ad - path cost 2 - designated cost 1
%   xe10/1: Designated Port Id 0x83ad - state Forwarding -Priority 128
%   xe10/1: Designated root 8000001823304db6
%   xe10/1: Designated Bridge 8000001823305244
%   xe10/1: Message Age 1 - Max Age 20
%   xe10/1: Hello Time 2 - Forward Delay 15
%   xe10/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   xe10/1: forward-transitions 2
%   xe10/1: No portfast configured - Current  portfast off
%   xe10/1: bpdu-guard  default  - Current bpdu-guard off
%   xe10/1: bpdu-filter default  - Current bpdu-filter off
%   xe10/1: no root guard configured     - Current root guard off
%
```

```
B1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe2/1       0018.23cb.fbbc    1     300
 1         1                   xe10/1      cc37.ab97.37d8    1     300
 1         5                   xe1/1       0000.11bc.5dec    1     300
 1         10                  xe4/1       0000.2d50.205c    1     300
Bridge1#


Bridge1#show vlan all bridge 1
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                      (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Success    xe10/1(u) xe2/1(u)
1       5       VLAN0005         ACTIVE  Success    xe1/1(u) xe10/1(t)
1       10      VLAN0010         ACTIVE  Success    xe4/1(u)xe2/1(t)


Bridge1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe2/1       0018.23cb.fbbc    1     300
 1         1                   xe10/1      cc37.ab97.37d8    1     300
 1         5                   xe1/1       0000.11bc.5dec    1     300
 1         10                  xe4/1       0000.2d50.205c    1     300
Bridge1#
```

Bridge 2

```
Bridge2#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 2         1                   ce10/1      0018.2326.166a    1     300
 2         1                   ce11/1      0018.23cb.fbe0    1     300
 2         1                   ce11/1      cc37.ab97.37d8    1     300
 2         5                   ce10/1      0000.11bc.5dec    1     300


Bridge2#show vlan all bridge 2
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                      (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
2       1       default          ACTIVE  Success    ce10/1(u) ce11/1(u)
2       5       VLAN0005         ACTIVE  Success    ce10/1(t) ce11/1(t)
2       10      VLAN0010         ACTIVE  Success    ce10/1(t) ce11/1(t)


Bridge2#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 2         1                   ce10/1      0018.2326.166a    1     300
 2         1                   ce11/1      0018.23cb.fbe0    1     300
 2         1                   ce11/1      cc37.ab97.37d8    1     300
 2         5                   ce10/1      0000.11bc.5dec    1     300
```

Bridge 3

```
Bridge3# show bridge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
```

```
 3         1                   xe2/1       cc37.ab97.37d8    1     300
 3         5                   xe11/1      0000.11bc.5dec    1     300
 3         10                  xe2/1       0000.2d50.205c    1     300
Bridge3#show vlan all bridge 3
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
3       1       default          ACTIVE  Success    xe11/1(u) xe2/1(u)
3       5       VLAN0005         ACTIVE  Success    xe11/1(t)
3       10      VLAN0010         ACTIVE  Success    xe1/1(u) xe2/1(t)
```

ErrDisable for Link-Flapping Configuration

If a link flaps continuously, the interface goes into ErrDisable state. When a port is the ErrDisable state, it is effectively shut down and no traffic is sent or received on that port. The port can be recovered from the ErrDisable state manually (shutting down the interface) or automatically (setting a timeout value).

Notes:

- An interface should change state as up-down to complete one cycle of a link flap.
- The LED does not glow when an interface is in the ErrDisable state.
- ErrDisable is supported only on physical interfaces.
- A LAG interface does not go into the ErrDisable state when all of its member ports are in the ErrDisable state
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. If the accumulated link flap count reaches the maximum flap count for a particular sliding window, a link flap error disable fault is triggered.

Topology

Figure 43. ErrDisable

Automatic Recovery

By default, an interface goes into the ErrDisable state when a link flaps 5 times in 10 seconds. An interface is recovered from the ErrDisable state when the configured non-zero ErrDisable time-out interval value expires.

RTR1

`#configure terminal`	Enter configure mode.
`(config)#errdisable cause link-flap`	Enable ErrDisable due to link-flap
`(config)#errdisable link-flap-setting max-flaps 2 time 30`	Configure Link flap settings. Max link flap count and interval for linkFlap Timer
`(config)#errdisable timeout interval 50`	Configure interval to recover from error disable state
`(config)#commit`	Commit the candidate configuration to the running configuration.
`(config)#exit`	Exit interface mode

© 2026 IP Infusion Inc. Proprietary

Note: Automatic recovery timeout is disabled, if you configure `errdisable timeout interval 0`

Validation

```
#show errdisable details

 Error Disable Recovery Timeout Interval : 50 secs
 Link Flap Timer Interval : 30 secs
 Link Flaps allowed Max. count : 2

ErrDisable Cause     Status
----------------     ------
Link-Flap            Enabled
Lag-Mismatch         Disabled
Stp-Bpdu-Guard       Enabled
```

Note: Stp-Bpdu-Guard is enabled by default on the global level configuration.

```
#show interface errdisable status
Interfaces that will be enabled at the next timeout
Interface    ErrDisable Cause   Time left(secs)
---------    ----------------   ---------------
xe11         link-flap          38

#show interface brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
xe11       ETH    --     --                down     ED      10g    --       No  No
#
```

Note: Interface xe11 went into the ErrDisable state after flapping 2 times in 30 seconds.

Log Message

`Edge1-SiteX#configure terminal`	Enter configure mode.
`Edge1-SiteX(config)#logging level nsm 4`	Enable Operational log to display recovery message
`Edge1-SiteX(config)#commit`	Commit the candidate configuration to the running configuration.
`Edge1-SiteX(config)#exit`	Exit interface mode

```
2017 Sep 18 11:52:12 : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface xe11 changed state to down
(config-if)#no shut
(config-if)#2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe11 changed state to up
2017 Sep 18 11:52:15 : NSM : WARN : [VXLAN_OPR_ACCESSPORT_UP_4]: VXLAN Access port on xe11 is up
2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_ERR_DISABLE_DOWN_2]: Interface xe11 moved to errdisable
state due to link-flap
2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface xe11 changed state to down
```

Note: Interface xe11 recovered from the ErrDisable state after a 50 second time-out.

© 2026 IP Infusion Inc. Proprietary

To get the log messages displayed, change the logging level to same on the console/monitor.

Manual Recovery

An interface can be recovered manually from the Errdisable state, when configure shutdown followed by no shutdown using CLI. Shutdown will recover the interface from Errdisable state and No shutdown will make the interface up state.

RTR1

`#configure terminal`	Enter configure mode.
`(config)#errdisable cause link-flap`	Enable ErrDisable due to link-flap
`(config)#errdisable link-flap-setting max-flaps 3 time 20`	Configure Link flap settings. Max link flap count and interval for linkFlap Timer
`(config)#commit`	Commit the candidate configuration to the running configuration.
`(config)#exit`	Exit interface mode

```
#show running-config | include errdisable
errdisable cause link-flap
errdisable link-flap-setting max-flaps 3 time 20
errdisable cause stp-bpdu-guard

#show errdisable details
 Error Disable Recovery Timeout Interval : 50 secs
 Link Flap Timer Interval : 20 secs
 Link Flaps allowed Max. count : 3

ErrDisable Cause     Status
----------------     ------
Link-Flap            Enabled
Lag-Mismatch         Disabled
Stp-Bpdu-Guard       Enabled
```

Note: Interface xe11 went into the ErrDisable state after flapping 3 times in 20 seconds.

```
(config)#do show interface errdisable status
Interfaces that will be enabled at the next timeout
Interface    ErrDisable Cause   Time left(secs)
---------    ----------------   ---------------
xe11         link-flap          NA
(config)#do show int brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
xe11       ETH   --    --               down    ED      10g   --       No  No
```

Note: Interface xe11 recovered from the ErrDisable state after entering `shutdown` followed by `no shutdown`.

```
(config)#interface xe11
(config-if)#shutdown
2017 Sep 18 13:02:20 : NSM : WARN : [IFMGR_ERR_DISABLE_UP_4]: Interface xe11 recovered from link-flap
errdisable
```

```
(config-if)#no shut
(config-if)#2017 Sep 18 13:02:21 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe11 changed state to up
2017 Sep 18 13:02:21 : NSM : WARN : [VXLAN_OPR_ACCESSPORT_UP_4]: VXLAN Access port on xe11 is up

config)#do show interface errdisable
(config)#do show interface brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
(config)#
```

If you configure `no errdisable cause link-flap`, at the global level, it recovers all the interfaces from the ErrDisable state.

For transaction clients (such as NetConf), to recover a port from an error disable state manually, use this command/RPC call:

- Command: clear interface IFNAME error-disable
- NetConf RPC: interface-clear-interface-error-disable

Note: This command/RPC applies only for an error disable state caused by an administrative shutdown. For an error disable state due to peer flapping or any other reason, recover from the error disable state by entering shutdown followed by no shutdown.

ErrDisable at the Interface Level

If you enable ErrDisable globally, by default all physical interfaces enable link-flap ErrDisable. To turn off ErrDisable for an interface, configure the commands below.

`#configure terminal`	Enter configure mode.
`(config)#interface xe11`	Enter into interface level
`(config-if)#no link-flap errdisable`	Disable link-flap ErrDisable for interface
`(config)#commit`	Commit the candidate configuration to the running configuration.
`(config)#exit`	Exit interface mode

Note: If you configure “no link-flap errdisable” in interface level, either it won’t allow the interface move to ErrDisable state or it will recover interface from ErrDisable state.

Validation

```
#show run int xe11
!
interface xe11
 description *1/2 member of PO3 - Connected to IXIA 6/6*
 channel-group 3 mode active
 no link-flap errdisable
!
```

ErrDisable for Storm-Control Configuration

An interface port state becomes ErrDisable when it continuously receives BUM traffic which is discarded due to storm control settings. Consequently, the port is down and does not allow or receive any traffic. The ErrDisable state is changed either manually by shut/no shut the interface or automatically through setting timeout value.

Notes:

- An interface discards BUM traffic during the specified interval to complete one discard-hit cycle.
- The LED does not glow when an interface is in the ErrDisable state.
- ErrDisable is supported only on physical interfaces.
- A LAG interface does not go into the ErrDisable state when all of its member ports are in the ErrDisable state
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. Every 5 seconds, a discard hit count increases if there is BUM traffic being discarded in that period. If the accumulated discard hit count reaches the maximum count for a particular configurable sliding window, a storm control error disable fault is triggered.

Topology

Figure 44. ErrDisable

Automatic Recovery

By default, an interface goes into the ErrDisable state when there is 1 discard hit in 5 seconds. An interface is recovered from the ErrDisable state when the configured non-zero `errdisable time-out` interval value expires.

RTR1

`#configure terminal`	Enter configure mode.
`(config)#errdisable cause storm-control`	Enable ErrDisable due to storm-control
`(config)#errdisable storm-control discard-hit 2 time 30`	Configure Storm control settings. Max discard hit count and interval for stormControl Timer
`(config)#errdisable timeout interval 50`	Configure interval to recover from error disable state
`(config)#commit`	Commit the candidate configuration to the

© 2026 IP Infusion Inc. Proprietary

	running configuration.
`(config)#exit`	Exit interface mode

Note: Automatic recovery timeout is disabled, if you configure `errdisable timeout interval 0` .

Validation

```
#show errdisable details
Storm Control Timer Interval : 30 secs
Storm Control allowed Max. discard-hit count : 2

ErrDisable Cause     Status
----------------     ------
Link-Flap            Disabled
Storm-Control        Enabled
Lag-Mismatch         Disabled
Stp-Bpdu-Guard       Enabled
Mac-move-limit       Disabled
```

Note: Stp-Bpdu-Guard is enabled by default on the global level configuration.

```
#show interface errdisable status
Interfaces that will be enabled at the next timeout

Interface    ErrDisable Cause   Time left(secs)
---------    ----------------   ---------------
xe11         storm-control          38


#show interface brief | include ED
      ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
xe11       ETH    --     --                down     ED      10g    --       No  No
#
```

Note: Interface xe11 went into the ErrDisable state after discarding packets 2 times (5 second windows are considered) in 30 seconds.

Log Message

`Edge1-SiteX#configure terminal`	Enter configure mode.
`Edge1-SiteX(config)#logging level nsm 4`	Enable Operational log to display recovery message
`Edge1-SiteX(config)#commit`	Commit the candidate configuration to the running configuration.
`Edge1-SiteX(config)#exit`	Exit interface mode

```
2017 Sep 18 11:52:12 : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface xe11 changed state to down
```

```
(config-if)#no shut
(config-if)#2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe11 changed state to up
2017 Sep 18 11:52:15 : NSM : WARN : [VXLAN_OPR_ACCESSPORT_UP_4]: VXLAN Access port on xe11 is up
2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_ERstorm-controlR_DISABLE_DOWN_2]: Interface xe11 moved to
errdisable state due to storm-control
2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface xe11 changed state to down
```

Note: Interface xe11 recovered from the ErrDisable state after a 50 second time-out.

Manual Recovery

An interface can be recovered manually from the ErrDisable state, by executing the CLIS `shutdown` which recovers the interface from ErrDisable state, followed by `no shutdown` that brings the interface to an up state.

RTR1

`#configure terminal`	Enter configure mode.
`(config)#errdisable cause storm-control`	Enable errdisable due to storm-control
(config)#errdisable storm-control discard-hit 3 time 20	Configure Storm control settings. Max discard hit count and interval for StormControl Timer
`(config)#commit`	Commit the candidate configuration to the running configuration.
`(config)#exit`	Exit interface mode

Validation

```
#show running-config | include errdisable
errdisable cause storm-control
errdisable storm-control-setting max-flaps 3 time 20
errdisable cause stp-bpdu-guard

#show errdisable details

 Link Flap Timer Interval : 20 secs
 Link Flaps allowed Max. count : 3

ErrDisable Cause     Status
----------------     ------
Link-Flap            Disabled
Storm-Control        Enabled
Lag-Mismatch         Disabled
Stp-Bpdu-Guard       Disabled
Mac-move-limit       Disabled
```

Note: Interface xe11 went into the ErrDisable state after discarding packets 3 times (5 second windows are considered) in 20 seconds.

```
(config)#do show interface errdisable status
Interfaces that will be enabled at the next timeout
Interface    ErrDisable Cause   Time left(secs)
---------    ----------------   ---------------
```

```
xe11         storm-control          NA
(config)#do show int brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
xe11       ETH   --    --               down    ED      10g   --       No  No
```

Note: Interface xe11 recovered from the ErrDisable state after entering `shutdown` followed by `no shutdown`.

```
(config)#interface xe11
(config-if)#shutdown
2017 Sep 18 13:02:20 : NSM : WARN : [IFMGR_ERR_DISABLE_UP_4]: Interface xe11 recovered from storm-
control errdisable
(config-if)#no shut
(config-if)#2017 Sep 18 13:02:21 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe11 changed state to up
2017 Sep 18 13:02:21 : NSM : WARN : [VXLAN_OPR_ACCESSPORT_UP_4]: VXLAN Access port on xe11 is up

config)#do show interface errdisable
(config)#do show interface brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
(config)#
```

If you configure `no errdisable cause storm-control`, at the global level, it recovers all the interfaces from the ErrDisable state

Errdisable at the Interface Level

If you enable errdisable globally, by default all physical interfaces enable storm-control errdisable. To turn off errdisable for an interface, configure the commands below.

`#configure terminal`	Enter configure mode.
`(config)#interface xe11`	Enter into interface level
`(config-if)#no storm-control errdisable`	Disable storm-control errdisable for interface
`(config)#commit`	Commit the candidate configuration to the running configuration.
`(config)#exit`	Exit interface mode

Note: If you configure “no storm-control errdisable” in interface level, either it won’t allow the interface move to errdisable state or it will recover interface from errdisable state

Validation

```
#show run int xe11
!
interface xe11
 description *1/2 member of PO3 - Connected to IXIA 6/6*
 channel-group 3 mode active
 no storm-control errdisable
!
```

Sample show running-configuration output

Global level configuration

```
ocnos#
ocnos#con t
Enter configuration commands, one per line.  End with CNTL/Z.
ocnos(config)#
ocnos(config)#errdisable cause storm-control
ocnos(config)#commit
ocnos(config)#end
ocnos#
ocnos#show errdisable details

 Storm Control Timer Interval : 5 secs
 Storm Control Max. discard-hit count : 1


ErrDisable Cause          Status
----------------          ------
Link-Flap                 Disabled
Storm-Control             Enabled
Lag-Mismatch              Disabled
Stp-Bpdu-Guard            Enabled
Mac-move-limit            Disabled
ocnos#
ocnos#show running-config | include err
errdisable cause storm-control
errdisable cause stp-bpdu-guard
ocnos#

ocnos(config)#no errdisable cause storm-control
ocnos(config)#commit
ocnos(config)#end
ocnos#
ocnos#show running-config | include err
errdisable cause stp-bpdu-guard
```

Interface level configuration

```
ocnos#
ocnos(config)#
ocnos(config)#errdisable cause storm-control
ocnos(config)#commit
ocnos(config)#end
ocnos#
ocnos#
Enter configuration commands, one per line.  End with CNTL/Z.
ocnos(config)#
ocnos(config)#interface ce21
ocnos(config-if)#no in
ocnos(config-if)#no storm-control errdisable
ocnos(config-if)#commit
ocnos(config-if)#ssto
ocnos(config-if)#storm-control errdisable
ocnos(config-if)#commit
ocnos(config-if)#end
ocnos#
ocnos#
ocnos#show running-config interface ce21
!
interface ce21
storm-control errdisable
!
ocnos#
ocnos#
```

```
ocnos#
ocnos#show running-config | include err
errdisable cause storm-control
errdisable cause stp-bpdu-guard
ocnos#
ocnos#
ocnos#
ocnos#
ocnos#con t
Enter configuration commands, one per line.  End with CNTL/Z.
ocnos(config)#
ocnos(config)#no sto
ocnos(config)#no errdisable et
ocnos(config)#no errdisable cause storm-control
ocnos(config)#commit
ocnos(config)#end
ocnos#
ocnos#
ocnos#
ocnos#show running-config | include err
errdisable cause stp-bpdu-guard
ocnos#
```

Discard hit configuration

```
ocnos#
ocnos#con t
Enter configuration commands, one per line.  End with CNTL/Z.
ocnos(config)#errdisable cause storm-control
ocnos(config)#commit
ocnos(config)#end
ocnos#
ocnos#show running-config | include err
errdisable cause storm-control
errdisable cause stp-bpdu-guard
ocnos#
ocnos#con t
Enter configuration commands, one per line.  End with CNTL/Z.
ocnos(config)#errdisable storm-control discard-hit 3 time 30
ocnos(config)#commit
% Warning: Err-disable setting has being updated, previous flaps won't
be                                                                              considered
ocnos(config)#end
ocnos#
ocnos#show running-config | include err
errdisable cause storm-control
errdisable cause stp-bpdu-guard
errdisable storm-control discard-hit 3 time 30
ocnos#
ocnos#con t
Enter configuration commands, one per line.  End with CNTL/Z.
ocnos(config)#no errdisable cause storm-control
ocnos(config)#commit
ocnos(config)#end
ocnos#
ocnos#show running-config | include err
errdisable cause stp-bpdu-guard
ocnos#
```

Time interval configuration

```
ocnos#con t
Enter configuration commands, one per line.  End with CNTL/Z.
ocnos(config)#errdisable to
ocnos(config)#errdisable timeout interval 10
ocnos(config)#commit
```

```
ocnos(config)#end
ocnos#

ocnos#show running-config | include err
errdisable cause stp-bpdu-guard
errdisable timeout interval 10
ocnos#

ocnos#con t
Enter configuration commands, one per line.  End with CNTL/Z.
ocnos(config)#no errdisable timeout im
ocnos(config)#no errdisable timeout interval
ocnos(config)#commit
ocnos(config)#end
ocnos#

ocnos#show running-config | include err
errdisable cause stp-bpdu-guard
ocnos#

ocnos#con t
Enter configuration commands, one per line.  End with CNTL/Z.
ocnos(config)#errdisable timeout interval 50
ocnos(config)#commit
ocnos(config)#end
ocnos#
ocnos#show running-config | include err
errdisable cause stp-bpdu-guard
errdisable timeout interval 50
ocnos#
ocnos#con t
Enter configuration commands, one per line.  End with CNTL/Z.
ocnos(config)#
ocnos(config)#no errdisable timeout im
ocnos(config)#no errdisable timeout interval
ocnos(config)#commit
ocnos(config)#end
ocnos#
ocnos#show running-config | include err
errdisable cause stp-bpdu-guard
ocnos#
```

Support IGMP Snooping for Provider Bridge

Overview

In Layer-2 switches, multicast IP traffic is handled in the same manner as broadcast traffic and forwards frames received on one interface to all other interfaces. This creates excessive traffic on the network, and affects network performance. The Internet Group Management Protocol (IGMP) Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic. Thus, at a time only an host's membership report is relayed from a group instead of a report from each host in the group.

A Provider Bridge (PB) network is a virtual bridge Local Area Network (LAN) that comprises of Service provider bridges (SVLAN and PB) and attached LANs controlled under a single service provider administration. Provider bridges interconnect the MACs of the IEEE 802 LANs separately. This combined provider bridged network relay frames to all the connected LANs that provide customer interfaces for each service instance.

Feature Characteristics

The existing IGMP Snooping extended to support in the Provider Bridged (PB) network. The PB connects customer LANs using the switched provider network consisting of SVLAN bridges and provider edge bridges. Each customer LAN is connected to a separate service VLAN inside the provider network. Current release supports the IGMPv1/IGMPv2/IGMPv3.

The following are supported:

- Snooping entries are captured in provider bridge network
- Egress traffic from router is tagged with single SVLAN ID
- IGMP snooping feature supported only in SVLAN

Benefits

This feature enables a Provider bridging network service provider to conserve bandwidth by efficiently switching the multicast packets.

Prerequisites

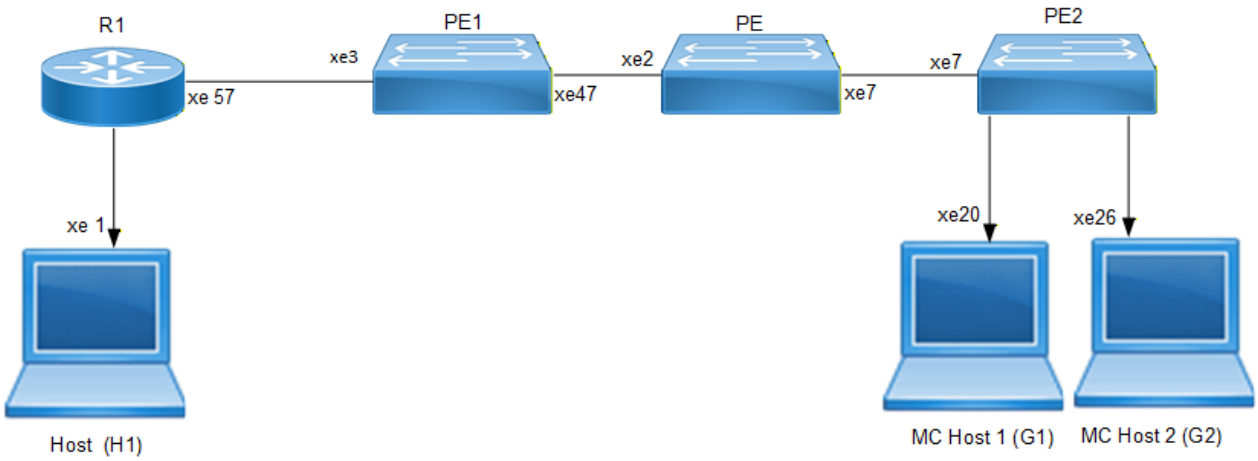
IGMP snooping is available over a number of network underlays. In this section, it is assumed that Provider Bridge support is configured.

© 2026 IP Infusion Inc. Proprietary

Configuration

Topology

Figure 45. IGMP Snooping Provider Bridge Topology



R1

`#configure terminal`	Enter the configure mode.
`R1(config)#bridge 1 protocol provider-rstp edge`	Configure bridge `1` to the spanning-tree table.
`R1(config)#vlan database`	Configure the VLAN database.
`R1(config)#vlan 2 type service point-point bridge 1 state enable`	Configure the SVLAN 2 to bridge 1.
`R1(config)#ip multicast-routing`	Configure the multicast routing on the router.
`R1(config)#ip pim rp-address 1.1.1.1`	Configure Rendezvous Point (RP) address for multicast groups.
`R1(config)#interface lo`	Enter into lo interface.
`R1(config-if)#ip address 1.1.1.1/24 secondary`	Configure rp address as secondary.
`R1(config-if)#ip pim sparse-mode`	Enable the PIM sparse mode.
`R1(config-if)#exit`	Exit the loopback interface mode.
`R1(config)#interface svlan1.2`	Create the SVLAN interface.
`R1(config-if)#ip address 20.1.1.1/24`	Configure IPv4 address to VLAN interface.
`R1(config-if)#ip pim sparse-mode`	Configure PIM sparse mode.
`R1(config-if)#exit`	Exit the SVLAN interface mode.

© 2026 IP Infusion Inc. Proprietary

R1(config)#interface xe1	Enter interface mode.
R1(config-if)#ip address 10.1.1.1/24	Configure IPv4 address to interface
R1(config-if)#ip pim sparse-mode	Configure PIM sparse mode.
R1(config-if)#commit	Commit the configurations.
R1(config-if)#exit	Exit the interface mode.
R1(config)#interface xe57	Enter interface mode.
R1(config-if)#switchport	Configure switchport.
R1(config-if)#dot1ad ethertype 0x8100	Configure ether type 0x8100.
R1(config-if)#bridge-group 1 spanning-tree disable	Configure bridge group.
R1(config-if)#switchport mode provider-network	Configure switchport trunk mode.
R1(config-if)#switchport provider-network allowed vlan add 2	Configure the VLAN to switchport trunk mode.
R1(config-if)#commit	Commit configurations

PE1

#configure terminal	Enter the configure mode.
PE1(config)#bridge 1 protocol provider-rstp edge	Configure bridge 1 to the spanning-tree table.
PE1(config)#vlan database	Configure the VLAN database.
PE1(config)#vlan 2 type service point-point bridge 1 state enable	Configure the SVLAN 2 to bridge 1.
PE1(config)#ip multicast-routing	Configure the multicast routing on the router.
PE1(config)#interface svlan1.2	Create VLAN interface.
PE1(config-if)#igmp snooping enable	Configure IPv4 address to VLAN interface .
PE1PE1(config-if)#exit	Exit the interface mode.
PE1(config)#interface xe3	Enter interface mode.
PE1(config-if)#switchport	Configure Switchport.
PE1(config-if)#dot1ad ethertype 0x8100	Configure ethertype.
PE1(config-if)#bridge-group 1 spanning-tree disable	Configure bridge group spanning tree disable .
PE1(config-if)#switchport mode provider-network	Configure provider network .
PE1(config-if)#switchport provider-network allowed vlan add 2	Configure the SVLAN to interface .
PE1(config-if)#commit	Commit configurations.

© 2026 IP Infusion Inc. Proprietary

PE1(config-if)#exit	Exit the interface mode.
PE1(config)#interface xe47	Enter interface mode.
PE1(config-if)#switchport	Configure switchport
PE1(config-if)#dot1ad ethertype 0x8100	Configure ethertype.
PE1(config-if)#bridge-group 1 spanning-tree disable	Configure bridge group spanning tree disable.
PE1(config-if)#switchport mode provider-network	Configure provider network.
PE1(config-if)#switchport provider-network allowed vlan add 2	Configure service vlan to provider network.
PE1(config-if)#commit	Commit configurations.
PE1(config-if)#exit	Exit the interface mode.

PE

#configure terminal	Enter the configure mode.
PE(config)#bridge 1 protocol provider-rstp edge	Configure bridge 1 to the spanning-tree table.
PE(config)#vlan database	Configure the VLAN database
PE(config)#vlan 2 type service point-point bridge 1 state enable	Configure the SVLAN 2 to bridge 1.
PE(config)#ip multicast-routing	Configure the multicast routing on the router.
PE(config)#interface svlan1.2	Create VLAN interface.
PE(config-if)#igmp snooping enable	Configure IPv4 address to VLAN interface.
PE(config-if)#exit	Exit the interface mode.
PE(config)#interface xe2	Enter interface mode.
PE(config-if)#switchport	Configure Switchport
PE(config-if)#dot1ad ethertype 0x8100	Configure ethertype
PE(config-if)#bridge-group 1 spanning-tree disable	Configure bridge group spanning tree disable.
PE(config-if)#switchport mode provider-network	Configure provider network.
PE(config-if)#switchport provider-network allowed vlan add 2	Configure the SVLAN to interface.
PE(config-if)#commit	Commit configurations.
PE(config-if)#exit	Exit the interface mode.
PE(config)#interface xe7	Enter interface mode.
PE(config-if)#switchport	Configure switchport.

PE(config-if)#dot1ad ethertype 0x8100	Configure ethertype.
PE(config-if)#bridge-group 1 spanning-tree disable	Configure bridge group spanning tree disable.
PE(config-if)#switchport mode provider-network	Configure provider network.
PE(config-if)#switchport provider-network allowed vlan add 2	Configure service vlan to provider network.
PE(config-if)#commit	Commit configurations.
PE(config-if)#exit	Exit the interface mode.

PE2

#configure terminal	Enter the configure mode.
PE2(config)#bridge 1 protocol provider-rstp edge	Configure bridge 1 to the spanning-tree table.
PE2(config)#vlan database	Configure the VLAN database.
PE2(config)#vlan 2 type service point-point bridge 1 state enable	Configure the SVLAN 2 to bridge 1.
PE2(config)#ip multicast-routing	Configure the multicast routing on the router.
PE2(config)#interface svlan1.2	Create VLAN interface.
PE2(config-if)#igmp snooping enable	Enable the IGMP snooping on VLAN interface.
PE2(config-if)#exit	Exit the VLAN interface mode.
PE2(config)#interface xe7	Enter interface mode.
PE2(config-if)#switchport	Configure Switchport.
PE2(config-if)#dot1ad ethertype 0x8100	Configure ethertype.
PE2(config-if)#bridge-group 1 spanning-tree disable	Configure bridge group spanning tree disable.
PE2(config-if)#switchport mode provider-network	Configure provider network.
PE2(config-if)#switchport provider-network allowed vlan add 2	Configure the SVLAN to interface.
PE2(config-if)#commit	Commit configurations.
PE2(config-if)#exit	Exit the interface mode.
PE2(config)#interface xe20	Enter interface mode.
PE2(config-if)#switchport	Configure switchport.
PE2(config-if)#dot1ad ethertype 0x8100	Configure ethertype.
PE2(config-if)#bridge-group 1 spanning-tree disable	Configure bridge group spanning tree disable.
PE2(config-if)#switchport mode provider-	Configure provider network.

network	
PE2(config-if)#switchport provider-network allowed vlan add 2	Configure service VLAN to provider network.
PE2(config-if)#commit	Commit configurations.
PE2(config-if)#exit	Exit the interface mode.
PE2(config)#interface xe22	Enter interface mode.
PE2(config-if)#switchport	Configure switchport.
PE2(config-if)#dot1ad ethertype 0x8100	Configure ethertype.
PE2(config-if)#bridge-group 1 spanning-tree disable	Configure bridge group spanning tree disable.
PE2(config-if)#switchport mode provider-network	Configure provider network.
PE2(config-if)#switchport provider-network allowed vlan add 2	Configure service VLAN to provider network.
PE2(config-if)#commit	Commit configurations.
PE2(config-if)#exit	Exit the interface mode.

Validation

R1

```
MCRTR#show ip igmp groups
IGMP Instance wide G-Recs Count is: 2
IGMP Connected Group Membership
Group Address    Interface            Uptime     Expires   State    Last Reporter
231.1.1.1        svlan1.2             00:00:12   00:04:07  Active   0.0.0.0
231.1.1.2        svlan1.2             00:00:12   00:04:07  Active   0.0.0.0
MCRTR#
MCRTR#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 2
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 231.1.1.1)
RP: 1.1.1.1
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................
FCR:

(*, 231.1.1.2)
RP: 1.1.1.1
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
```

```
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................
FCR:

MCRTR#
```

PE1

```
PEB1-7014#show igmp snooping interface
Global IGMP Snooping information
 IGMP Snooping Enabled
 IGMPv1/v2 Report suppression Enabled
 IGMPv3 Report suppression Enabled

IGMP Snooping information for svlan1.2
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression enabled
 IGMPv3 Report suppression enabled
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v2-reports: 0
 Number of v2-leaves: 0
 Number of v3-reports: 0
 Active Ports:
  xe3
  xe47
PEB1-7014#show igmp snooping groups
IGMP Instance wide G-Recs Count is: 2
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static, > - Hw Installed)
Vlan   Group/Source Address    Interface      Flags   Uptime      Expires  Last Reporter     Version
2      231.1.1.1               xe47           R    >  00:07:15    00:03:48 0.0.0.0           V3
2      231.1.1.2               xe47           R    >  00:07:15    00:03:48 0.0.0.0           V3
PEB1-7014#
```

PE

```
PB-7024#show igmp snooping interface
Global IGMP Snooping information
 IGMP Snooping Enabled
 IGMPv1/v2 Report suppression Enabled
 IGMPv3 Report suppression Enabled

IGMP Snooping information for svlan1.2
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression enabled
 IGMPv3 Report suppression enabled
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v2-reports: 0
 Number of v2-leaves: 0
 Number of v3-reports: 0
 Active Ports:
```

```
  xe7
  xe2
PB-7024#
PB-7024#show igmp snooping groups
IGMP Instance wide G-Recs Count is: 2
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static, > - Hw Installed)
Vlan   Group/Source
Address    Interface      Flags   Uptime
            Expires  Last Reporter     Version
2      231.1.1.1               xe7            R    >  00:07:15         00:03:45 20.1.1.2          V3
2      231.1.1.2               xe7            R    >  00:07:15         00:03:51 20.1.1.3          V3
PB-7024#
```

PE2

```
PEB2-7019#show igmp snooping interface
Global IGMP Snooping information
 IGMP Snooping Enabled
 IGMPv1/v2 Report suppression Disabled
 IGMPv3 Report suppression Disabled

IGMP Snooping information for svlan1.2
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression disabled
 IGMPv3 Report suppression disabled
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v2-reports: 0
 Number of v2-leaves: 0
 Number of v3-reports: 0
 Active Ports:
  xe20
  xe26
  xe7
PEB2-7019#
PEB2-7019#show igmp snooping groups
IGMP Instance wide G-Recs Count is: 2
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static, > - Hw Installed)
Vlan   Group/Source Address    Interface      Flags   Uptime  Expires  Last Reporter     Version
2      231.1.1.1               xe20           R    >  00:07:14  00:03:45 20.1.1.2          V3
2      231.1.1.2               xe26           R    >  00:07:15  00:03:51 20.1.1.3       V3
PEB2-7019#
```

Abbreviations

Table 8.

Acronym	Description
IGMP	Internet Group Management Protocol
PB	Provider Bridged
SVLAN	Service Provider VLAN

Unidirectional Link Detection Configuration

This section shows a complete configuration to enable UDLD in a simple network topology.

The purpose of Unidirectional Link Detection protocol (UDLD) is to monitor the physical links and detect when a unidirectional link exists. Upon detection user can either block the port or notify the link status based on the network administrator's configuration.

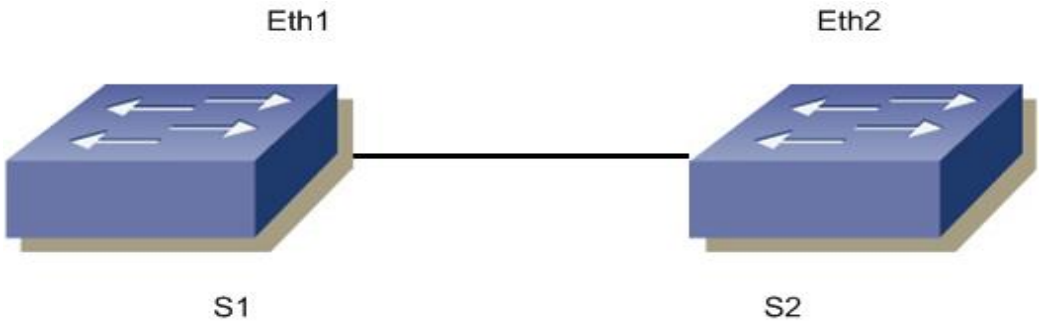
UDLD works in two different modes:

- Normal mode
- Aggressive mode

Topology

Below diagram shows the topology of the UDLD configuration.

Figure 46. UDLD Configuration



Configuration

S1

`#configure terminal`	Enter configure mode
`(config)#udld enable`	Enable UDLD globally
`(config)# udld message-time 7`	Configure message time for UDLD packets
`(config)#interface eth1`	Enter interface mode
`(config-if)#switchport`	Configure the interface as switch port
`(config-if)#udld state enable`	Enable UDLD on the interface
`(config-if)udld mode normal`	Configure udld mode as normal or aggressive
`(config-if)#commit`	Commit config.
`(config-if)#exit`	Exit from the interface mode

© 2026 IP Infusion Inc. Proprietary

S2

#configure terminal	Enter configure mode.
(config)#udld enable	Enable UDLD globally.
(config)#udld message-time 7	Configure message time for UDLD packets
(config)#interface eth2	Enter interface mode
(config-if)#switchport	Configure the interface as switch port.
(config-if)#udld state enable	Enable UDLD on the interface.
(config-if)udld mode normal	Configure udld mode as normal or aggressive
(config-if)#commit	Commit config.
(config-if)#exit	Exit from the interface mode

Validation

```
#show udld
UDLD   : Enable
Message Interval(sec) : 7

Port      UDLD Status         Mode         Link-Status
-----------------------------------------------
Eth1      Enable              Normal       Bi-directional
Eth2      Disable             Normal       Unknown
Eth3      Disable             Normal       Unknown
Eth4      Disable             Normal       Unknown
Eth5      Disable             Normal       Unknown
Eth6      Disable             Normal       Unknown
```

Once the links is made Uni-directional, the output of the command Show udld is as follows:

```
#show udld
UDLD   : Enable
Message Interval(sec) : 7

Port      UDLD Status         Mode          Link-Status
-----------------------------------------------
Eth1      Enable              Normal        Unidirectional
Eth2      Disable             Normal        Unknown
Eth3      Disable             Normal        Unknown
Eth4      Disable             Normal        Unknown
Eth5      Disable             Normal        Unknown
Eth6      Disable             Normal        Unknown


#sh running-config
udld Enable
udld message-time 7

#sh running-config in eth1
!
interface eth1
 switchport
 udld state Enable
!

#sh udld interface eth1
UDLD Status           : Enable
UDLD Mode             : Normal
Link-State            : Unknown
```

For aggressive mode, udld output is as follows:

```
#show udld
    UDLD     : Enable
    Message Interval(sec) : 7


Port      UDLD Status        Mode           Link-Status
-----------------------------------------------
eth1      Enable             Aggressive     Bi-Directional


#sh running config
udld Enable
udld message-time 7

#sh running-config in eth1
  interface eth1
switchport
```

Enable UDLD under bridge-group

S1

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol rstp`	Bridge 1 config
`(config)#udld enable`	Enable UDLD globally
`(config)#udld message-time 7`	Configure message time for UDLD packets
`(config)#commit`	Commit config.
`(config)#interface eth1`	Enter interface mode
`(config-if)#switchport`	Configure the interface as switch port
`(config-if)#bridge-group 1`	Bridge group 1
`(config-if)#udld state enable`	Enable UDLD on the interface
`(config-if)#udld mode normal`	Configure udld mode as normal or aggressive
`(config-if)#commit`	Commit config.
`(config-if)#exit`	Exit from the interface mode

S2

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol rstp`	Bridge 1 config.
`(config)#udld enable`	Enable UDLD globally.
`(config)#udld message-time 7`	Configure message time for UDLD packets
`(config)#commit`	Commit config.

© 2026 IP Infusion Inc. Proprietary

(config)#interface eth2	Enter interface mode
(config-if)#switchport	Configure the interface as switch port.
(config-if)#bridge-group 1	Bridge group 1
(config-if)#udld state enable	Enable UDLD on the interface.
(config-if)#udld mode normal	Configure udld mode as normal or aggressive
(config-if)#commit	Commit config.
(config-if)#exit	Exit from the interface mode

Validation

```
#sh running-config | i bridge 1
bridge 1 protocol rstp

#sh running-config in eth1
 interface eth1
 switchport
 bridge-group 1
 udld state Enable


#sh udld
UDLD                    : Enable
Message Interval(sec)   : 15

Port   UDLD Status    Mode           Link-Status
--------------------------------------------------
eth1    Enable         Normal     Bi-Directional
```

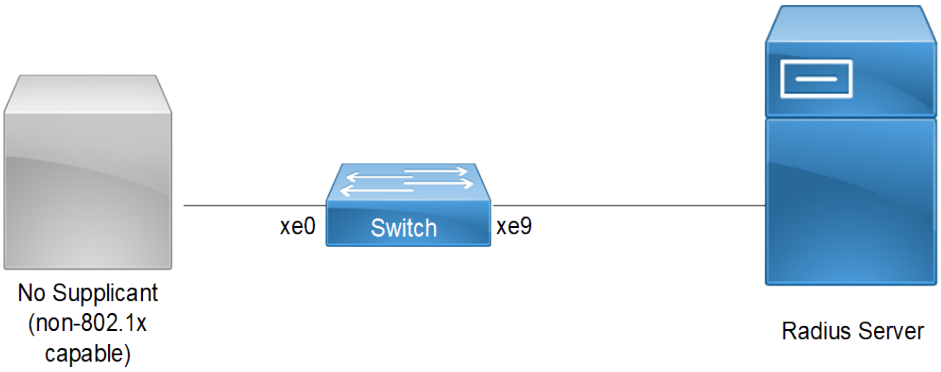
MAC Authentication Bypass

MAC Authentication Bypass (MAB) is used for a non-authenticating device (a device without an 802.1X supplicant running on it) connecting to a network with 802.1X enabled. Since there is no supplicant to answer the EAP identity requests from the authenticator (switch, wireless controller, etc.) the authenticator will generate the authentication request for the endpoint using the endpoint's MAC address as the username/password for the Access-Request message.

Note: Multicast address is not accepted for host address of radius-server.

Topology

Figure 47. MAB Topology



Configuration

Switch Configuration for MAC Authentication Bypass (MAB)

`OcNOS#configure terminal`	Enter configure mode
`OcNOS(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1
`OcNOS(config)#commit`	Commit candidate configuration to be running configuration
`OcNOS(config)#port-security disable`	Disable port security
`OcNOS(config)#dot1x system-auth-ctrl`	Enable dot1x authentication globally
`OcNOS(config)#auth-mac system-auth-ctrl`	Enable MAC authentication bypass globally
`OcNOS(config)#radius-server dot1x host 10.1.1.1 key 0 testing123`	Specify the host IP and key with string name between radius server and client.
`OcNOS(config)#commit`	Commit transaction
`OcNOS(config)#interface xe0`	Configure interface xe0

© 2026 IP Infusion Inc. Proprietary

`OcNOS(config-if)#switchport`	Enable switch port on interface.
`OcNOS(config-if)#bridge-group 1`	Associate bridge to an interface.
`OcNOS(config-if)#switchport mode access`	Configure port as access
`OcNOS(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (xe0)
`OcNOS(config-if)#dot1x mac-auth-bypass enable`	Enable MAC authentication bypass on interface
`OcNOS(config)#commit`	Commit candidate configuration to be running configuration
`OcNOS(config)#interface xe9`	Configure interface xe9
`OcNOS(config-if)#ip address 10.1.1.2/24`	Set the IP address on interface xe9
`OcNOS(config-if)#commit`	Commit transaction
`OcNOS(config-if)#end`	Exit config mode.

Validation

Verify MAB on Switch

```
Switch#show mab all
Global MAC Authentication Enabled
  RADIUS server address: 10.1.1.1:1812
  Next radius message id: 4
  RADIUS client address: not configured

MAB info for interface xe0
  Dot1x timer: Expired
  MAB Authentication Enabled
  Supplicant name: 00:07:E9:A5:3D:FA
  Status: MAC Authorized
  Last rejected MAC:
```

Configuration

MAC Authentication Configuration

`OcNOS#configure terminal`	Enter configure mode
`OcNOS(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1
`OcNOS(config)#port-security disable`	Disable port security
`OcNOS(config)#dot1x system-auth-ctrl`	Enable dot1x authentication globally
`OcNOS(config)#auth-mac system-auth-ctrl`	Enable MAC authentication bypass globally
`OcNOS(config)#radius-server dot1x host 10.1.1.1 key 0 testing123`	Specify the host IP and key with string name between radius server and client.
`OcNOS(config)#commit`	Commit transaction
`OcNOS(config)#interface xe0`	Configure interface xe0
`OcNOS(config-if)#switchport`	Enable switch port on interface.
`OcNOS(config-if)#bridge-group 1`	Associate bridge to an interface.
`OcNOS(config-if)#switchport mode access`	Configure port as access

© 2026 IP Infusion Inc. Proprietary

`OcNOS(config-if)#auth-mac enable`	Enable MAC authentication on interface
`OcNOS(config)#commit`	Commit candidate configuration to be running configuration
`OcNOS(config)#interface xe9`	Configure interface xe9
`OcNOS(config-if)#ip address 10.1.1.2/24`	Set the IP address on interface xe9
`OcNOS(config-if)#commit`	Commit transaction
`OcNOS(config-if)#end`	Exit config mode.

Note: When AUTH-MAC is enabled on the interface MAC-AUTH bypass cannot be enabled and vice-versa.

Validation

Verify MAB on Switch

```
Switch#show mab all
Global MAC Authentication Enabled
  RADIUS server address: 10.1.1.1:1812
  Next radius message id: 9
  RADIUS client address: not configured

MAB info for interface xe0
  Dot1x timer: Expired
  MAB Authentication Disabled
  Supplicant name: 00:07:E9:A5:3D:FA
  Status: MAC Authorized
  Last rejected MAC: 00:07:E9:A5:4E:25
```

© 2026 IP Infusion Inc. Proprietary

Traffic Segmentation-Protected Port

The protected port is a feature that does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. However, a protected port can communicate with an unprotected port and vice-versa.

The protected port is a feature that does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. However, a protected port can communicate with an unprotected port and vice-versa.

- Protected port(isolated) to protected port(isolated) - communication is not allowed.
- Protected port(isolated) to protected port(community) - communication is not allowed.
- Protected port(isolated) to protected port(promiscuous) - communication is allowed.
- Protected port(community) to protected port(community) - communication is allowed.
- Protected port(community) to protected port(promiscuous) - communication is allowed.
- Protected port(promiscuous) to protected port(promiscuous) - communication is allowed.
- Unprotected port to protected port(any type) - communication is allowed.

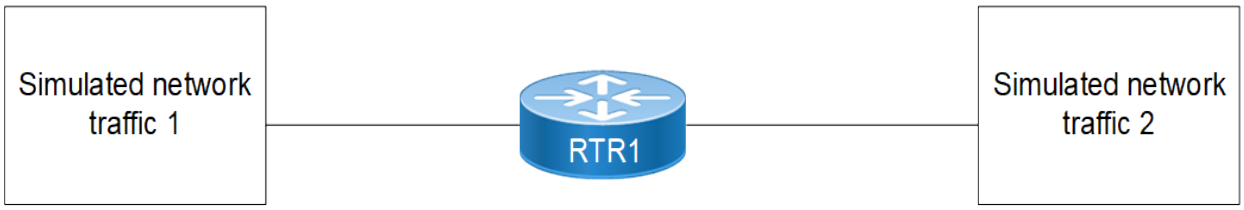
The protected port configuration is local to the switch. This information is not propagated outside the switch. Protected ports across switches can still be able to communicate with each other.

The use of protected ports ensures that there is no exchange of unicast, broadcast, or multicast data traffic between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor.

Topology

Below diagram shows Traffic Segmentation-Protected Port Topology

Figure 48. Traffic Segmentation-Protected Port Topology



Isolated-Promiscuous Configuration

RTR1

Bridge Configuration:

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge

VLAN Configuration:

`#configure terminal`	Enter configterminal mode
`(config)#vlan database`	Enter into the vlan database
`(config-vlan)# vlan 30 bridge 1 state enable`	Configure vlan 30 to bridge 1
`(config-vlan)#Exit`	Exit from the vlan database.
`(config)#int xe1`	Enter interface configuration mode for xe1
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`(config-if)#switchport trunk allowed vlan add 30`	Configure vlan 30
`(config-if)#switchport protected isolated`	Configure interface as isolated port
`(config-if)#exit`	Exit from interface
`(config)#int xe2`	Enter interface configuration mode for xe2
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`(config-if)#switchport trunk allowed vlan add 30`	Configure vlan 30
`(config-if)#switchport protected promiscuous`	Configure interface as promiscuous port
`(config-if)#exit`	Exit from interface mode
`(config)#commit`	Commit the configure on the node.

Validation

RTR1

```
#show running-config interface xe1
!
interface xe1
switchport
    switchport protected isolated
    bridge-group 1
    switchport mode trunk
    switchport trunk allowed vlan add 30
!
#show running-config interface xe2
!
interface xe2
```

```
 switchport
 switchport protected promiscuous
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 30

#show interface xe1
Interface xe1
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: 80a2.353f.edb7
  Physical:80a2.353f.edb7  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Protected Mode is Isolated
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  Bandwidth 10g
  DHCP client is disabled.
  Last Flapped: 2022 Jan 06 13:13:42 (00:24:53 ago)
  Statistics last cleared: 2022 Jan 06 13:13:42 (00:24:53 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 256 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 7 bytes 814
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 7
    Rx pause 0
  TX
    unicast packets 0 multicast packets 749 broadcast packets 0
    output packets 749 bytes 47944
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show interface xe2
Interface xe2
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: 80a2.353f.edb9
  Physical:80a2.353f.edb9  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Protected Mode is Promiscuous
  Interface index: 5003
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  Bandwidth 10g
  DHCP client is disabled.
  Last Flapped: Never
  Statistics last cleared: 2022 Jan 06 13:15:32 (00:23:52 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 4569 broadcast packets 0
    input packets 4569 bytes 327802
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
Send the vlan 30 tagged traffic from traffic 1 to traffic 2,
 #show interface counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|   Interface   |   Rx mbps   |   Rx pps   |   Tx mbps   |   Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
     Xe1     100.01     20   0.00     0
     Xe2      0.00         0    100.01   20


Send the vlan 30 tagged traffic from traffic 1 to traffic 2,
 #show interface counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|   Interface   |   Rx mbps   |   Rx pps   |   Tx mbps   |   Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
      Xe1     0.00        20    100.00     0
      Xe2     100.00      0        0.00       20
```

Isolated-Isolated Configuration

RTR1

Bridge Configuration:

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge

VLAN Configuration:

`#configure terminal`	Enter configterminal mode
`(config)#vlan database`	Enter into the vlan database
`(config-vlan)# vlan 30 bridge 1 state enable`	Configure vlan 30 to bridge 1
`(config-vlan)#Exit`	Exit from the vlan database.
`(config)#int xe1`	Enter interface configuration mode for xe1
`(config-if)#switchport`	Configure switchport

(config-if)#bridge-group 1	Associate interface with bridge-group 1
(config-if)#switchport mode trunk	Set the switching characteristics of this interface as trunk
(config-if)#switchport trunk allowed vlan add 30	Configure vlan 30
(config-if)#switchport protected isolated	Configure interface as isolated port
(config-if)#exit	Exit from interface
(config)#int xe2	Enter interface configuration mode for xe2
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Associate interface with bridge-group 1
(config-if)#switchport mode trunk	Set the switching characteristics of this interface as trunk
(config-if)#switchport trunk allowed vlan add 30	Configure vlan 30
(config-if)#switchport protected isolated	Configure interface as isolated port
(config-if)#exit	Exit from interface mode
(config)#commit	Commit the configure on the node.

Validation

RTR1

```
#show running-config interface xe1
!
interface xe1
switchport
    switchport protected isolated
    bridge-group 1
    switchport mode trunk
    switchport trunk allowed vlan add 30
!
#show running-config interface xe2
!
interface xe2
 switchport
 switchport protected isolated
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 30

#show interface xe1
Interface xe1
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: 80a2.353f.edb7
  Physical:80a2.353f.edb7  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Protected Mode is Isolated
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
```

```
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  Bandwidth 10g
  DHCP client is disabled.
  Last Flapped: 2022 Jan 06 13:13:42 (00:24:53 ago)
  Statistics last cleared: 2022 Jan 06 13:13:42 (00:24:53 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 256 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 7 bytes 814
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 7
    Rx pause 0
  TX
    unicast packets 0 multicast packets 749 broadcast packets 0
    output packets 749 bytes 47944
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show interface xe2
Interface xe2
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: 80a2.353f.edb9
  Physical:80a2.353f.edb9  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Protected Mode is Isolated
  Interface index: 5003
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  Bandwidth 10g
  DHCP client is disabled.
  Last Flapped: Never
  Statistics last cleared: 2022 Jan 06 13:15:32 (00:23:52 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 0 broadcast packets 0
    output packets 0 bytes 0
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

Send the vlan 30 tagged traffic from traffic 1 to traffic 2,
#show interface counters rate mbps
```

```
+------------------+-------------+-------------+-------------+-------------+
|   Interface   |   Rx mbps   |   Rx pps   |   Tx mbps   |   Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
     Xe1      100.01      20       0.00        0
     Xe2      0.00        0        0.00        0
```

Mirror Filtered Packets to CPU

Mirroring to CPU with filter feature provides the ability to mirror filtered data plane packets to CPU. It enables sniffing of selected packets that match the programmed filter condition and real-time monitoring in the Network Operating System.

The mirrored packets can be viewed by running `tcpdump` in Linux shell to capture runtime traffic and inspect them for troubleshooting, monitoring, and analyzing network behavior at the interface level in real-time or can be subsequently saved as PCAP files for further analysis and offline detailed examination.

Feature Characteristics

The main characteristics of Mirroring to CPU are as follows:

- Enables monitoring in the switching devices, such as leaf and spine switches.
  - Monitoring at the leaf provides visibility into north-south traffic (between endpoints and external networks or services).
  - Monitoring at the spine provides visibility into east-west traffic, i.e., between leaf switches.
- Supports one or more source interfaces and one or more VLAN sources in the ingress direction.
- Supports port-based mirroring on ingress and egress direction and filter based mirroring only on ingress direction
- Works similar to *monitor session* and supports stop or delete function.
- Overcomes the issue of latency or delay incurred on the path of mirrored traffic to reach its monitoring device while using SPAN, RSPAN, or ERSPAN.

Note: Enabling only port-based mirroring, without selecting streams using filter rules on high traffic ports starves the protocol packets.

Benefits

This feature helps to overcome the situations mentioned below:

- Latency or delay incurred on the path of mirrored traffic to reach its monitoring device.
- Reserving switch ports bandwidth for the additional mirrored traffic.
- If the port that forwards mirrored traffic is congested, the mirrored copy will not reach, impairing the monitoring ability to debug the issue.

Limitations

- This feature does not capture VXLAN-OAM packets.
- TTL and TCP flags are not supported on TR3 platforms.
- Truncation of packets is not supported on TH2 platforms.
- The BFD packets, original and mirrored, redirect to `hw-bfd` cpu-queue and are not captured in tcpdump on TH3 and TH2 devices

© 2026 IP Infusion Inc. Proprietary

Supported Hardware

The following XGS platforms are supported:

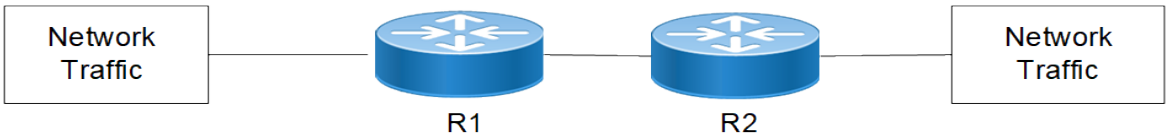
- Maverick2 (AS5835-54X)
- TR3-X7 (AS7326-56X, AS7726-32X, S9110-32X)
- TR3-X5 (S8901-54XC)
- TH2 (AS7816-64X)
- TH3 (AS9716-32D)

Configuration

Topology

A network traffic simulator device connects to routers R1 and R2 to generate and send various types of network traffic. The traffic passing through these routers are monitored real-time in the router itself.

Using the mirroring to CPU capability, sniffing is done on selective packets that match the programmed filter condition, and a copy of the packet is lifted to the CPU of the device.



Here are the configuration steps:

1. Enter configure mode and create a session for Mirror to CPU

```
R1(config)#monitor session 1 type sniff
```

2. Optionally, add sources such as `source VLAN` and/or `source interface` to the sessions. For example, the command `source interface` configures the monitored source interface and the direction of the traffic to be monitored. If not specified, both ingress and egress traffic are monitored.

```
R1(config-monitor)#source interface xe57 rx
```

3. Configure the CPU interface sniff as destination interface for ingress or egress directions.

```
R1config-monitor)#destination interface sniff
```

Packets mirrored from ingress direction are sent to `sniff0` whereas packets mirrored from egress direction are sent to `sniff1`.

4. Configure filter rules for IPv4/IPv6 packets using the filter attributes as follows:
    a. Configure DSCP for IPv4/IPv6 frame type in the range 0 to 63

```
R1(config-monitor)#filter frame-type ipv4 (dscp <0-63>
```

or

```
R1(config-monitor)#filter frame-type ipv6 (dscp <0-63>
```

    b. Configure filter rules of L2 matching parameters for L2/IPv4 packets or IPv5 packets

© 2026 IP Infusion Inc. Proprietary

```
filter vlan 2 cos 2 frametype 0x8100
dest-mac host 0044.0055.0066 src-mac host 0011.0022.0033
```

or

```
filter frame-type ipv6 cos 2 vlan 2
```

c. Configure hop limit for IPv6 frame type in the range 1 to 255

```
R1(config-monitor)#filter frame-type ipv6 (hop-limit <1-255>
```

d. Configure TTL for IPv4 frame type in the range 1 to 255

```
R1(config-monitor)#filter frame-type ipv4 (ttl <1-255>
```

e. Configure ICMP, TCP, and UDP protocols for IPv4/IPv6 frame type in the range 0 to 255

```
R1(config-monitor)#filter frame-type ipv4 (protocol (icmp | tcp | udp | <0-  255>)
```

or

```
R1(config-monitor)#filter frame-type ipv6 (next-header (icmpv6 | tcp | udp | <0-255>)
```

f. Configure ICMP type for IPv4/IPv6 frame types in the range 0 to 255

```
R1(config-monitor)#filter frame-type  ipv4 protocol icmp icmp-type <0-255>
```

or

```
R1(config-monitor)#filter frame-type  ipv6 next-header icmp icmp-type <0-255>
```

g. Configure ICMP code in the range <0-255>

```
R1(config-monitor)#filter frame-type ipv4 protocol icmp icmp-type <0-255> icmp-code <0-255>
```

or

```
R1(config-monitor)#filter frame-type ipv6 next-header icmpv6 icmp-type <0-255> icmp-code <0-255>
```

h. Configure source port with TCP and UDP protocols

```
R1(config-monitor)#filter frame-type filter frame-type ipv4 protocol udp sport <0-65535>
R1(config-monitor)#filter frame-type ipv4 protocol tcp sport <0-65535>
```

or

```
R1(config-monitor)#filter frame-type filter frame-type ipv6 next-header udp sport <0-65535>
R1(config-monitor)#filter frame-type ipv6 next-header tcp sport <0-65535>
```

i. Configure destination port with TCP and UDP protocols

```
R1(config-monitor)#filter frame-type ipv4 protocol udp dport <0-65535>
R1(config-monitor)#filter frame-type ipv4 protocol tcp dport <0-65535>
```

or

```
R1(config-monitor)#filter frame-type ipv6 next-header udp dport <0-65535>
R1(config-monitor)#filter frame-type ipv6 next-header tcp dport <0-65535>
```

j. Configure TCP flags with TCP protocol

```
R1(config-monitor)#filter frame-type ipv4 protocol tcp tcp-flags {established | urg | ack | psh | rst
| syn | fin}
```

or

```
R1(config-monitor)#filter frame-type ipv6 next-header tcp tcp-flags {established | urg | ack | psh |
rst | syn | fin}
```

5. Enable the configured session on the interface.

```
no shut
```

The packets that are enqueued in a dedicated cpu-queue `sniff` have a default rate-limits of 200 (max upto 10000 pps) assigned to them, which can be seen in the output of the following command

```
show cpu-queue details
```

You can modify the default rate-limits of cpu-queue upto 10000, using below command:

```
cpu-queue sniff rate 10000 (pps)
```

Validation

```
OcNOS#sh running-config monitor
!
monitor session 1 type sniff
 source interface xe33 rx
 destination interface sniff
 10 filter frame-type ipv4 src-ip 20.20.20.0/24
 20 filter frame-type ipv6 next-header icmpv6
 no shut

OcNOS#
OcNOS#sh monitor session all
   session 1
---------------
type              : sniff
state             : up
source intf       :
    tx            :
    rx            : xe33
    both          :
source VLANs      :
    rx            :
destination ports : sniff
sniff-truncate    : enabled
filter count      : 2

Legend: f = forwarding enabled, l = learning enabled

OcNOS#
OcNOS#sh monitor session 1
   session 1
---------------
type              : sniff
state             : up
source intf       :
    tx            :
    rx            : xe33
    both          :
source VLANs      :
    rx            :
destination ports : sniff
sniff-truncate    : enabled
filter count      : 2

Legend: f = forwarding enabled, l = learning enabled

OcNOS#
OcNOS#sh monitor session 1 filter
   session 1
---------------
filter count      : 2
```

```
  ---------------
  match set 1
  ---------------
Sequence number : 10
  frame type : ipv4
  source ip address : 20.20.20.0/24

  ---------------
  match set 2
  ---------------
Sequence number : 20
  frame type : ipv6
  next header : icmpv6


OcNOS#
OcNOS#
```

CLI Commands

The Mirror to CPU feature introduces the following configuration commands.

monitor destination sniff truncate

Use this command to enable truncation of the packets sniffed to CPU.

Use `no` form of this command to disable truncation of the packets sniffed to CPU.

Note: Truncation of packets is not supported on TH2 platforms.

Command Syntax

```
monitor destination sniff truncate
(no) monitor destination sniff truncate
```

Parameters

None

Default

When monitor session of type `sniff` is created, truncation is enabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 7.0.0.

The below commands have been revised for this feature. For more details, refer to theTraffic Mirroring Commands (page 542) section.

- Command syntax in `monitor session`
- Command syntax in `filter`

This feature also supports the existing Traffic Mirroring commands listed here:

source interface (page 557)
source vlan (page 559)

LAYER 2 COMMAND REFERENCE

Link Layer Discovery Protocol v2 Commands 395
clear lldp counters 396
clear lldp neighbors 397
lldp-agent 398
debug lldp 399
lldp run 400
lldp tlv-select 401
lldp tlv-select med 402
lldp tlv-select basic-mgmt 403
lldp tlv-select ieee-8021-org-specific 404
lldp tlv-select ieee-8023-org-specific 405
set lldp agt-circuit-id 406
set lldp chassis-id-tlv 407
set lldp chassis locally-assigned 408
set lldp disable 409
set lldp enable 410
set lldp locally-assigned 411
set lldp management-address-tlv 412
set lldp med-devtype 413
set lldp msg-tx-hold 414
set lldp port-id-tlv 415
set lldp system-description 416
set lldp system-name 417
set lldp timer 418
set lldp too-many-neighbors 420
set lldp tx-fast-init 422
set lldp tx-max-credit 423
show debugging lldp 424
show lldp neighbors 425
show lldp interface 428
snmp restart lldp 430
Port Based xConnect Commands 431
backup 432
cross-connect 433
cross-connect-switchover-type-revertive 434
disable 435
ep1ep2 436

© 2026 IP Infusion Inc. Proprietary

link-fault-pass-through enable 437
show cross-connect 438
Fundamental Layer 2 Commands 440
errdisable cause 441
errdisable link-flap-setting 442
errdisable storm-control 443
errdisable timeout 445
l2protocol all learn-disable 446
show errdisable details 447
show interface errdisable status 448
show running-config switch 449
show tcp 451
watch static-mac-movement 453
Bridge Commands 454
bridge acquire 455
bridge address 456
bridge ageing 458
bridge forward-time 459
bridge-group 460
bridge hello-time 461
bridge mac-priority-override 462
bridge max-age 464
bridge max-hops 465
bridge priority 466
bridge shutdown 467
bridge transmit-holdcount 468
bridge-group path-cost 469
bridge-group priority 470
clear allowed-ethertype 471
clear mac address-table 472
dot1ad ethertype 474
l2protocol all learn-disable 475
bridge forward-time 476
show allowed-ethertype 477
show bridge 478
show interface switchport 479
show mac address-table count bridge 481
show mac address-table bridge 483
show mac-address-table bridge 1 learning 485
switchport 486

© 2026 IP Infusion Inc. Proprietary

switchport allowed ethertype 487
Link Aggregation Commands 488
channel-group mode 489
clear lacp 491
debug lacp 492
interface po 493
interface sa 494
lacp destination-mac 495
lacp force-up 496
lacp port-priority 497
lacp system-priority 498
lacp timeout 499
port-channel load-balance 500
port-channel min-bandwidth - dynamic LAG min-bandwidth 502
port-channel min-bandwidth - static LAG min-bandwidth 503
port-channel min-links - dynamic LAG min-links 504
port-channel min-links - static LAG min-links 505
show debugging lacp 506
show etherchannel 507
show lacp-counter 510
show lacp sys-id 511
show port etherchannel 512
show static-channel-group 515
show static-channel load-balance 516
snmp restart lacp 517
static-channel-group 518
Multi-chassis Link Aggregation Commands 520
clear mcec statistics 521
debug mcec 522
domain-address 523
domain hello timeout 524
domain priority 525
domain-system-number 526
idl-higig 527
intra-domain-peer 528
mcec domain configuration 529
mlag 530
mode 531
show mcec statistics 532
show mlag detail 533

© 2026 IP Infusion Inc. Proprietary

show mlag domain ... 535
show mlag stp-synchronization status ... 538
show spanning-tree mlag operational-config ... 539
show spanning-tree mlag sync-detail ... 540
switchover type ... 541
Traffic Mirroring Commands ... 542
description ... 543
destination interface ... 544
filter ... 545
monitor session ... 547
monitor session shut ... 548
no shut ... 549
remote destination ... 550
show filter ... 551
show monitor ... 552
show monitor running configuration ... 553
show monitor session ... 554
shut ... 556
source interface ... 557
source vlan ... 559
VLAN and Private VLAN Commands ... 560
feature vlan classifier ... 562
global-bridge-vlan-check enable ... 563
private-vlan association ... 564
private-vlan community ... 565
private-vlan isolated ... 566
private-vlan primary ... 567
show dtag vlan ... 568
show vlan ... 569
show vlan access-map ... 571
show vlan brief ... 572
show vlan classifier ... 573
show vlan-reservation ... 575
switchport access ... 577
switchport hybrid ... 578
switchport mode ... 580
switchport mode access ingress-filter ... 581
switchport mode hybrid acceptable-frame-type ... 582
switchport mode hybrid ingress-filter ... 583
switchport mode private-vlan ... 584

© 2026 IP Infusion Inc. Proprietary

switchport mode trunk disable-native-vlan 585
switchport mode (trunk) disable-native-vlan 586
switchport mode trunk ingress-filter 587
switchport private-vlan association-trunk 588
switchport mode trunk ingress-filter 589
switchport private-vlan host-association 590
switchport private-vlan mapping 591
switchport trunk allowed 592
switchport trunk allowed vlan dtag 594
switchport trunk native 595
vlan classifier activate 596
vlan classifier group 597
vlan classifier rule ipv4 598
vlan classifier rule mac 599
vlan classifier rule proto 600
vlan database 602
vlan database 603
vlan VLAN_RANGE bridge 604
vlan VLAN_RANGE type customer 605
vlan VLAN_RANGE type service 606
VLAN Cross-Connect Commands 608
cross-connect 609
disable 610
outer-vlan VLAN_RANGE2 (inner-vlan VLAN_RANGE2 |) 612
show cross-connect 613
802.1x Commands 614
auth-mac 615
auth-mac dynamic-vlan-creation 616
auth-mac mac-aging 617
auth-mac mode 618
auth-mac system-auth-ctrl 619
auth-port 620
dot1x port-control 621
dot1x protocol-version 622
dot1x quiet-period 623
dot1x reauthentication 624
dot1x reauthMax 625
dot1x system-auth-ctrl 626
dot1x timeout re-authperiod 627
dot1x timeout server-timeout 628

© 2026 IP Infusion Inc. Proprietary

dot1x timeout supp-timeout 629
dot1x timeout tx-period 630
ip radius source-interface 631
key-string 632
key-string encrypted 633
radius-server dot1x host 634
retransmit 635
show debugging dot1x 636
show dot1x 637
Layer 2 Control Protocols Tunneling Commands 640
clear l2protocol interface counters 641
l2protocol 642
l2protocol encapsulation dest-mac 644
show l2protocol interface counters 646
show l2protocol processing interface 647
Provider Bridging Commands 648
bridge protocol provider-mstp 649
bridge protocol provider-rstp 650
cvlan registration table 651
cvlan svlan 652
dot1ad ethertype 654
show cvlan registration table 655
switchport customer-edge 656
switchport customer-edge hybrid 657
switchport customer-edge trunk 658
switchport customer-edge vlan registration 659
switchport customer-network allowed vlan 660
switchport customer-network vlan 661
switchport mode 662
switchport mode customer-edge 663
switchport mode customer-edge hybrid acceptable-frame-type 664
switchport provider-network 665
switchport provider-network isolated-vlan 666
vlan type 667
vlan type customer 668
Port Security Commands 669
port-security 669
show port-security 669
switchport port-security 670
switchport port-security logging 671

© 2026 IP Infusion Inc. Proprietary

switchport port-security mac-address 672
switchport port-security maximum 673
Link Layer Discovery Protocol Commands 675
lldp debug 676
lldp (disable|enable) default-agent 677
lldp ip 678
lldp run 679
lldp tlv 680
lldp tlv-select 681
set lldp chassis-id-tlv 683
set lldp disable 684
set lldp enable 685
set lldp locally-assigned 686
set lldp management-address-tlv 687
set lldp msg-tx-hold 688
set lldp timer 689
set lldp too-many-neighbors 690
show lldp 691
snmp restart lldp 692
Unidirectional Link Detection Commands 693
udld 694
udld message-time 695
udld mode 696
udld state 697
show udld 698
show udld interface 699
Spanning Tree Protocol Commands 700
bridge cisco-interoperability 702
bridge-group instance 703
bridge-group instance path-cost 704
bridge-group instance priority 705
bridge-group path-cost 706
bridge-group priority 707
bridge-group spanning-tree 708
bridge instance 709
bridge instance priority 710
bridge instance vlan 711
bridge multiple-spanning-tree 713
bridge protocol ieee 714
bridge protocol mstp 715

© 2026 IP Infusion Inc. Proprietary

bridge protocol rstp 716
bridge rapid-spanning-tree 717
bridge region 718
bridge revision 719
bridge spanning-tree 720
bridge spanning-tree errdisable-timeout 721
bridge spanning-tree force-version 722
bridge spanning-tree pathcost 723
bridge te-msti 724
bridge te-msti vlan 725
clear spanning-tree detected protocols 727
clear spanning-tree statistics 728
customer-spanning-tree customer-edge priority 729
customer-spanning-tree customer-edge path-cost 730
customer-spanning-tree hello-time 731
customer-spanning-tree max-age 732
customer-spanning-tree priority 733
customer-spanning-tree provider-edge path-cost 734
customer-spanning-tree provider-edge priority 735
customer-spanning-tree transmit-holdcount 736
debug mstp 737
show debugging mstp 739
show spanning-tree 740
show spanning-tree mst 744
show spanning-tree statistics 746
snmp restart mstp 748
spanning-tree autoedge 749
spanning-tree edgeport 750
spanning-tree guard 751
spanning-tree instance restricted-role 752
spanning-tree instance restricted-tcn 753
spanning-tree link-type 754
spanning-tree mst configuration 755
spanning-tree restricted-domain-role 756
spanning-tree restricted-role 757
spanning-tree restricted-tcn 758
spanning-tree te-msti configuration 759
Errdisable Commands 760
errdisable cause 761
errdisable link-flap-setting 763

© 2026 IP Infusion Inc. Proprietary

errdisable mac-move-limit 764
errdisable storm-control 765
errdisable timeout 767
link-flap errdisable 768
mac-move-limit priority 769
show errdisable details 770
show interface errdisable status 771
RPVST+ Commands 772
bridge-group vlan 773
bridge protocol rpvst+ 774
bridge rapid-pervlan-spanning-tree 775
bridge vlan 776
bridge vlan priority 777
show spanning-tree rpvst+ 778
spanning-tree rpvst+ configuration 782
spanning-tree vlan restricted-role 783
spanning-tree vlan restricted-tcn 784

© 2026 IP Infusion Inc. Proprietary

Link Layer Discovery Protocol v2 Commands

The commands in this section support:

- Link Layer Discovery Protocol (LLDP) version 2 as described in IEEE 802.1AB 2009
- LLDP-MED protocol extension as per ANSI/TIA-1057 April 2006.

Note: To enable LLDPv2, LLDP (previous version) should be disabled or vice versa.

clear lldp counters 396
clear lldp neighbors 397
lldp-agent 398
debug lldp 399
lldp run 400
lldp tlv-select 401
lldp tlv-select med 402
lldp tlv-select basic-mgmt 403
lldp tlv-select ieee-8021-org-specific 404
lldp tlv-select ieee-8023-org-specific 405
set lldp agt-circuit-id 406
set lldp chassis-id-tlv 407
set lldp chassis locally-assigned 408
set lldp disable 409
set lldp enable 410
set lldp locally-assigned 411
set lldp management-address-tlv 412
set lldp med-devtype 413
set lldp msg-tx-hold 414
set lldp port-id-tlv 415
set lldp system-description 416
set lldp system-name 417
set lldp timer 418
set lldp too-many-neighbors 420
set lldp tx-fast-init 422
set lldp tx-max-credit 423
show debugging lldp 424
show lldp neighbors 425
show lldp interface 428
snmp restart lldp 430

© 2026 IP Infusion Inc. Proprietary

clear lldp counters

Use this command to clear the LLDP statistics on all the interfaces.

Command Syntax

```
clear lldp counters
```

Parameters

counters
Reset the LLDP traffic counters to zero.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear lldp counters
```

© 2026 IP Infusion Inc. Proprietary

clear lldp neighbors

Use this command to clear the learned lldp neighbors information.

Command Syntax

```
clear lldp neighbors (IFNAME|)
```

Parameters

(IFNAME|)
Clears information only of this interface.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 7.0.0.

Examples

```
OcNOS#show lldp neighbors

Loc PortID        Rem Host Name         Rem Chassis Id                          Rem Port
Name      Rem Port Id                              Agent Mode
-------------------------------------------------------------------------------------------------------
-----------------------------------------------------
eth0              VN48KYC0C5            34c5.15b9.c740                          20                 2
0                                       Nearest bridge
ce5               OcNOS                 5c07.5828.4fb0                          ce5                5
c07.5828.4fb5                           Nearest bridge

OcNOS#clear lldp neighbors

OcNOS#show lldp neighbors

Loc PortID        Rem Host Name         Rem Chassis Id                          Rem Port
Name      Rem Port Id                              Agent Mode
-------------------------------------------------------------------------------------------------------
-----------------------------------------------------
```

lldp-agent

Use this command to create an LLDP agent mode.

Note: This command is not supported in SVLAN, VLAN, and loopback interfaces.

Use the `no` parameter to remove configured lldp agent mode.

Command Syntax

```
lldp-agent (non-tpmr-bridge |customer-bridge| )
no lldp-agent (non-tpmr-bridge |customer-bridge| )
```

Parameters

non-tpmr-bridge
non-tpmr-bridge

customer-bridge
customer-bridge

Default

By default LLDP agent is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent customer-bridge
(if-lldp-agent)#

(if-lldp-agent)#no lldp-agent customer-bridge
(if-lldp-agent)#exit
(config-if)#
```

© 2026 IP Infusion Inc. Proprietary

debug lldp

Use this command to set the debugging functions for LLDP.

Use the **no** form of this command to turn off LLDP debugging functions

Command Syntax

```
lldp debug (event|rx|tx|message)
no lldp debug (event|rx|tx|message)
```

Parameters

event
Enable or disable event debugging

rx
Enable or disable RX debugging

tx
Enable or disable TX debugging

message
Enable or disable NSM message debugging

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug lldp event
#debug lldp message
```

© 2026 IP Infusion Inc. Proprietary

lldp run

Use this command to start the Link Layer Discovery Protocol (LLDP)

Use the `no` form of this command to stop LLDP.

Command Syntax

```
lldp run
no lldp run
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#lldp run
(config)#no lldp run
```

lldp tlv-select

Use this command to select the set of optional TLV's to be included in the LLDP frames.

Use the `no` parameter to disable the selected set of optional TLV's.

Command Syntax

```
lldp tlv-select {basic-mgmt| ieee-8021-org-specific| ieee-8023-org-specific}
no lldp tlv-select {basic-mgmt| ieee-8021-org-specific| ieee-8023-org-specific}
```

Parameters

basic-mgmt
Basic management specific TLV.

ieee-8021-org-specific
IEEE 802.1 organizationally-specific TLV.

ieee-8023-org-specific
IEEE 803.1 organizationally-specific TLV

Default

None

Command Mode

LLDP agent mode

Applicability

This command was introduced before OcNOS version 1.3

Examples

```
#configure terminal
(config)#interface eth0
(config-if) lldp-agent
(lldp-agent)#lldp tlv-select basic-mgmt
(lldp-agent)#exit
```

© 2026 IP Infusion Inc. Proprietary

lldp tlv-select med

Use this command to select the set of optional TLV's which can enabled for transmission.

Use the `no` parameter to disable the selected set of optional TLV's.

Command Syntax

```
lldp tlv-select med (media-capabilities | network-policy| location | extended-power-via-mdi |
inventory|)
no lldp tlv-select med (media-capabilities | network-policy| location | extended-power-via-mdi |
inventory|)
```

Parameters

network-policy
Select the Network-policy as optinal TLV

media-capabilities
Select the Media-capabilities as optional TLV

location
Select the Location as optional TLV

extended-power-via-mdi
Select the extended-power-via-mdi as optional TLV, when PoE feature is available

inventory
Select the Inventory as optional TLV

Default

None

Command Mode

LLDP agent mode

Applicability

This command was introduced before OcNOS version 1.3

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(lldp-agent)#lldp tlv-select network-policy
(lldp-agent)#exit
```

© 2026 IP Infusion Inc. Proprietary

lldp tlv-select basic-mgmt

Use this command to select basic management TLVs to be include in the LLDP frames.

Use the `no` parameter to disable basic management TLVs.

Command Syntax

```
lldp tlv-select basic-mgmt (management-address|port-description|system-capabilities|system-
description|system-name)
no lldp tlv-select basic-mgmt (management-address|port-description|system-capabilities|system-
description|system-name)
```

Parameters

management-address
Management address specific TLV

port-description
Port description specific TLV

system-capabilities
System capabilities specific TLV

system-description
System Description specific TLV

system-name
System name specific TLV

Default Value

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select basic-mgmt system-name
```

© 2026 IP Infusion Inc. Proprietary

lldp tlv-select ieee-8021-org-specific

Use this command to select ieee-8021-org-specific TLVs to include in the LLDP frames.

Use the `no` parameter to disable ieee-8021-org-specific TLVs.

Command Syntax

```
lldp tlv-select ieee-8021-org-specific (link-agg|mgmt-vid|port-ptcl-vlanid|port-vlanid|ptcl-
identity|vid-digest|vlan-name)
no lldp tlv-select ieee-8021-org-specific {port-vlanid| port-ptcl-vlanid| vlan-name|ptcl-identity|
vid-digest|mgmt-vid|link-agg}
```

Parameters

link-agg
Link-aggregation TLV

mgmt-vid
Management VLAN identifier TLV

port-ptcl-vlanid
Port protocol VLAN identifier TLV

port-vlanid
Port VLAN identifier TLV

ptcl-identity
Protocol-identifier TLV

vid-digest
VLAN identifier digest TLV

vlan-name
VLAN name TLV

Default Value

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select ieee-8021-org-specific port-vlanid
```

© 2026 IP Infusion Inc. Proprietary

lldp tlv-select ieee-8023-org-specific

Use this command to select ieee-8023-org-specific TLVs to be include in LLDP frames.

Use the `no` parameter to disable ieee-8023-org-specific TLVs.

Command Syntax

```
lldp tlv-select ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
no lldp tlv-select ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
```

Parameters

mac-phy
VLAN ID Of the provider edge port <2-4094>.

power-via-mdi
Power-via-MDI (only when PoE feature is available)

max-mtu-size
Maximum MTU size TLV

Default Value

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select ieee-8023-org-specific mac-phy
```

© 2026 IP Infusion Inc. Proprietary

set lldp agt-circuit-id

Use this command to configure LLDP agt-circuit-id.

Command Syntax

```
set lldp agt-circuit-id  VALUE
```

Parameters

VALUE
Specify LLDP global agt-circuit ID.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#set lldp agt-circuit-id sample
```

© 2026 IP Infusion Inc. Proprietary

set lldp chassis-id-tlv

Use this command to set the chassis ID subtype for the LLDP agent on a port.

Use `no` form of this command to unset the chassis ID subtype.

In configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the configure mode command.

Command Syntax

```
set lldp chassis-id-tlv (if-alias | ip-address | mac-address | if-name | locally-assigned | ipv6-
address)
no set lldp chassis-id-tlv
```

Parameters

mac-address
Use the MAC address as the chassis ID.

ip-address
Use the management IP address as the chassis ID.

if-alias
Use the interface description as the chassis ID.

if-name
Use the interface name as the chassis ID.

locally-assigned
Use the locally assigned value as the chassis ID.

ipv6-address
Use the management IPv6 address as the chassis ID.

Command Mode

LLDP agent modeand Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp chassis-id-tlv ip-address
(if-lldp-agent)#no set lldp chassis-id-tlv
```

© 2026 IP Infusion Inc. Proprietary

set lldp chassis locally-assigned

Use this command to set the locally assigned chassis name for the LLDP interface.

Command Syntax

```
set lldp chassis locally-assigned NAME
```

Parameters

NAME
Name assigned to the chassis.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#set lldp chassis locally-assigned box1
```

set lldp disable

Use this command to disable the admin status of a LLDP agent on a port.

Use the `no` form of this command to unset the admin status.

Command Syntax

```
set lldp disable
no set lldp disable
```

Parameters

None

Command Mode

LLDP agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp disable
(if-lldp-agent)#no set lldp disable
(if-lldp-agent)#exit
```

© 2026 IP Infusion Inc. Proprietary

set lldp enable

Use this command to set the admin status of a LLDP agent on a port.

Use the `no` form of this command to unset the admin status.

In configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the configure mode command.

Command Syntax

```
set lldp enable (txonly|rxtx|rxonly)
no set lldp enable (txonly|rxtx|rxonly)
```

Parameters

rxonly
Receive-only

txonly
Transmit-only

txrx
Transmit and receive

Default

By default, no LLDP agent is enabled for a port.

Command Mode

LLDP agent modeand Configure mode

Applicability

This command was introduced before OcNOS version 1.3. The `no` form CLI is introduced in OcNOS version 6.6.0.

Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp enable rxonly
(if-lldp-agent)#no set lldp enable rxonly
(if-lldp-agent)#exit
```

© 2026 IP Infusion Inc. Proprietary

set lldp locally-assigned

Use this command to set the locally assigned name for LLDP interface.

Use no form of this command to remove the locally assigned name for LLDP interface.

Command Syntax

```
set lldp locally-assigned NAME
no set lldp locally-assigned NAME
```

Parameters

NAME

Name assigned to the port.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp locally-assigned port1
(config-if)#no set lldp locally-assigned
```

© 2026 IP Infusion Inc. Proprietary

set lldp management-address-tlv

Use this command to set the sub type of the Management Address TLV.

Use `no` form of this command to unset the sub type of the Management Address TLV.

In configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the configure mode command.

Command Syntax

```
set lldp management-address-tlv (mac-address | ip-address | ipv6-address)
no set lldp management-address-tlv
```

Parameters

mac-address
Use the MAC address as the Management Address.

ip-address
Use the management IP address as the Management Address.

ipv6-address
Use the management IP address as the Management Address.

Command Mode

LLDP agent modeand Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp management-address-tlv ip-address
(if-lldp-agent)#no set lldp management-address-tlv
```

© 2026 IP Infusion Inc. Proprietary

set lldp med-devtype

Use this command to configure the LLDP device type as Network-Connectivity/ End-Point Class1/ End-Point Class2/ End-Point Class3 device.

Use the `no` parameter to un set the configured LLDP device type.

Command Syntax

```
set lldp med-devtype (net-connect| ep-class1| ep-class2| ep-class3)
no lldp med-devtype (net-connect| ep-class1| ep-class2| ep-class3)
```

Parameters

net-connect
Set device type as Network-Connectivity

ep-class1
Set device type as End-Point Class1

ep-class2
Set device type as End-Point Class2

ep-class3
Set device type as End-Point Class3

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp med-devtype ep-class1
(config-if)#exit

#configure terminal
(config)#interface eth0
(config-if)#no set lldp med-devtype
(config-if)#exit
```

© 2026 IP Infusion Inc. Proprietary

set lldp msg-tx-hold

Use this command to set the `msg-tx-hold` parameter that determines the Time To Live (TTL) value for LLDPDUs to be transmitted by the port. The value set with this command is multiplied by the `lldp timer msg-tx-interval` value, which determines the final TTL value.

Use `no` form of this command to set the default value of message transmit hold.

In configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the configure mode command.

Command Syntax

```
set lldp msg-tx-hold <1-100>
no set lldp msg-tx-hold
```

Parameters

<1-100>
Time in seconds to set message transmit hold.

Default

The default value of message transmit hold is 4 seconds.

Command Mode

LLDP agent modeand Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp msg-tx-hold 3
(if-lldp-agent)#no set lldp msg-tx-hold
```

© 2026 IP Infusion Inc. Proprietary

set lldp port-id-tlv

Use this command to set the sub type of the Port ID.

Use `no` form of this command to unset the sub type of the Port ID.

In configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the configure mode command.

Command Syntax

```
set lldp port-id-tlv (if-alias | ip-address | mac-address | if-name | agt-circuit-id | locally-
assigned | ipv6-address)
no set lldp port-id-tlv
```

Parameters

mac-address
Use the MAC address as the port-id-tlv.

ip-address
Use the management IP address as the port-id-tlv

if-alias
Use the IP alias as the port-id-tlv

if-name
Use the interface name as the port-id-tlv

agt-circuit-id
Use the agt-circuit-id name as the port-id-tlv

locally-assigned
Use the locally assigned value as the port-id-tlv

ipv6-address
Use the management IP address as the port-id-tlv

Command Mode

LLDP agent modeand Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp port-id-tlv ip-address
(if-lldp-agent)#no set lldp port-id-tlv
```

© 2026 IP Infusion Inc. Proprietary

set lldp system-description

Use this command to identify the string that describes the LLDP system.

Use `no` form of this command to unset the system description.

Command Syntax

```
set lldp system-description LINE
unset lldp system-description
```

Parameters

LINE

Set the description of the LLDP system.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3

Example

```
#configure terminal
(config)#set lldp system-description LLDP agent on B1
(config)#unset lldp system-description
```

set lldp system-name

Use this command to identify the system name of the LLDP function.

Command Syntax

```
set lldp system-name NAME
unset lldp system-name
```

Parameters

NAME
Name of the LLDP system.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3

Example

```
#configure terminal
(config)#set lldp system-name LLDP1
(config)#unset lldp system-name
```

© 2026 IP Infusion Inc. Proprietary

set lldp timer

Use this command to set the interval at which LLDP frames are transmitted.

Use `no` form of this command to set the default value for timer.

In configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the configure mode command.

Command Syntax

```
set lldp timer msg-fast-tx <1-3600>
set lldp timer msg-tx-interval <5-3600>
set lldp timer reinit-delay <1-10>
no set lldp timer msg-fast-tx
no set lldp timer msg-tx-interval
no set lldp timer reinit-delay
```

Parameters

msg-fast-tx
Set the value in range <1-3600>

msg-tx-interval
Set the value in range <5-3600>

reinit-delay
Set the value in range <1-10>

Default

The default value for `msg-fast-tx` is 1 second.

The default value for `msg-tx-interval` is 30 seconds.

The default value for `reinit-delay` is 2 seconds.

Command Mode

LLDP agent modeand Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp timer msg-fast-tx 40
(if-lldp-agent)#no set lldp timer msg-fast-tx
(if-lldp-agent)#exit

#configure terminal
(config)#interface eth0
```

© 2026 IP Infusion Inc. Proprietary

```
(config-if)#lldp-agent
(if-lldp-agent)#set lldp timer msg-tx-interval 40
(if-lldp-agent)#no set lldp timer msg-tx-interval
(if-lldp-agent)#exit

#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp timer reinitDelay 3
(if-lldp-agent)#no set lldp timer reinitDelay
(if-lldp-agent)#exit
```

© 2026 IP Infusion Inc. Proprietary

set lldp too-many-neighbors

Use this command to set the action to take when the remote table is full.

Use no form of this command to unset too many neighbors parameters.

In Configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the Configure mode command.

Command Syntax

```
set lldp too-many-neighbors limit <1-65535> discard received-info timer <1-65535>
set lldp too-many-neighbors limit <1-65535> discard existing-info MAC timer <1-65535>
no set lldp too-many-neighbors limit
```

Parameters

limit
The limit on the number of LLDP neighbors.

<1-65535>
Upper limit for the number of Remote LLDP Information.

received-info
The information received for this neighbor.

timer
The period after which received information is discarded.

<1-65535>
The period in seconds after which received information is discarded.

existing-info
The information for this neighbor.

MAC
Identifies the remote LLDP Agent for which information is discarded.

timer
The period in seconds after which existing information is discarded.

<1-65535>
The period in seconds after which existing information is discarded.

Default

No upper limit is enforced for the number of remote LLDP agents.

Command Mode

LLDP agent modeand Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

© 2026 IP Infusion Inc. Proprietary

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#lldp-agent
(if-lldp-agent)#set lldp too-many-neighbors limit 20 disc existing-info 1001.1001.1001 timer 1

(config)#interface eth1
(config-if)#lldp-agent
(if-lldp-agent)#set lldp too-many-neighbors limit 1 discard received-info timer 1
```

© 2026 IP Infusion Inc. Proprietary

set lldp tx-fast-init

Use this command to determine the maximum value of LLDP frames that are transmitted during a fast transmission period.

Use `no` form of this command to set fast transmission period to default value.

In Configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the Configure mode command.

Command Syntax

```
set lldp tx-fast-init <1-8>
no set lldp tx-fast-init
```

Parameters

tx-fast-init

Set the message transmit interval value <1-8>.

Default

Default value is 4.

Command Mode

LLDP agent mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp tx-fast-init 4
(if-lldp-agent)#no set lldp tx-fast-init
(if-lldp-agent)#exit
```

© 2026 IP Infusion Inc. Proprietary

set lldp tx-max-credit

Use this command to set the maximum value of transmission credit, which signifies the number of consecutive LLDP frames transmitted.

Use `no` form of this command to set the maximum value of transmission credit to default value.

In configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the configure mode command.

Command Syntax

```
set lldp tx-max-credit <1-10>
no set lldp tx-max-credit
```

Parameters

tx-max-credit
The maximum value of transmission credit.

Default

Default value is 5

Command Mode

LLDP agent modeand Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#set lldp tx-max-credit <1-10>
(if-lldp-agent)#no set lldp tx-max-credit
(if-lldp-agent)#exit
```

© 2026 IP Infusion Inc. Proprietary

show debugging lldp

Use this command to display LLDP debugging information.

Command Syntax

```
show debugging lldp
```

Parameters

None

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following sample output displays information about an LLDP debugging.

```
#show debugging lldp
LLDP debugging status:
 LLDP message debugging is on
```

show lldp neighbors

Use this command to display LLDP neighbors information.

Command Syntax

```
show lldp (nearest-bridge| non-tpmr-bridge| customer-bridge|) neighbors (brief|details)
```

Parameters

nearest-bridge
Display LLDP nearest bridge information

non-tpmr-bridge
Display LLDP non-TPMR-bridge information

customer-bridge
Display LLDP customer-bridge information

neighbor
Neighbor

brief
Brief

details
Details

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.1.

Example

The following sample output displays information about an LLDP neighbors

```
#sh lldp nearest-bridgr neighbors brief
Loc PortID  Rem Host Name   Rem Chassis Id  Rem Port Id   Agent Mode

-------------------------------------------------------------------------------------
xe3/1               ecf4.bbfe.2864  ecf4.bbb2.4c65 Nearest bridge


#show lldp neighbors detail

-------------------------------------------------------------------------------------
Nearest bridge Neighbors
 Interface Name : xe11
 Mandatory TLVs
 Chassis id type : MAC address [8cea.1b67.236c]
 Port id type : MAC address [8cea.1b28.4f6d]
 Time to live : 121
 Basic Management TLVs
 System Name :
 System Description : Hardware Model:EC_AS5912-54X, Software version: ,1.3.1.122
```

© 2026 IP Infusion Inc. Proprietary

```
Port Description : xe11
Remote System Capabilities : Bridge Router
Capabilities Enabled : Router
Management Address : MAC Address [8cea.1b67.236c]
Interface Number subtype : ifindex
Interface Number : 10011
OID Number : 0
802.1 Org specific TLVs
Port vlan id : 0
Port & Protocol vlan id : 0
Remote Configured VLANs : None
Remote Protocols Advertised: None
Remote VID Usage Digest : 0
Remote Management Vlan : 0
Link Aggregation Capability: capable of being aggregated
Link Aggregation Status : not currently in aggregation
Link Aggregation Port ID :
802.3 Org specific TLVs
AutoNego Support : Supported
AutoNego Status : Disabled
AutoNego Capability : 16
Operational MAU Type : 54 [Four-pair Category 6A or better, full duplex mode only]
Max Frame Size : 1518
```

Table 9. show lldp neighbor output details

Entry	Description
Loc Port ID	Local interface SNMP index (appears when the interface option is used).
Rem Host Name	Name of the remote host.
Rem Chassis Id	Remote chassis identifier of the chassis type listed.
Rem Port Id	Remote port identifier of the port type listed.
Agent Mode	Agent mode enabled to the nearest bridge.
Time to live	Number of seconds for which this information is valid.
Interface Name	Name of the interface.
Chassis id type	Chassis identifier of the chassis type listed.
Port id type	Type of port identifier supplied, such as Locally assigned.
System Name	Name supplied by the system on the interface.
System Description	Description supplied by the system on the interface.
Port Description	The port description field uses the configured port description, the port name or the SNMP if Index (appears when the interface option is used).
Remote System Capabilities	Remote system capabilities (such as Bridge, Bridge Router, and Bridge Telephone) that are supported.
Capabilities Enabled	Enabled by the system on the interface (appears when the interface option is used).
Management Address	Details of management address (such as 10.204.35.34).
Interface Number subtype	Interfaces subtype for which neighbor information is available.
Interface Number	Interfaces for which neighbor information is available.

© 2026 IP Infusion Inc. Proprietary

Table 9. show lldp neighbor output details (continued)

Entry	Description
OID Number	Number of identifier.
Port VLAN ID	Details of the port VLAN identifier.
Protocol VLAN ID	Details of the protocol VLAN identifier.
Remote Configured VLANs	Details of the remote configured VLAN.
Remote Protocols Advertised	Details of the remote protocols.
Remote VID usage Digest	Details of the VID usage.
Remote Management VLAN	Details of the management VLAN.
Link Aggregation Capability	Capabilities that supported by the link aggregation on the interface.
Link Aggregation Status	Status of the link aggregation.
Link Aggregation Port ID	Details of the link aggregation port identifier.
Auto Nego Support	Support of the auto nego on the interface.
Auto Nego Status	Status of the auto nego.
Auto Nego Capability	Capabilities that supported by the auto nego on the interface.
Operational MAU Type	Type of operational MAU on the interface.
Max Frame Size	Maximum frame size on the transit.

Table 9. show lldp neighbor output details (page 426)shows the output details.

© 2026 IP Infusion Inc. Proprietary

show lldp interface

Use this command to display LLDP interface information.

Command Syntax

```
show lldp interface IFNAME (nearest-bridge| non-tpmr-bridge| customer-bridge | ) (neighbor| )
```

Parameters

IFNAME
Display LLDP interface information for all agent

nearest-bridge
Display LLDP nearest bridge information

non-TPMR-bridge
Display LLDP non-TPMR-bridge information

customer-bridge
Display LLDP customer-bridge information

neighbor
Display LLDP neighbor details.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lldp interface eth0
Agent Mode : Customer-bridge
Enable (tx/rx): N/N
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 0
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0

Agent Mode : Non-TPMR-bridge
Enable (tx/rx): N/N
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 0
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
```

© 2026 IP Infusion Inc. Proprietary

```
Total discarded TLVs: 0
Total unrecognised TLVs: 0

Agent Mode : Nearest bridge
Enable (tx/rx): Y/Y
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 2495
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0
```

Table 10. show lldp interface output details

Entry	Description
Agent Mode	Agent mode enabled to the customer-bridge, Non-TPMR-bridge, and nearest bridge.
Enable (tx/rx)	Enables the transmit and receive on the interface.
Device Type	Type of device in the networks.
LLDP Agent traffic statistics	Statistics on exchanged LLDP frames between a device and neighbors.
Total frames transmitted	Number of frames transmitted in network.
Total entries aged	Number of aged entries in a networks.
Total frames received	Number of frames received from the neighbor network.
Total frames received in error	Number of frames not received from the neighbor network.
Total discarded TLVs	Number of TLVs discarded in transit.
Total unrecognised TLVs	Number of unrecognised TLVs in transit.

Table 10. show lldp interface output details (page 429) shows the output details.

© 2026 IP Infusion Inc. Proprietary

snmp restart lldp

Use this command to restart SNMP in Link Layer Discovery Protocol (LLDP)

Command Syntax

```
snmp restart lldp
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#snmp restart lldp
```

© 2026 IP Infusion Inc. Proprietary

Port Based xConnect Commands

This chapter contains the port based xConnect commands.

backup 432
cross-connect 433
cross-connect-switchover-type-revertive 434
disable 435
ep1ep2 436
link-fault-pass-through enable 437
show cross-connect 438

© 2026 IP Infusion Inc. Proprietary

backup

Use this command to configure backup for primary endpoints. Use `no` form of this command to unconfigure backup for primary endpoint.

Command Syntax

```
backup (ep1|ep2) IFNAME
no backup (ep1|ep2)
```

Parameters

IFNAME
Interface name for backup endpoint

Default

None

Command Mode

Configure-XC mode

Applicability

This command was introduced in OcNOS-DC version 2.0.

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#backup ep1 xe35
(config-XC)#no backup ep1
```

© 2026 IP Infusion Inc. Proprietary

cross-connect

Use this command to provide name for a xConnect. This command will change mode from config to cross-connect mode.

Command Syntax

```
cross-connect <xc-name>
```

Parameters

xc-name
Cross-connect name

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-DC version 2.0

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#
```

© 2026 IP Infusion Inc. Proprietary

cross-connect-switchover-type-revertive

Use this command to configure revertive mode for cross-connect.

Use the `no` form of this command to make it non-revertive mode for cross-connect.

Command Syntax

```
cross-connect switchover type revertive
no cross-connect switchover type revertive
```

Parameters

None

Default

Non-revertive by default.

Command Mode

Configure-XC mode

Applicability

This command was introduced in OcNOS-DC version 2.0.

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#cross-connect switchover type revertive
(config-XC)#no cross-connect switchover type revertive
```

© 2026 IP Infusion Inc. Proprietary

disable

Use this command to do admin shutdown on a cross-connect.

Use the `no` form of this command to enable cross-connect.

Command Syntax

```
disable
no disable
```

Parameters

None

Default

By default, the cross-connect will be enabled.

Command Mode

Configure-XC mode

Applicability

This command was introduced in OcNOS-DC version 2.0

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#disable
(config-XC)#no disable
```

© 2026 IP Infusion Inc. Proprietary

ep1ep2

Use this command to configure xConnect between two endpoints.

Command Syntax

```
ep1 IFNAME1 ep2 IFNAME2
```

Parameters

IFNAME1
Interface name for ep1

IFNAME2
Interface name for ep2

Default

None

Command Mode

Configure-XC mode

Applicability

This command was introduced in OcNOS-DC version 2.0.

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#ep1 xe33 ep2 xe34
```

link-fault-pass-through enable

Use this command to enable LFPT in the cross-connect.

Use the `no` form of this command to disable LFPT.

Command Syntax

```
link-fault-pass-through enable
no link-fault-pass-through enable
```

Parameters

None

Default

LFPT is disabled by default.

Command Mode

Configure-XC mode

Applicability

This command was introduced in OcNOS-DC version 2.0.

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#link-fault-pass-through enable
(config-XC)#no link-fault-pass-through enable
```

© 2026 IP Infusion Inc. Proprietary

show cross-connect

Use this command to show cross-connect entry.

Command Syntax

```
show cross-connect (name WORD| count|)
```

Parameters

WORD
Cross-connect name

count
Cross-connect count

Default

None

Command Mode

Execution mode

Applicability

This command was introduced in OcNOS-DC version 2.0.

Example

```
OcNOS#sh cross-connect

Cross-connect name : temp
EP1:ce13/1     EP2:ce4/1      Revertive:No         Bkp_EP1:ce14/1     Bkp_EP2:ce15/1     Admin
Status:UP         Oper Status:UP
+=============================================================================================================
==============+
| EP        | OVID     | IVID     | Rx packets    | Rx bytes      | Tx packets    |Tx
bytes       |Interface Status|
+=============================================================================================================
==============+
| EP1*      |     -    |     -
    |177629         |12078772       |0              |0              |UP             |
| EP2*      |     -    |     -
    |0              |0              |177633         |12079044       |UP             |
| bkp_EP1   |     -    |     -
    |0              |0              |0              |0              |UP             |
| bkp_EP2   |     -    |     -
    |0              |0              |0              |0              |UP             |
+=============================================================================================================
==============+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

```
OcNOS#sh cross-connect temp

Cross-connect name : temp
EP1:ce13/1     EP2:ce4/1      Revertive:No         Bkp_EP1:ce14/1     Bkp_EP2:ce15/1     Admin
Status:UP         Oper Status:UP
+=============================================================================================================
==============+
| EP       | OVID     | IVID     | Rx packets    | Rx bytes      | Tx packets    |Tx
bytes       |Interface Status|
+=============================================================================================================
==============+
| EP1*     |     -    |     -
    |177629          |12078772       |0              |0              |UP             |
| EP2*     |     -    |     -
    |0               |0              |177633         |12079044       |UP             |
| bkp_EP1  |     -    |     -
    |0               |0              |0              |0              |UP             |
| bkp_EP2  |     -    |     -
    |0               |0              |0              |0              |UP             |
+=============================================================================================================
==============+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1

OcNOS#sh cross-connect count
cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

Fundamental Layer 2 Commands

This chapter contains fundamental Layer 2 commands.

errdisable cause 441
errdisable link-flap-setting 442
errdisable storm-control 443
errdisable timeout 445
l2protocol all learn-disable 446
show errdisable details 447
show interface errdisable status 448
show running-config switch 449
show tcp 451
watch static-mac-movement 453

© 2026 IP Infusion Inc. Proprietary

errdisable cause

Use this command to globally shut down a port when certain errors happen:

- BPDU guard puts an interface configured for Spanning Tree Protocol (STP) Port Fast into the ErrDisable state upon receipt of a STP BPDU to avoid a potential bridging loop.
- If one side of a link-access group (LAG) is configured as a static LAG and the other side as a dynamic LAG, the ports on the side receiving LACP BPDUs go into the ErrDisable state.

Notes:

- When link-flap ErrDisable is enabled globally, then all interfaces are enabled. Link-flap ErrDisable can be enabled globally, but disabled for a specific interface with the no link-flap errdisable command.
- Stp-Bpdu-Guard is enabled by default on the global level configuration.

Use `no` form of this command to not shut down a port when certain errors happen.

Command Syntax

```
errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap|storm-control}
no errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap|storm-control}
```

Parameters

stp-bpdu-guard
ErrDisable on stp-bpdu-guard

lag-mismatch
ErrDisable on lag-mismatch

link-flap
ErrDisable on link-flap

storm-control
ErrDisable on storm-control

Default

No default value is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable cause lag-mismatch
```

errdisable link-flap-setting

Use this command to configure the link-flap errdisable feature:

- An interface should change state as up-down to complete one cycle of a link flap.
- The LED does not glow when an interface is in the errdisable state.
- Errdisable is supported only on physical interfaces.
- A LAG interface does not go into the errdisable state when all of its member ports are in the errdisable state
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. If the accumulated link flap count reaches the maximum flap count for a particular sliding window, a link flap error disable fault is triggered.

Note: Any previous flapping accumulated is flushed when you execute this command.

Command Syntax

```
errdisable link-flap-setting max-flaps <1-100> time <1-1800>
```

Parameters

<1-100>
Maximum flap count

<1-1800>
Sliding window size in seconds

Default

Five flaps in ten seconds:

Maximum flap count: 5

Sliding window size: 10 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable link-flap-setting max-flaps 5 time 20
```

errdisable storm-control

Use this command to configure the storm-control errdisable. Following are the limitation:

- An interface discards BUM traffic during the specified interval to complete one discard-hit cycle.
- The LED does not glow when an interface is in the errdisable state.
- Errdisable is supported only on physical interfaces.
- A LAG interface does not go into the errdisable state when all of its member ports are in the errdisable state.
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. Every 5 seconds, a discard hit count increases if there is BUM traffic being dicarded in that period. If the accumulated discard hit count reaches the maximum count for a particular configurable sliding window, a storm control error disable fault is triggered.

Note: Any previous discard hits accumulated are flushed when you execute this command.

Command Syntax

```
errdisable storm-control discard-hit <1-100> time <1-1800>
no errdisable cause storm-control
```

Parameters

discard-hit <1-100>

The maximum number of times that BUM traffic can hit the configured bandwidth threshold in an interface within a certain time window before disabling the interface. During continuous storm control discards, this counter is increased approximately every 5 seconds. Default value is 1.

time <1-1800>

Sliding window size in seconds. The time window in seconds in which to consider storm control threshold hits for the purposes of disabling the interface if the discard-hit is overcome during that time. This value must have a minimum value of 6 times discard-hit. Default value is 5 seconds.

Default

- One hit: ten seconds
- Maximum discard hit count: 1
- Sliding window size: 5 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 6.5.1.

© 2026 IP Infusion Inc. Proprietary

Examples

```
#configure terminal
(config)#errdisable storm-control discard-hit 3 time 20
```

© 2026 IP Infusion Inc. Proprietary

errdisable timeout

Use this command to set the debugging functions for LLDP.

Use the **no** form of this command to turn off LLDP debugging functions

Command Syntax

```
errdisable timeout interval <10-1000000>
```

Parameters

<10-1000000>
Timeout interval in seconds

Default

By default, zero: timer is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable timeout interval 1000
```

© 2026 IP Infusion Inc. Proprietary

l2protocol all learn-disable

Use this command to disable MAC address learning from all Layer 2 protocol data units (BPDUs) received on the device. When configured, the device does not learn the source MAC addresses of Layer 2 control protocol packets, including xSTP, LACP, EAP, LLDP, EFM, SyncE, and ELMI, on any interface.

Notes:

- If the source MAC address of a Layer 2 BPDU has already been learned before this command is applied, it must be manually cleared by the user.
- This command is not supported on LTSW DC variants.

Use `no` form of this command to enable MAC address learning.

Command Syntax

```
l2protocol all learn-disable
no l2protocol all learn-disable
```

Parameters

None

Default

MAC address learning from Layer 2 BPDUs is enabled by default.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 7.0.0.

Examples

```
#configure terminal
(config)#Disable MAC learning from all Layer 2 BPDUs
(config)#l2protocol all learn-disable

(config)#Re-enable MAC learning (default behaviour)
(config)#no l2protocol all learn-disable
```

© 2026 IP Infusion Inc. Proprietary

show errdisable details

Use this command to display ErrDisable settings.

Command Syntax

```
show errdisable details
```

Parameters

None

Default

None

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show errdisable details
```

© 2026 IP Infusion Inc. Proprietary

show interface errdisable status

Use this command to display ErrDisable conditions for an interface.

Command Syntax

```
show interface errdisable status
```

Parameters

None

Default

None

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show interface errdisable status
ge1 lag-mismatch-errdisable
ge2 stp-bpdu-guard-errdisable
```

© 2026 IP Infusion Inc. Proprietary

show running-config switch

Use this command to display the running system switch configuration.

Command Syntax

```
show running-config switch bridge
show running-config switch dot1x
show running-config switch gmrp
show running-config switch gvrp
show running-config switch lacp
show running-config switch lmi
show running-config switch mstp
show running-config switch radius-server
show running-config switch rpsvt+
show running-config switch rstp
show running-config switch ptp
show running-config switch stp
show running-config switch synce
show running-config switch vlan
```

Parameters

bridge
Display Bridge group information.

dot1x
Display 802.1x port-based authentication information.

gmrp
Display GARP Multicast Registration Protocol (GMRP) information.

gvrp
Display GARP VLAN Registration Protocol (GVRP) information.

lacp
Display Link Aggregation Control Protocol (LACP) information.

lmi
Display Ethernet Local Management Interface Protocol (LMI) information.

mstp
Display Multiple Spanning Tree Protocol (MSTP) information.

radius-server
Display RADIUS server information.

rpvst+
Display Rapid Per-VLAN Spanning Tree (rpvst+) information.

rstp
Display Rapid Spanning Tree Protocol (RSTP) information.

ptp
Display Precision time Protocol (PTP)

stp
Display Spanning Tree Protocol (STP) information.

synce
Display synce information.

© 2026 IP Infusion Inc. Proprietary

vlan
Display values associated with a single VLAN.

Default

None

Command Mode

Privileged execution mode, Configure mode, and Route map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#show running-config switch stp
!
bridge 6 ageing-time 45
bridge 6 priority 4096
bridge 6 max-age 7
```

show tcp

Use this command to display the Transmission Control Protocol (TCP) connections details.

Command Syntax

```
show tcp
```

Parameters

None

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show tcp
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 0.0.0.0:22            0.0.0.0:*              LISTEN
tcp        0      0 127.0.0.1:25          0.0.0.0:*              LISTEN
tcp        0      1 10.12.44.1:57740      127.0.0.1:705          CLOSE_WAIT
tcp       52      0 10.12.44.21:22        10.12.7.89:705         ESTABLISHED
tcp       85      0 10.12.44.21:57742     10.12.44.21:57738      ESTABLISHED
```

Table 11. Show tcp output

Field	Description
Proto	Protocol - TCP
Recv-Q	Number of TCP packets in the Receive Queue
Send-Q	Number of TCP packets in the Send-Q
Local Address and port number	Local IP address and the port number
Foreign Address and port number	Foreign (received) IP address and the port number.
State	Current state of TCP connections: ESTABLISHED SYN_SENT SYN_RECV FIN_WAIT1 FIN_WAIT2

Table 11. Show tcp output (continued)

Field	Description
	TIME_WAIT CLOSE CLOSE_WAIT LAST_ACK LISTEN CLOSING UNKNOWN

watch static-mac-movement

Use this command to watch if any MAC movement is detected over static MAC entries for a time period. Notification will be displaying if static MAC movement happens before the timer expires.

The counters can be validated with `show interface cpu counters queue-stats` for the L2 movement queue (Tx pkts and Dropped pkts columns).

Without enabling `watch static-mac-movement`, the statistics are reflected in the `Rx EGR Port Unavail` of `show interface counters queue-drop-stats`.

For VXLAN, `watch static-mac-movement` applies to all the MAC entries learned from the remote peer (remote dynamic or static remote), as these learned MACs are installed as static MAC entries in the hardware.

Command Syntax

```
watch static-mac-movement (<1-300>|)
```

Parameters

<1-300>
Timer value in seconds.

Default

By default, the timer is 10 seconds.

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#watch static-mac-movement
```

© 2026 IP Infusion Inc. Proprietary

Bridge Commands

This section provides a description, syntax, and examples of the bridge commands. It includes the following commands:

bridge acquire 455
bridge address 456
bridge ageing 458
bridge forward-time 459
bridge-group 460
bridge hello-time 461
bridge mac-priority-override 462
bridge max-age 464
bridge max-hops 465
bridge priority 466
bridge shutdown 467
bridge transmit-holdcount 468
bridge-group path-cost 469
bridge-group priority 470
clear allowed-ethertype 471
clear mac address-table 472
dot1ad ethertype 474
l2protocol all learn-disable 475
bridge forward-time 476
show allowed-ethertype 477
show bridge 478
show interface switchport 479
show mac address-table count bridge 481
show mac address-table bridge 483
show mac-address-table bridge 1 learning 485
switchport 486
switchport allowed ethertype 487

© 2026 IP Infusion Inc. Proprietary

bridge acquire

Use this command to enable a bridge to learn station location information for an instance. This helps in making forwarding decisions.

Use the `no` parameter with this command to disable learning.

Note: OcNOS supports only configuration of a single bridge.

Command Syntax

```
bridge <1-32> acquire
no bridge <1-32> acquire
```

Parameter

<1-32>
Bridge group ID.

Default

Enabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 acquire
(config)#no bridge 3 acquire
```

© 2026 IP Infusion Inc. Proprietary

bridge address

Use this command to add a static forwarding table entry for the bridge.

Use the no parameter with this command to remove the entry for the bridge

Note: Forward MAC must refer to the source MAC, and discard MAC must refer to the destination MAC.

Command Syntax

```
bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME
bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME vlan <2-4094>
bridge <1-32> address XXXX.XXXX.XXXX  (forward|discard) IFNAME vlan <2-4094> svlan <2-4094>
no bridge <1-32> address XXXX.XXXX.XXXX
no bridge <1-32> address XXXX.XXXX.XXXX vlan <2-4094>
no bridge <1-32> address XXXX.XXXX.XXXX vlan <2-4094> svlan <2-4094>
```

Parameters

<1-32>
Bridge identifier

XXXX.XXXX.XXXX
Media Access Control (MAC) address in HHHH.HHHH.HHHH format.

forward
Forward matching frames.

discard
Discard matching frames.

IFNAME
Interface on which the frame comes out.

vlan
Identity of the VLAN in the range of <2-4094>.

svlan
Identity of the SVLAN in the range of <2-4094>.

Default

By default, bridge address is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

© 2026 IP Infusion Inc. Proprietary

Example

```
#configure terminal
(config)#bridge 1 address 0000.000a.0021 forward eth0
(config)#no bridge 1 address 0000.000a.0021
(config)#bridge 1 address 0011.2222.3333 forward xe5 vlan 23
(config)#no bridge 1 address 0011.2222.3333 vlan 23
(config)#bridge 1 address 0011.2222.3333 forward xe5 vlan 11 svlan 21
(config)#no bridge 1 address 0011.2222.3333 vlan 11 svlan 21
(config)#bridge 1 address 0011.2222.3334 discard xe6 vlan 12 svlan 22
(config)#no bridge 1 address 0011.2222.3334 vlan 12 svlan 22
```

© 2026 IP Infusion Inc. Proprietary

bridge ageing

Use this command to specify the aging time for a learned MAC address. A learned MAC address persists until this specified time.

Notes:

- On XGS devices, it takes up to two ageing cycles to remove the mac entry from hardware, hence the timeout will be anywhere between mac-ageing-time to two times the mac-ageing-time. For example, if the MAC ageing time is set to 100 seconds, MAC ageing can happen anywhere between 100 to 199 seconds.
- The bridge aging time affects the ARP entries which are dependent upon the MAC addresses in hardware. If a MAC address ages out, it causes the corresponding ARP entry to refresh.

Use the `no` form of this command to set the MAC address aging time to its default (300).

Command Syntax

```
bridge <1-32> ageing-time (0|<10-572>)
bridge <1-32> ageing disable
no bridge <1-32> ageing-time
```

Parameters

0
Disable Ageing Time

<1-32>
Bridge group ID.

<10-572>
Aging time in seconds.

disable
Turn off MAC address aging completely.

Default

300 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 ageing-time 100
(config)#no bridge 3 ageing-time
```

© 2026 IP Infusion Inc. Proprietary

bridge forward-time

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances.

Use the `no` parameter with this command to restore the default value of 15 seconds.

Command Syntax

```
bridge <1-32> forward-time <4-30>
no bridge <1-32> forward-time
```

Parameters

<1-32>
Specify the bridge group ID.

<4-30>
Specify the forwarding time delay in seconds.

Note: Care should be exercised if the value is to be made below 7 seconds.

Default

15 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 forward-time 6
(config)#no bridge 3 forward-time
```

bridge-group

Use this command to bind an interface with a bridge specified by the parameter.

Use the `no` parameter with this command to disable this command.

Command Syntax

```
bridge-group (<1-32>)
no bridge-group (<1-32>)
```

Parameters

<1-32>
Specify the bridge group ID.

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 2

(config)#interface eth1
(config-if)#no bridge-group 2
```

© 2026 IP Infusion Inc. Proprietary

bridge hello-time

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). A very low value of this parameter leads to excessive traffic on the network, while a higher value delays the detection of topology change.This value is used by all instances.

Configure the bridge instance name before using this command. The allowable range of values is 1-10 seconds. However, make sure that the value of hello time is always greater than the value of hold time (2 seconds by default).

Use the `no` parameter to restore the default value of the hello time.

Notes: A Bridge enforces the following relationships for Hello-time, Max-age and Forward-delay.

- 2 × (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
- Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds).
- Hello-time is allowed only on RSTP, IEEE and Provider-RSTP types of bridges. For MSTP and Provider-MSTP hello timer is restricted.

Command Syntax

```
bridge <1-32> hello-time <1-10>
no bridge <1-32> hello-time
```

Parameters

<1-32>
Specify the bridge group ID.

<1-10>
Specify the hello BPDU interval in seconds.

Default

2 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 3 hello-time 3

(config)#no bridge 3 hello-time
```

bridge mac-priority-override

Use this command to set a MAC priority override.

Use the **no** parameter with this command to unset a MAC priority override.

Command Syntax

```
bridge <1-32> mac-priority-override mac-address MAC interface IFNAME vlan VLANID (static|static-
priority-override|static-mgmt|static-mgmt-priority-overide) priority <0-7>
no bridge <1-32> mac-priority-override mac-address MAC interface IFNAME vlan VLANID
```

Parameters

<1-32>
Specify the bridge group ID.

mac-address
Enter a MAC address in HHHH.HHHH.HHHH format.

interface
Interface information.

vlan
Add the values associated with a single VLAN

static
The MAC is a static entry

static-mgmt
The MAC is a Static Management

static-mgmt-priority-overide
The MAC is a Static Management with priority override

static-priority-override
The MAC is a static with priority override

priority
priority <0-7> priority value

Default

Not Specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 1 mac-priority-override mac-address 1111.1111.1111 interface eth1 vlan 2 static
priority 2
```

© 2026 IP Infusion Inc. Proprietary

```
(config)#no bridge 1 mac-priority-override mac-address 1111.1111.1111 interface eth1 vlan 2
```

bridge max-age

Use this command to set the maximum age for a bridge. This value is used by all instances.

Maximum age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of maximum age should be greater than twice the value of hello time plus 1, but less than twice the value of forward delay minus 1. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the maximum age.

Use the `no` parameter with this command to restore the default value of the maximum age.

Notes: A Bridge shall enforce the following relationships for Hello-time, Max-age and Forward-delay.

- 2 × (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
- Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds)

Command Syntax

```
bridge <1-32> max-age <6-40>
no bridge <1-32> max-age
```

Parameters

<1-32>
Specify the bridge group ID.

<6-40>
Specify the maximum time, in seconds, to listen for the root bridge <6-40>.

Default

20 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 max-age 12

(config)#no bridge 2 max-age
```

© 2026 IP Infusion Inc. Proprietary

bridge max-hops

Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST. Specifying the maximum hops for a BPDU prevents the messages from looping indefinitely in the network. When a bridge receives an MST BPDU that has exceeded the allowed maximum hops, it discards the BPDU.

Use the `no` parameter with this command to restore the default value.

Command Syntax

```
bridge <1-32> max-hops <1-40>
no bridge <1-32> max-hops
```

Parameters

<1-32>
Specify the bridge-group ID.

<1-40>
Specify the maximum hops for which the BPDU will be valid <1-40>.

Default

In an MST region are 20

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 3 max-hops 25

#configure terminal
(config)#no bridge 3 max-hops
```

© 2026 IP Infusion Inc. Proprietary

bridge priority

Use this command to set the bridge priority for the common instance. Using a lower priority indicates a greater likelihood of the bridge becoming root. The priority values can be set only in increments of 4096.

Use the no form of the command to reset it to the default value.

Command Syntax

```
bridge (<1-32> | ) priority <0-61440>
no bridge (<1-32> | )priority
```

Parameters

<1-32>
Specify the bridge group ID.

<0-61440>
Specify the bridge priority in the range of <0-61440>.

Default

32768 (or hex 0x8000)

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 priority 4096

(config)#no bridge 2 priority
```

© 2026 IP Infusion Inc. Proprietary

bridge shutdown

Use this command to disable a bridge.

Use the `no` parameter to reset the bridge.

Command Syntax

```
bridge shutdown <1-32>
bridge shutdown <1-32> ((bridge-blocked|bridge-forward)|)
no bridge shutdown <1-32>
```

Parameters

<1-32>
Specify the bridge group ID.

bridge-forward
Put all ports of the bridge into forwarding state

bridge-blocked
Put all ports of the bridge into blocked state

Default

Not Specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge shutdown 4
(config)#no bridge shutdown 4
```

© 2026 IP Infusion Inc. Proprietary

bridge transmit-holdcount

Use this command to set the maximum number of transmissions of BPDUs by the transmit state machine.

Use the `no` parameter with this command to restore the default transmit hold-count value.

Command Syntax

```
bridge <1-32> transmit-holdcount <1-10>
no bridge <1-32> transmit-holdcount
```

Parameters

<1-32>
Specify the bridge group ID.

<1-10>
Transmit hold-count value.

Default

6

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 transmit-holdcount 5

(config)#no bridge 1 transmit-holdcount
```

© 2026 IP Infusion Inc. Proprietary

bridge-group path-cost

Use this command to set the cost of a path associated with a bridge group. The lower the path cost, the greater the likelihood of the bridge becoming root.

Use the no parameter with this command to restore the default priority value.

Command Syntax

```
bridge-group <1-32> path-cost <1-200000000>
no bridge-group <1-32> path-cost
```

Parameters

<1-32>
Specify the bridge group ID.

path-cost
Specify the path-cost of a port.

<1-200000000>
Specify the cost to be assigned to the group.

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 3 path-cost 123

(config-if)#no bridge-group 3 path-cost
```

© 2026 IP Infusion Inc. Proprietary

bridge-group priority

Use this command to set the port priority for a bridge. A lower priority indicates a greater likelihood of the bridge becoming root.

Command Syntax

```
bridge-group <1-32> priority <0-240>
no bridge-group <1-32> priority
```

Parameters

<1-32>
Specify the bridge group ID.

<0-240>
Specify the port priority range (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 4 priority 96

(config)#interface eth1
(config-if)#no bridge-group 4 priority
```

© 2026 IP Infusion Inc. Proprietary

clear allowed-ethertype

Use this command to clear statistics for each ethertype per interfaces.

Command Syntax

```
clear allowed-ethertype statistics (IFNAME|)
```

Parameters

IFNAME
Interface name.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

#clear allowed-ethertype statistics xe54/1

```
#clear allowed-ethertype statistics xe54/1

#show allowed-ethertype statistics xe54/1
Interface xe54/1
arp: 0 Packets, 0 Bytes
ipv4: 0 Packets, 0 Bytes
ipv6: 0 Packets, 0 Bytes
dropped: 0 Packets, 0 Bytes
```

© 2026 IP Infusion Inc. Proprietary

clear mac address-table

Use this command to clear the filtering database for the bridge. This command can be issued to do the following:

- clear the filtering database
- clear all filtering database entries configured through CLI (static)
- clear all multicast filtering database entries
- clear all multicast filtering database entries for a given VLAN or interface
- clear all static or multicast database entries based on a mac address

Command Syntax

```
clear mac address-table (dynamic|multicast) bridge <1-32>
clear mac address-table (dynamic|multicast) (address MACADDR | interface IFNAME | vlan VID ) bridge
<1-32>
clear mac address-table (dynamic|multicast) (address MACADDR | interface IFNAME | vlan VID )
(instance INST) bridge <1-32>
```

Parameters

dynamic
Clears all dynamic entries.

multicast
Clears all multicast filtering database entries.

address
Clear the specified MAC Address.

MACADDR
When filtering database, entries are cleared based on the MAC address.

bridge
Clears the bridge group ID. Value range is 1-32.

bridge
Clears the bridge group ID. Value range is 1-32.

interface
Clears all MAC address for the specified interface.

bridge
Clears the bridge group ID. Value range is 1-32.

instance
Clears MSTP instance ID. Value range is <1-63>.

vlan
Clears all MAC address for the specified VLAN. Value range is 1-4094.

bridge
Clears the bridge group ID. Value range is 1-32.

Command Mode

Privileged execution mode

© 2026 IP Infusion Inc. Proprietary

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to clear multicast filtering database entries:

```
#clear mac address-table multicast bridge 1
```

This example shows how to clear multicast filtering database entries for a given VLAN.

```
#clear mac address-table multicast vlan 2 bridge 1
```

This example shows how to clear all filtering database entries learned through bridge operation for a given MAC address.

```
#clear mac address-table dynamic address 0202.0202.0202 bridge 1
```

© 2026 IP Infusion Inc. Proprietary

dot1ad ethertype

Use this command to change the TPID for a port.

Use the no form of this command to set the TPID to its default value.

Command Syntax

```
dot1ad ethertype (0x8100 | 0x88a8 | 0x9100 | 0x9200)
no dot1ad ethertype
```

Parameters

0x8100
IEEE 802.1Q VLAN-tagged frame

0x88a8
IEEE 802.1ad Provider Bridging Service VLAN tag identifier (S-Tag)

0x9100
Supported for interoperability with legacy devices

0x9200
Supported for interoperability with legacy devices

Default

8100

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
(config)#interface xe1
(config-if)#dot1ad ethertype 0x9100
(config-if)#exit
(config)#interface xe1
(config-if)#no dot1ad ethertype
(config-if)#exit
```

© 2026 IP Infusion Inc. Proprietary

l2protocol all learn-disable

Use this command to disable MAC address learning from all Layer 2 protocol data units (BPDUs) received on the device. When configured, the device does not learn the source MAC addresses of Layer 2 control protocol packets, including xSTP, LACP, EAP, LLDP, EFM, SyncE, and ELMI, on any interface.

Note: If the source MAC address of a Layer 2 BPDU has already been learned before this command is applied, it must be manually cleared by the user.

Use `no` form of this command to enable MAC address learning.

Command Syntax

```
l2protocol all learn-disable
no l2protocol all learn-disable
```

Parameters

None

Default

Enabled

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.5.4.

Examples

Disable MAC learning from all Layer 2 BPDUs

```
#configure terminal
(config)#l2protocol all learn-disable
Re-enable MAC learning (default behavior)
(config)#no l2protocol all learn-disable
```

bridge forward-time

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances.

Use the **no** parameter with this command to restore the default value of 15 seconds.

Command Syntax

```
bridge <1-32> forward-time <4-30>
no bridge <1-32> forward-time
```

Parameters

<1-32>
Specify the bridge group ID.

<4-30>
Specify the forwarding time delay in seconds.

Note: Care should be exercised if the value is to be made below 7 seconds.

Default

15 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 forward-time 6
(config)#no bridge 3 forward-time
```

show allowed-ethertype

Use this command to show allowed and denied traffic statistics.

Note: Dropped slow protocol packets provides the count of slow protocol packets among the total dropped count. Total drop count is fetched from hardware and slow protocol packet count is fetched from software. Hence there can be one or two packet difference.

Command Syntax

```
show allowed-ethertype statistics (IFNAME|)
```

Parameters

IFNAME
Interface name.

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show allowed-ethertype statistics
Interface po1
arp : 0 Packets, 0 Bytes
ipv4 : 511016709 Packets, 184897169366 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 220 Packets, 28160 Bytes
dropped slow protocol pkts : lacp 220, efm 0, others 0
Interface xe47
arp : 0 Packets, 0 Bytes
ipv4 : 169763534 Packets, 61427990740 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 0 Packets, 0 Bytes
Interface xe48
arp : 0 Packets, 0 Bytes
ipv4 : 0 Packets, 0 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 0 Packets, 0 Bytes
```

© 2026 IP Infusion Inc. Proprietary

show bridge

Use this command to display the filtering database for the bridge. The filtering database is used by a switch to store the MAC addresses that have been learned and which ports that MAC address was learned on.

Command Syntax

```
show bridge (ieee|rpvst+|mstp|)
```

Parameters

ieee
STP bridges.

rpvst+
RPVST+ bridges.

mstp
MSTP bridges.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   eth1        5254.0029.929c    1     0
 1         2                   eth1        5254.004c.dcc6    1     297
 1         1                   eth1        5254.004c.dcc6    1     291
```

The table explains the show command output fields.

Table 12. show bridge output fields

Field	Description
Bridge	Bridge identifier.
VLAN, SVLAN, BVLAN	CVLAN, SVLAN, and BVLAN identifiers.
Port	Interface name.
MAC Address	Learned MAC address.
FWD	Whether frames for the MAC addresses are forwarded.
Time-out	How long the learned MAC address persists.

© 2026 IP Infusion Inc. Proprietary

show interface switchport

Use this command to display the characteristics of the interface with the current VLAN.

Command Syntax

```
show interface switchport bridge <1-32>
```

Parameter

bridge
Bridge name.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is an output of this command displaying the characteristics of this interface on bridge 2.

```
#show interface switchport bridge 2
 Interface name         : eth5
 Switchport mode        : access
 Ingress filter         : disable
 Acceptable frame types : all
 Vid swap               : disable
 Default vlan           : 2
 Configured vlans       :    2
 Interface name         : eth4
 Switchport mode        : access
 Ingress filter         : disable
 Acceptable frame types : all
 Vid swap               : disable
 Default vlan           : 1
 Configured vlans       :    1
```

The table explains the show command output fields.

Table 13. show interface switchport output fields

Field	Description
Interface name	Display the name of interface.
Switchport mode	Port that used to connect between switches and access port.
Ingress filter	Ingress filtering examines all inbound packets and then permits or denies entry to the network.
Acceptable frame types	Type of acceptable frame in the interface.

© 2026 IP Infusion Inc. Proprietary

Table 13. show interface switchport output fields (continued)

Field	Description
VID swap	Displays the status of the VID swap.
Default vlan	Default value for the VLAN.
Configured vlans	Displays the information on configured VLANs.

show mac address-table count bridge

Use this command to display a count of MAC entries from the filtering database.

Command Syntax

```
show mac address-table (local|remote|) count bridge <1-32> ({(dynamic | multicast | static) | address
MAC | interface IFNAME | vlan <1-4094> }|)
```

Parameter

local
Local dynamic FDB entries

remote
Remote dynamic FDB entries

<1-32>
Bridge group

dynamic
Dynamic entries

multicast
Multicast entries

static
Static entries

MAC
MAC address in HHHH.HHHH.HHHH format

IFNAME
Name of the interface

<1-4094>
VLAN identifier

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac address-table count bridge 1
MAC Entries for all vlans:
Total MAC Addresses in Use: 3
```

The table explains the show command output fields.

© 2026 IP Infusion Inc. Proprietary

Table 14. show mac address-table count output fields

Field	Description
Multicast MAC Address Count	Number of multicast addresses.
Total MAC Addresses	Total number of addresses.

show mac address-table bridge

Use this command to display MAC entries from the filtering database.

Command Syntax

```
show mac address-table (local|remote|) bridge <1-32> ({(dynamic | multicast | static) | address MAC |
interface IFNAME | vlan <1-4094> }|)
```

Parameter

local
MAC entries learned locally

remote
MAC entries learned from MLAG MAC sync

<1-32>
Bridge group

dynamic
Dynamic entries

multicast
Multicast entries

static
Static entries

MAC
MAC address in HHHH.HHHH.HHHH format

IFNAME
Name of the interface

<1-4094>
VLAN identifier

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac address-table bridge 1 static interface ge14
 VLAN     MAC Address     Type      Ports
  ------+---------------+---------+---------+--------------
  1      3333.3333.3333   static    ge14

#show mac address-table bridge 1
 VLAN     MAC Address     Type      Ports
  ------+---------------+---------+---------+--------------
  1      3417.ebf6.0ace   dynamic   po1
  1      6400.6a8e.48ab   dynamic   po1
```

© 2026 IP Infusion Inc. Proprietary

```
1      a82b.b5b5.c37b   dynamic   po1
200    0000.5e00.0101   dynamic   po1
200    3417.ebf6.0ac5   dynamic   po1
200    3417.ebf6.0ace   dynamic   po1
200    6400.6a8e.48ab   dynamic   po1
200    a82b.b5b5.c375   dynamic   po1
200    a82b.b5b5.c37b   dynamic   po1
800    0000.5e00.0102   dynamic   po1
800    3417.ebf6.0ac5   dynamic   po1
800    3417.ebf6.0ace   dynamic   po1
800    6400.6a8e.48ab   dynamic   po1
800    a82b.b5b5.c375   dynamic   po1
800    a82b.b5b5.c37b   dynamic   po1
```

The table explains the show command output fields.

Table 15. show mac address-table output fields

Field	Description
VLAN	VLAN identifier.
MAC Address	Media Access Control address.
Type	Dynamic, multicast, or static.
Ports	Interface name.

show mac-address-table bridge 1 learning

Use this command to display if we have disabled mac learning in any of the interfaces.

Command Syntax

```
show mac-address-table bridge <1-32> learning
```

Parameter

<1-32>
Bridge group

Learning
mac learning

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#no mac-address-table learning bridge 1 ?

interface     Interface
vlan              range(s): 2-5 10 or 2-5 7-19
OcNOS(config)#no mac-address-table learning bridge 1 interface xe1/1
OcNOS#show mac-address-table bridge 1 learning
!
no mac-address-table learning bridge 1 interface xe1/1
!
```

© 2026 IP Infusion Inc. Proprietary

switchport

Use this command to set the mode of an interface to switched.

All interfaces are configured routed by default. To change the behavior of an interface from switched to routed, you must explicitly give the no switchport command.

Note: When you change the mode of an interface from switched to routed and vice-versa, all configurations for that interface are erased.

Use the `no` form of this command to set the mode to routed.

Command Syntax

```
switchport
no switchport
```

Parameters

None

Default

All interfaces are configured routed by default. To change the behavior of an interface from switched to routed, you must explicitly give the no switchport command.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport

(config)#interface eth0
(config-if)#no switchport
```

switchport allowed ethertype

Use this command to allow a set of ethertype on the access port and deny remaining traffic.

Use the no command to remove ethertype configuration.

Command Syntax

```
switchport allowed ethertype {arp|ipv4|ipv6|mpls|WORD|log}
no switchport allowed ethertype ({arp|ipv4|ipv6|mpls|WORD|log}|)
```

Parameters

arp
Ethertype 0x0806.

ipv4
Ethertype 0x0800.

ipv6
Ethertype 0x086dd.

mpls
Ethertype 0x8847.

WORD
Any Ethertype value (0x600 - 0xFFFF).

log
Log unwanted ethertype packets.

Default

Not specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport allowed ethertype arp ipv4 ipv6 log

(config-if)#no switchport allowed ethertype ipv4
```

© 2026 IP Infusion Inc. Proprietary

Link Aggregation Commands

This section describes link aggregation commands.

channel-group mode 489
clear lacp 491
debug lacp 492
interface po 493
interface sa 494
lacp destination-mac 495
lacp force-up 496
lacp port-priority 497
lacp system-priority 498
lacp timeout 499
port-channel load-balance 500
port-channel min-bandwidth - dynamic LAG min-bandwidth 502
port-channel min-bandwidth - static LAG min-bandwidth 503
port-channel min-links - dynamic LAG min-links 504
port-channel min-links - static LAG min-links 505
show debugging lacp 506
show etherchannel 507
show lacp-counter 510
show lacp sys-id 511
show port etherchannel 512
show static-channel-group 515
show static-channel load-balance 516
snmp restart lacp 517
static-channel-group 518

© 2026 IP Infusion Inc. Proprietary

channel-group mode

Use this command to add an interface to an existing link aggregation group.

After you execute this command, the interface loses its properties and takes the properties of the aggregated interface.

Use the `no` parameter of this command to remove an interface from a dynamic link aggregation group. When you remove an interface from a LAG, the interface acquires the default interface properties.

Command Syntax

```
channel-group <1-16383> mode (active|passive)
no channel-group
```

Parameters

<1-16383>
Specify a channel group number (with DRNI).

mode
Specify a channel mode.

`active`
Enable LACP negotiation.

`passive`
Disable LACP negotiation.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#channel-group 1 mode active
(config-if)#exit

#sh run in po1
!
interface po1
 switchport
```

The is an example of `no channel-group`:

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#no channel-group
(config-if)#exit
```

© 2026 IP Infusion Inc. Proprietary

```
#sh run in xe1
!
interface xe1 switchport
!
#sh run in po1
!
interface po1
 switchport
!
```

clear lacp

Use this command to clear the counters of all LACP aggregators or a given LACP aggregator.

Command Syntax

```
clear lacp <1-16383> counters
clear lacp counters
```

Parameters

<1-16383>
Clears a channel-group number.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear lacp 2 counters
```

© 2026 IP Infusion Inc. Proprietary

debug lacp

Use this command to enable LACP debugging.

Use the `no` parameter of this command to disable debugging.

Command Syntax

```
debug lacp (event|cli|timer|packet|sync|ha|all|rx|tx)
no debug lacp (event|cli|timer|packet|sync|ha|allrx|tx)
```

Parameters

all
Enables all LACP debugging.

cli
Echo commands to console.

event
Sets the debug options for LACP events.

ha
Echo High availability events to console.

packet
Sets the debug option for LACP packets.

sync
Echo synchronization to console.

timer
Echo timer expiry to console.

rx
Echo receiving of lacpdus to console.

tx
Echo transmission of lacpdus to console.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug lacp all
```

© 2026 IP Infusion Inc. Proprietary

interface po

Use this command to create a dummy dynamic link aggregate interface (by default an L3 LAG interface).

Use the `no` parameter of this command to remove a dynamic link aggregate group and also it remove the properties of the po from all member ports.

Note: Switchport/routed mode needs to be set for the PO before adding member ports to it.

Command Syntax

```
interface po<1-16383>
no interface po<1-16383>
```

Parameters

<1-16383>
Channel group number.

Default

By default, interface po is L3 LAG interface

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface po1
(config-if)#switchport
(config-if)#exit
```

interface sa

Use this command to create a dummy static link aggregate interface (by default an L3 LAG interface) and to add an interface to an existing static link aggregation group.

Use the `no` parameter of this command to remove a static link aggregate group and also remove the properties of the po from all member ports.

Command Syntax

```
interface sa<1-16383>
no interface sa<1-16383>
```

Parameters

<1-16383>
Channel group number.

Default

By default, interface sa is L3 LAG interface

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface sa1
(config-if)#switchport
(config-if)#exit
```

© 2026 IP Infusion Inc. Proprietary

lacp destination-mac

Use this command to set the address type to use for sending LACPDUs (Link Aggregation Control Protocol Data Units).

Note: The interface must be an aggregation port.

Use the `no` parameter of this command to set the address type to its default (multicast group address).

Command Syntax

```
lacp destination-mac  (customer-bridge-group-address | multicast-group-address | non-tmpr-group-address)
no lacp destination-mac
```

Parameters

customer-bridge-group-address
Customer bridge group address

multicast-group-address
Multicast group address (default)

non-TPMR-group-address
Non-Two-Port Media Access Control Relay (TPMR) group address

Default

By default, lacp destination-mac is multicast-group-address

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#interface eth1
(config-if)#lacp destination-mac customer-bridge-group-address
```

lacp force-up

Use this command to make a port immediately begin forwarding packets and not wait for an LACPDU. After you execute this command, the member port is forcefully up even if LACP is not in sync (only if no other member in the aggregator is in sync).

If a force-up port stops receiving LACPDUs, the port ignores the time-out and remains in operation.

This command can be configured on one member interface of a port channel.

Notes:

- This command can only be given after executing the channel-group mode (page 489) command on an interface. Force-up mode is not supported for LACP passive mode.
- For MLAG, only configure a force-up port on either on the master node or the slave node to prevent traffic drops/loops.

Use the `no`parameter of this command to disable force-up mode.

Command Syntax:

```
lacp force-up
no lacp force-up
```

Parameters

None

Default

By default, LACP force-up mode is disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#channel-group 1 mode active
(config-if)#lacp force-up
(config-if)#exit
```

© 2026 IP Infusion Inc. Proprietary

lacp port-priority

Use this command to set the priority of a channel. Channels are selected for aggregation based on their priority with the higher priority (numerically lower) channels selected first.

Use the `no` parameter of this command to set the priority of port to the default value (32768).

Command Syntax

```
lacp port-priority <1-65535>
no lacp port-priority
```

Parameters

<1-65535>
Specify the LACP port priority.

Default

By default, lacp port priority is 32768

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#lacp port-priority 34
```

© 2026 IP Infusion Inc. Proprietary

lacp system-priority

Use this command to set the LACP system priority. This priority determines the system responsible for resolving conflicts in the choice of aggregation groups.

Note: A lower numerical value has a higher priority.

Use the `no` parameter of this command to set the system priority to its default value (32768).

Command Syntax

```
lacp system-priority <1-65535>
no lacp system-priority
```

Parameters

<1-65535>
System priority.

Default

By default, system priority is 32768

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#lacp system-priority 6700
```

lacp timeout

Use this command to set either a short or long timeout value on a port. The timeout value is the number of seconds before invalidating a received LACP data unit (DU).

Command Syntax

```
lacp timeout (short|long)
```

Parameters

short
LACP short timeout. 3 seconds.

long
LACP long timeout. 90 seconds.

Notes:

- Short: With this mode, BPDU will be sent at Fast_Periodic_Time of 1 second interval. It will timeout, before invalidating received LACPDU, after 3xFast_Periodic_Time(3seconds),
- Long: With this mode, BPDU will be sent at Slow_Periodic_Time of 30 seconds intervals. It will timeout, before invalidating received LACPDU, after 3xSlow_Periodic_Time(90seconds).

Default

By default, lacp timeout is long.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following sets the LACP short timeout on a port.

```
#configure terminal
(config)#interface eth0
(config-if)#lacp timeout short

#configure terminal
(config)#interface eth0
(config-if)#lacp timeout long
```

© 2026 IP Infusion Inc. Proprietary

port-channel load-balance

Use this command to configure LACP port-channel load-balancing and set port-selection criteria (PSC) for an interface.

Use the `no` parameter of this command to remove the load-balancing configuration and unset PSC.

Command Syntax

```
port-channel load-balance (dst-mac|src-mac|src-dst-mac|dst-ip|src-ip|src-dst-ip|dst-port|src-
port|src-dst-port|rtag7)
no port-channel load-balance
```

Parameters

dst-ip
Destination IP address-based load balancing.

dst-mac
Destination MAC address-based load balancing.

dst-port
Destination TCP/UDP address-based load balancing.

src-dst-ip
Source and Destination IP address-based load balancing.

src-dst-mac
Source and Destination MAC address-based load balancing.

src-dst-port
Source and Destination TCP/UDP address-based load balancing.

src-ip
Source IP address-based load balancing.

src-mac
Source MAC address-based load balancing.

src-port
Source port address-based load balancing.

rtag7
Hashing is based on global rtag configuration.

Default

By default load balance is src-dst-ip for L3 port and src-dst-mac for L2 port.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

© 2026 IP Infusion Inc. Proprietary

Note: The port-channel load-balance CLI option is not applicable for Tomahawk 3 boards.

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel load-balance src-dst-mac
```

port-channel min-bandwidth - dynamic LAG min-bandwidth

Use this command to set the minimum number of aggregated bandwidth that need to be up in the LAG(PO) interface. When the minimum number of bandwidth are configured for a LAG(PO), if the active links bandwidth for that interface become less than the configured value, then the whole LAG(PO) is brought down. When the number of active links bandwidth become the same or more than the configured value, then the whole LAG is restored.

Use the `no` parameter of this command to remove the minimum number of aggregated bandwidth that need to be up in the LAG interface.

Notes:

- The minimum number of aggregated bandwidth should be same across both ends of an aggregation interface. If not configured, then on one of the nodes the LAG port will be treated as up and on the other as down and traffic will be discarded.
- When a LAG port is moved to the down state because it does not have the minimum number of required bandwidth up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.
- The port-channel min-links - dynamic LAG min-links feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Command Syntax

```
port-channel min-bandwidth <1-1000>g
no port-channel min-bandwidth
```

Parameters

<1-1000>g
Specifies the value for 1 to 1000 gigabits/s

Default

By default, port channel min- bandwidth is disabled.

Command Mode

Interface mode

Applicability

This command was introduced from OcNOS version 1.3.8.

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel min-bandwidth 10g
```

port-channel min-bandwidth - static LAG min-bandwidth

Use this command to set the minimum number of aggregated bandwidth that need to be up in the LAG(SA) interface. When the minimum number of bandwidth are configured for a LAG(SA), if the active links bandwidth for that interface become less than the configured value, then the whole LAG(SA) is brought down. When the number of active links bandwidth become the same or more than the configured value, then the whole LAG is restored.

Use the `no` parameter of this command to remove the minimum number of aggregated bandwidth that need to be up in the LAG interface.

Notes:

- The minimum number of aggregated bandwidth should be same across both ends of an aggregation interface. If not configured, then on one of the nodes the LAG port will be treated as up and on the other as down and traffic will be discarded.
- When a LAG port is moved to the down state because it does not have the minimum number of required bandwidth up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.
- The port-channel min-links - static LAG min-links feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Command Syntax

```
port-channel min-bandwidth <1-1000>g
no port-channel min-bandwidth
```

Parameters

<1-1000>g
Specifies the value for 1 to 1000 gigabits/s

Default

By default, port channel min- bandwidth is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.8.

Example

```
#configure terminal
(config)#interface sa1
(config-if)#port-channel min-bandwidth 10g
```

© 2026 IP Infusion Inc. Proprietary

port-channel min-links - dynamic LAG min-links

Use this command to set the minimum number of aggregated links that need to be up in the LAG(PO) interface. When the minimum number of links are configured for a LAG(PO), if the active links for that interface become less than the configured value, then the whole LAG(PO) is brought down. When the number of active links become the same or more than the configured value, then the whole LAG is restored.

Use the `no` parameter of this command to remove the minimum number of aggregated links that need to be up in the LAG interface.

Notes:

- The minimum number of aggregated links should be same across both ends of an aggregation interface. If not configured, then on one of the nodes the LAG port will be treated as up and on the other as down and traffic will be discarded.
- When a LAG port is moved to the down state because it does not have the minimum number of required links up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.
- The show debugging lacp feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Command Syntax

```
port-channel min-links <2-32>
no port-channel min-links
```

Parameters

<2-32>
Specifies the value of minimum number of links

Default

By default, port channel min-link is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.8.

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel min-links 10
(config-if)#exit
```

© 2026 IP Infusion Inc. Proprietary

port-channel min-links - static LAG min-links

Use this command to set the minimum number of aggregated links that need to be up in the LAG(SA) interface. When the minimum number of links are configured for a LAG(SA), if the active links for that interface become less than the configured value, then the whole LAG(SA) is brought down. When the number of active links become the same or more than the configured value, then the whole LAG is restored.

Use the `no`parameter of this command to remove the minimum number of aggregated links that need to be up in the LAG interface.

Notes:

- The minimum number of aggregated links should be same across both ends of an aggregation interface. If not configured, then on one of the nodes the LAG port will be treated as up and on the other as down and traffic will be discarded.
- When a LAG port is moved to the down state because it does not have the minimum number of required links up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.
- The port-channel min-bandwidth - static LAG min-bandwidth feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Command Syntax

```
port-channel min-links <2-32>
no port-channel min-links
```

Parameters

<2-32>
Specifies the value of minimum number of links

Default

By default, port channel min-link is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.8.

Example

```
#configure terminal
(config)#interface sa1
(config-if)#port-channel min-links 10
(config-if)#exit
```

show debugging lacp

Use this command to display the status of the debugging of the LACP system.

Command Syntax

```
show debugging lacp
```

Parameters

None

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging lacp

LACP debugging status:
LACP timer debugging is on
```

© 2026 IP Infusion Inc. Proprietary

show etherchannel

Use this command to display information about link aggregation groups.

Command Syntax

```
show etherchannel
show etherchannel <1-16383>
```

With MLAG:

```
show etherchannel (<1-16383>|) detail
show etherchannel (<1-16383>|) limit
show etherchannel (<1-16383>|) load-balance
show etherchannel (<1-16383>|) summary
```

Without MLAG:

```
show etherchannel (<1-16383>|) detail
show etherchannel (<1-16383>|) limit
show etherchannel (<1-16383>|) load-balance
show etherchannel (<1-16383>|) summary
```

Parameters

<1-16383>
Specify channel-group number.

detail
Specify detailed etherchannel information.

limit
Specify channel limit.

Max Aggregators
Maximum number of aggregators supported is 128.

Max Ports in Aggregator
Maximum number of ports supported in aggregator 16.

load-balance
Specify load balancing.

summary
Specify Etherchannel summary information.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
OcNOS#show etherchannel limit
Max Aggregators         : 256
```

© 2026 IP Infusion Inc. Proprietary

```
Max Ports in Aggregator : 64

OcNOS#show etherchannel summary
% Aggregator po1 185
% Aggregator Type: Layer3
% Admin Key: 0001 - Oper Key 0001
%   Link: eth3 (5) sync: 0
-------------------------------------
% Aggregator po4 186
% Admin Key: 0004 - Oper Key 0004
%   Link: eth2 (4) sync: 0
-------------------------------------
% Aggregator po5 187
% Admin Key: 0005 - Oper Key 0005
%   Link: eth1 (3) sync: 0


OcNOS#show etherchannel detail
% Aggregator po1 185
% Aggregator Type: Layer3
%  Mac address: 08:00:27:36:f5:7d
%  Admin Key: 0001 - Oper Key 0001
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0001
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 0
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth3 (5) sync: 0
%  Collector max delay: 5
-------------------------------------------------
% Aggregator po4 186
%  Mac address: 08:00:27:76:0c:57
%  Admin Key: 0004 - Oper Key 0004
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0004
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth2 (4) sync: 0
%  Collector max delay: 5
-------------------------------------------------
% Aggregator po5 187
%  Mac address: 08:00:27:2f:d5:ae
%  Admin Key: 0005 - Oper Key 0005
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0005
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 0
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth1 (3) sync: 0
%  Collector max delay: 5
```

Table 16. show etherchannel detail output

Field	Description
Aggregator	Link aggregators name and ID number.
Mac address	Unique MAC address for link identification.
Admin Key	LACP administrative key – automatically configured value on each port configured to use LACP.
Oper Key	LACP operator key on Partner – automatically configured value on each port configured to use LACP.
Actor LAG ID	LAG ID consisting of MAC address plus aggregator ID number for this Actor.
Receive link count	The number of link received from the peer LAG.

Table 16. show etherchannel detail output (continued)

Field	Description
Transmit link count	The number of links contained transmitted to the peer LAG.
Individual	The individual physical network interfaces or ports contained in the LAG.
Ready	The number of links in the active state on this Actor.
Partner LAG ID	Partner LAG ID consisting of MAC address plus aggregator ID number.
Link	Interface and ID number of the link.
sync	MAC address synchronization enables a MLAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.
Collector max delay	Maximum period of wait time between sending of two subsequent Ethernet frames on a link.

© 2026 IP Infusion Inc. Proprietary

show lacp-counter

Use this command to display the packet traffic on all ports of all present LACP aggregators, or a given LACP aggregator.

Command Syntax

```
show lacp-counte
show lacp-counter <1-16383>
```

Parameters

<1-16383>
Channel-group number

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lacp-counter 555

Port      LACPDUs         Marker          Pckt err
        Sent    Recv    Sent    Recv    Sent    Recv
```

show lacp sys-id

Use this command to display the LACP system identifier and priority.

Command Syntax

```
show lacp sys-id
```

Parameters

sys-id
Display LACP system ID and priority

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lacp sys-id
% System 8000,00-0e-0c-83-37-27
```

© 2026 IP Infusion Inc. Proprietary

show port etherchannel

Use this command to display details about a PO and its members' interfaces or to display details of a single member interface of a PO.

Command Syntax

```
show port etherchannel IFNAME
```

Parameters

IFNAME
Interface name

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show port etherchannel ce29/1
LAG ID                        : 0x8000,cc-37-ab-a0-89-ca,0x0002
Partner oper LAG ID           : 0x8000,a8-2b-b5-38-1e-48,0x0004
Aggregator ID                 : 100002
  LACP link info              : ce29/1 - 10001
  Periodic Transmission
  machine state               : Slow periodic
  Receive machine state       : Current
  Mux machine state           : Collecting/Distributing
  Actor Info :
  ===========
  Actor Port priority         : 0x8000 (32768)
  Admin key                   : 0x0002 (2) Oper key: 0x0002 (2)
  Physical admin key          : (2)
  Actor Oper state            : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Actor Admin state           : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
  Partner Info:
  ============
  Partner oper port           : 10009
  Partner link info           : admin port 0
  Partner admin LAG ID        : 0x0000-00:00:00:00:0000
  Partner system priority     : admin:0x0000 - oper:0x8000
  Partner port priority       : admin:0x0000 - oper:0x8000
  Partner oper state          : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Partner admin state         : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0


#show port etherchannel po2
LAG ID                        : 0x8000,cc-37-ab-a0-89-ca,0x0002
Partner oper LAG ID           : 0x8000,a8-2b-b5-38-1e-48,0x0004
Aggregator ID                 : 100002
  LACP link info              : ce29/1 - 10001
  Periodic Transmission
  machine state               : Slow periodic
```

```
Receive machine state      : Current
Mux machine state          : Collecting/Distributing
Actor Info :
===========
Actor Port priority        : 0x8000 (32768)
Admin key                  : 0x0002 (2) Oper key: 0x0002 (2)
Physical admin key         : (2)
Actor Oper state           : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Actor Admin state          : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
Partner Info:
============
Partner oper port          : 10009
Partner link info          : admin port 0
Partner admin LAG ID       : 0x0000-00:00:00:00:0000
Partner system priority    : admin:0x0000 - oper:0x8000
Partner port priority      : admin:0x0000 - oper:0x8000
Partner oper state         : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner admin state        : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0

LACP link info             : ce30/1 - 10005
Periodic Transmission
machine state              : Slow periodic
Receive machine state      : Current
Mux machine state          : Collecting/Distributing
Actor Info :
===========
Actor Port priority        : 0x8000 (32768)
Admin key                  : 0x0002 (2) Oper key: 0x0002 (2)
Physical admin key         : (2)
Actor Oper state           : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Actor Admin state          : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
Partner Info:
============
Partner oper port          : 10013
Partner link info          : admin port 0
Partner admin LAG ID       : 0x0000-00:00:00:00:0000
Partner system priority    : admin:0x0000 - oper:0x8000
Partner port priority      : admin:0x0000 - oper:0x8000
Partner oper state         : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner admin state        : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
```

Note: Most of the output of this command is duplicated in the show etherchannel (page 507) command (see also the 802.3ad specificiation). The output of the `show port etherchannel` command is primarily a list of state machine values. An explanation of the state machine bits follows. See Figure 49.

Table 17. show port etherchannel detailed output

Entry	Description
Actor/Partner state	The Actor's and Partner's state variables, encoded as individual bits within a single octet.
ACT	LACP_Activity is encoded in bit 0. Active LACP is encoded as a 1; Passive LACP as a 0.
TIM	LACP_Timeout is encoded in bit 1. Short Timeout is encoded as a 1; Long Timeout as a 0.
AGG	Aggregability is encoded in bit 2. Aggregatable is encoded as a 1; Individual is encoded as a 0.
SYN	Synchronization is encoded in bit 3. In_Sync is encoded as a 1; Out_Of_Sync is encoded as a 0.
COL	Collecting is encoded in bit 4. True is encoded as a 1; False is encoded as a 0.

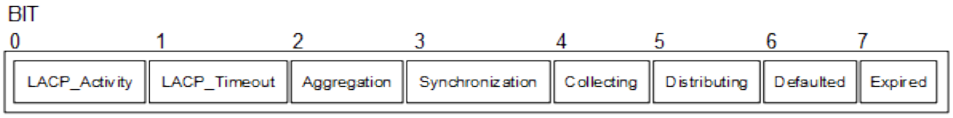
© 2026 IP Infusion Inc. Proprietary

Table 17. show port etherchannel detailed output (continued)

Entry	Description
DIS	Distributing is encoded in bit 5. True is encoded as a 1; False is encoded as a 0.
DEF	Defaulted is encoded in bit 6.
EXP	Defaulted is encoded in bit 7.

Bits 7 and 8 are reserved; these are ignored on receipt and transmitted as zero. However, the received value of these bits is recorded on receipt to accurately reflect the actor's view of the partner's state in outgoing PDUs.

Figure 49. Diagram of state machine octet



show static-channel-group

Use this command to display the types of load-balancing port selection criteria (PSC) used on configured static aggregators.

Command Syntax

```
show static-channel-group   (<1-16383>|)
```

Parameters

<1-16383>
Specify channel-group number.

Command Mode

Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is an example of the output of this command:

```
#show  static-channel-group 1
% Static Aggregator: sa1
% Member:
   eth1
```

show static-channel load-balance

Use this command to display information about static channel groups.

Command Syntax

```
show static-channel (<1-16383>|) load-balance
```

Parameters

<1-16383>
Specify static-channel-group number.

Command Mode

Privileged execution mode

Applicability

This command was introduced before OcNOS version SP 1.0.

Examples

The following is an example of the output of this command:

```
#show static-channel load-balance
% Static Aggregator: sa5
Flow based division
```

snmp restart lacp

Use this command to restart SNMP in LACP.

Command Syntax

```
snmp restart lacp
```

Parameters

None

Default

By default, snmp restart lacp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#snmp restart lacp
```

© 2026 IP Infusion Inc. Proprietary

static-channel-group

Use this command to create a static link aggregation group or to add an interface to an existing link aggregation group.

Use the `no` parameter of this command to remove an interface from a static link aggregation group without removing the static link aggregation group itself.

Command Syntax

```
static-channel-group <1-16383>
no static-channel-group
```

Parameter

<1-16383>
Channel group number.

Default

By default, static channel group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#static-channel-group 1
(config-if)#exit

#sh run in sa1
!
interface sa1
 switchport
```

This is an example of `no static-channel-group`:

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#no static-channel-group
(config-if)#exit

#sh run in xe1
!
interface xe1 switchport
!
#sh run in sa1
!
```

© 2026 IP Infusion Inc. Proprietary

```
interface sa1
 switchport
!
```

Multi-chassis Link Aggregation Commands

This section describes the Multi-Chassis Link Aggregation commands.

Multi-Chassis Link Aggregation is also called MC-LAG, MLAG, or Distributed Resilient Network Interconnect (DRNI). In this document, it is called MLAG.

clear mcec statistics 521
debug mcec 522
domain-address 523
domain hello timeout 524
domain priority 525
domain-system-number 526
idl-higig 527
intra-domain-peer 528
mcec domain configuration 529
mlag 530
mode 531
show mcec statistics 532
show mlag detail 533
show mlag domain 535
show mlag stp-synchronization status 538
show spanning-tree mlag operational-config 539
show spanning-tree mlag sync-detail 540
switchover type 541

© 2026 IP Infusion Inc. Proprietary

clear mcec statistics

Use this command to clear the statistics related to hello and information PDUs in the MCEC domain.

Command Syntax

```
clear mcec statistics
```

Parameters

None

Command Mode

Privileged execution mode

Applicability

This command was introduced before OcNOS version 4.0.

Examples

```
#clear mcec statistics
```

© 2026 IP Infusion Inc. Proprietary

debug mcec

Use this command to view debugging logs for MLAG.

Use the `no` form of this command to remove debugging logs for MLAG.

Command Syntax

```
debug mcec (timer|event|hello|info|cli|mac-sync|all)
no debug mcec (timer|event|hello|info|cli|mac-sync|all)
```

Parameters

all
ALL

cli
CLI

event
Event

hello
Hello

info
Info

mac-sync
Mac Sync

timer
Timer

Command Mode

Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug mcec all
#no debug mcec all
```

© 2026 IP Infusion Inc. Proprietary

domain-address

Use this command to configure domain address, which helps to identify the mcec domain.

Use the `no` form of this command to remove the domain address.

Command Syntax

```
domain-address <domain-id>
no domain-address
```

Parameters

domain-id

domain address in HHHH.HHHH.HHHH format

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-address 1111.2222.3333
```

domain hello timeout

Use this command to specify the domain hello-timeout value.

Command Syntax

```
domain-hello-timeout (long|short)
no domain-hello-timeout
```

Parameters

long
Long Timeout

short
Short Timeout

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-hello-timeout long
```

© 2026 IP Infusion Inc. Proprietary

domain priority

Use this command to specify the priority value associated with mcec domain.

Use the `no` form of this command to remove the priority value associated with mcec domain.

Command Syntax

```
domain-priority <1-65535>
no domain-priority
```

Parameters

<1-65535>
Priority Value

Default

The default value is 32768.

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-priority 2
```

domain-system-number

Use this command to configure domain system number, which uniquely identifies domain system in mcec domain.

Use the `no` form of this command to configure domain system number.

Command Syntax

```
domain-systm-number <1-2>
no domain-systm-number
```

Parameters

<1-2>
Domain System Number

Command Mode

MLAC mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-system-number 2
```

idl-higig

Use this command to configure MLAG Inter domain link (IDL) to Higig mode. The Higig mode is required for MLAG port isolation to work when the MLAG link fails.

Use the `no` form command to unconfigure the IDLHigig mode.

Note: The idl-higig CLI is not supported on Tomahawk3 series platforms.

Command Syntax

```
idl-higig
no idl-higig
```

Parameters

None

Default

None

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 6.0.0

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#idl-higig
(config-mcec-domain)#no idl-higig
```

© 2026 IP Infusion Inc. Proprietary

intra-domain-peer

Use this command to map an interface as intra domain peer that connects the domain system with its neighbor in a mcec domain.

Use the `no` form of this command to unmap the interface configured as intra domain peer that connects the domain system with its neighbor in a mcec domain.

Command Syntax

```
intra-domain-peer A.B.C.D source-address A.B.C.D (vrf VRF_NAME|)
no intra-domain-peer
```

Parameters

Peer Address
Peer/Target IPv4 address

A.B.C.D
IPv4 address.

source-address
Source IPv4 address

A.B.C.D
IPv4 address.

VRF_NAME
VRF Interface name

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 3.0.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#intra-domain-peer 1.1.1.1 source-address 2.2.2.2 vrf myvrf
```

© 2026 IP Infusion Inc. Proprietary

mcec domain configuration

Use this command to enter MCEC Domain configuration mode to configure mcec domain information.

Command Syntax

```
mcec domain configuration
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#
```

mlag

Use this command to map a port-channel to an MLAG instance.

Notes:

- The MLAG port-channel (interface) must be created before mapping.
- All MLAG nodes must use the same MAC table size.

Use the `no`form of this command to un-map the port channel from the MLAG instance.

Command Syntax

```
mlag <1-255>
no mlag
```

Parameters

<1-255>
MLAG identifier

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3 and updated for static channel groups in OcNOS version 1.3.6

Example

```
#config terminal
(config)#interface mlag1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport mode trunk allowed vlan all
(config-if)#exit
(config)#interface sa1
(config-if)#switchport
 (config-if)#mlag 1
(config-if)#exit

#configure terminal
(config)#interface sa1
(config-if)#no mlag
```

© 2026 IP Infusion Inc. Proprietary

mode

Use this command to set the MLAG mode.

Use the `no` form of this command to turn off this feature.

Command Syntax

```
mode (active-active | active-standby)
no mode (active-active | active-standby)
```

Parameters

active-active
The interface is the active interface that carries the traffic.

active-standby
The interface is ready for transition to the active state if a failure occurs in the other node.

Default

active-active

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 4.0.

Examples

```
(config)#
(config)#interface mlag1
(config-if)#mode active-active

(config)#
(config)#interface mlag1
(config-if)#mode active-standby
```

© 2026 IP Infusion Inc. Proprietary

show mcec statistics

Use this command to display all the statistics related to hello and info pdu's in mcec domain.

Command Syntax

```
show mcec statistics
```

Parameters

None

Command Mode

Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh mcec statistics
Unknown MCCPDU received on the system : 0

-----------------------------------
IDP xe49
-----------------------------------
Valid RX Hello PDUs : 109
Valid TX Hello PDUs : 201
Valid RX Info PDUs: 23
Valid TX Info PDUs : 28
Valid RX Mac Sync PDUs : 5
Valid TX Mac Sync PDUs : 4
Valid RX Dhcps Sync PDUs : 2
Valid TX Dhcps Sync PDUs : 1

MLAG 1
Valid RX Info PDUs : 5
Valid TX Info PDUs : 7
```

Table 18. Show mcec statistics details

Entry	Description
RX Hello PDUs	Total number of received hello PDUs.
TX Hello PDUs	Total number of transmitted hello PDUs.
RX Info PDUs	Total number of received Info PDUs.
TX Info PDUs	Total number of transmitted Info PDUs.
RX Mac Sync PDUs	Total number of received Mac Sync PDUs.
TX Mac Sync PDUs	Total number of transmitted Mac Sync PDUs.
RX Dhcps Sync PDUs	Total number of received Dhcps Sync PDUs
TX Dhcps Sync PDUs	Total number of transmitted Dhcps Sync PDUs

© 2026 IP Infusion Inc. Proprietary

show mlag detail

Use this command to display details about MLAG configuration and status.

Command Syntax

```
show mlag <1-255> detail
```

Parameters

<1-255>
MLAG group number

Command Mode

Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3 and updated for static channel groups in OcNOS version 1.3.6.

Examples

```
#sh mlag 1 detail

MLAG-17
Mapped Aggregator : po1
Admin Key : 32769
Oper Key: 16385
Physical properties Digest : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

Neigh Admin Key: 16385
Neigh Physical Digest: dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
Info RCV State : Current
Info Periodic Time State : Standby
Mlag Sync                : IN_SYNC
Mode                     : Active
```

Table 19. Show mlag output details

Entry	Description
Mapped Aggregator	Map the output of the aggregator in the interface which is active transformation.
Admin Key	MLAG administrative key – automatically configured value on each port configured to use MLAG.
Oper Key	MLAG operator key on Partner – automatically configured value on each port configured to use MLAG.
Physical properties Digest	Physical properties of the digest.
Neigh Admin Key	Neigh administrative key – automatically configured value on each port configured to use MLAG.

© 2026 IP Infusion Inc. Proprietary

Table 19. Show mlag output details (continued)

Entry	Description
Neigh Physical Digest	Neigh physical properties of the digest.
Info RCV State	Details of the RCV.
Info Periodic Time State	A simple state space formulation of a general digital periodic time series is constructed.
Mlag Sync	MAC address synchronization enables a MLAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.

show mlag domain

Use this command to display MLAG configuration and status.

Command Syntax

```
show mlag domain <details|summary>
```

Parameters

details
details

summary
summary

Command Mode

Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : sa5
Domain Adjacency                : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator             : sa1
  Physical properties Digest    : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc
  Total Bandwidth               : 40g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active

MLAG-2
  Mapped Aggregator             : sa2
  Physical properties Digest    : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8

  Total Bandwidth               : 40g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active


# show mlag domain details
-------------------------------------
```

```
Domain Configuration
------------------------------------
Domain System Number           : 1
Domain Address                 : 1111.2222.3333
Domain Priority                : 32768
Intra Domain Interface         : sa5

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP
------------------------------------
MLAG Configuration
------------------------------------
MLAG-1
  Mapped Aggregator            : sa1
  Admin Key                    : 16385
  Oper Key                     : 16385
  Physical properties Digest   : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc

  Neigh Admin Key              : 32769
  Neigh Physical Digest        : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Total Bandwidth              : 40g
  Mlag Sync                    : IN_SYNC

MLAG-2
  Mapped Aggregator            : sa2
  Admin Key                    : 16386
  Oper Key                     : 16386
  Physical properties Digest   : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8
  Neigh Admin Key              : 32770
  Neigh Physical Digest        : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8

  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Total Bandwidth              : 40g
  Mlag Sync                    : IN_SYNC
```

Table 20. Show mlag summary details

Entry	Description
Domain System Number	Number to identify the node in domain.
Domain Address	Domain address for the MLAG domain.
Domain Priority	Domain priority for the MLAG domain.
Intra Domain Interface	Intra domain interface between MLAG domains.
Domain Adjacency	Domain adjacency details and configuration.
Physical properties Digest	physical properties of the digest algorithm.
Total Bandwidth	Total bandwidth available on the interface.
Domain System Number	Number of the domain system.
Domain Address	Domain address for the MLAG domain.
Domain Priority	Domain priority for the MLAG domain.
Intra Domain Interface	Details of the intra domain in the interface.

© 2026 IP Infusion Inc. Proprietary

Table 20. Show mlag summary details (continued)

Entry	Description
Hello RCV State	State of the hello RCV in the interface.
Hello Periodic Timer State	State of the hello periodic timer in the interface.
Domain Sync	Detail of the domain configuration synchronization.
Mapped Aggregator	Map the output of the aggregator in the interface which is active transformation.
Admin Key	MLAG administrative key – automatically configured value on each port configured to use MLAG.
Oper Key	MLAG operator key on Partner – automatically configured value on each port configured to use MLAG.
Physical properties Digest	Physical properties of the digest.
Neigh Admin Key	Neigh administrative key – automatically configured value on each port configured to use MLAG.
Neigh Physical Digest	Neigh physical properties of the digest.
Info RCV State	Details of the RCV.
Info Periodic Time State	A simple state space formulation of a general digital periodic time series is constructed.
Mlag Sync	MAC address synchronization enables a MLAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.

show mlag stp-synchronization status

Use this command to display information about MLAG STP Syncronization status

Command Syntax

```
show mlag stp-synchronization status
```

Parameters

stp-synchronization
STP synchronization related show commands

status
STP synchronization status

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
OcNOS#show mlag stp-synchronization status

 Home STP Domain Digest     : 27 e7 22 79 76 b2 c8 4e 49 9f b4 45 4f 20 68 aa
 Neighbor STP Domain Digest : 27 e7 22 79 76 b2 c8 4e 49 9f b4 45 4f 20 68 aa
 STP Sync Status            : IN_SYNC

-------------------------------------------------------

 MLAG Interface Status:

 MLAG1:

  Home Interface Digest       : 76 88 b9 cd 43 c1 b0 9d b 86 64 e5 b7 d2 7f a7
  Neighbor Interface Digest   : 76 88 b9 cd 43 c1 b0 9d b 86 64 e5 b7 d2 7f a7
  STP Sync Status             : IN_SYNC
#

Entry                                  Description
Home STP Domain Digest                STP Domain properties of the digest
Neighbor STP Domain Digest            Neighbor STP Domain properties of the digest
STP Sync Status                       Detail of configurated STP synchronization.
Home Interface Digest                 Interface properties of the digest.
Neighbor Interface Digest             Neigh Interface properties of the digest.
```

show spanning-tree mlag operational-config

Use this command to display the operational information for MLAG.

Command Syntax

```
show spanning-tree mlag operational-config
```

Parameters

None

Command Mode

Privileged execution mode

Applicability

This command was introduced before OcNOS version 4.0.

Examples

```
#show spanning-tree mlag operational-config
 Operational Configuration
----------------------------------------
 Bridge Priority       : 32768
 Pathcost method       : Long
 Interface             : mlag1
 Pathcost              : 1000
 Priority              : 0
```

show spanning-tree mlag sync-detail

Use this command to display the spanning-tree properties shared with the domain peer node.

Command Syntax

```
show spanning-tree mlag sync-detail
```

Parameters

None

Command Mode

Privileged execution mode

Applicability

This command was introduced before OcNOS version 4.0.

Examples

```
#show spanning-tree mlag sync-detail
 Domain Digest Parameters
----------------------------------------
 Max Age             : 20
 BPDU Filter         : Disabled
 BPDU Guard          : Disabled
 Hello time          : 2
 Forward Delay       : 15
 Force Version       : 2
 Err-disable status  : Disabled
 Err-disable timeout : 300
 MSTP Enabled        : Enabled
 MSTP Bridge Forward : Disabled

 Interface Digest parameters
----------------------------
  Port Name              : mlag1
  Admin Root Guard       : Disabled
  Admin Edge port        : Disabled
  Portfast configuration : Disabled
  Restricted TCN         : Disabled
  Admin BPDU filter      : Default
  Admin BPDU guard       : Default
```

© 2026 IP Infusion Inc. Proprietary

switchover type

Use this command to set the MLAG switchover type.

Use the `no` form of this command to turn off switchover.

Command Syntax

```
switchover type revertive <1-3600>
switchover type non-revertive
no switchover type (revertive | non-revertive)
```

Parameters

revertive <1-3600>

A network failure triggers a switchover, the initially active node becomes active again after failure recovery. Configure the number of seconds within this range to switch back to the initially active node after the failure recovery. The default time is 10 seconds.

non-revertive

A network failure triggers a switchover, the initially active node remains on standby after failure recovery.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 4.0 and the `revertive <1-3600>` is revised in OcNOS version 6.6.0.

Examples

```
OcNOS(config)#interface mlag1
OcNOS(config-if)#switchover type revertive 20

OcNOS(config)#interface mlag1
OcNOS(config-if)#switchover type non-revertive
```

© 2026 IP Infusion Inc. Proprietary

Traffic Mirroring Commands

This section provides a description of syntax, and examples for Traffic Mirroring. It includes the following commands:

description 543
destination interface 544
filter 545
monitor session 547
monitor session shut 548
no shut 549
remote destination 550
show filter 551
show monitor 552
show monitor running configuration 553
show monitor session 554
shut 556
source interface 557
source vlan 559

© 2026 IP Infusion Inc. Proprietary

description

Use this command to add a description to the monitor session.

Use the `no` parameter to delete a description of the monitor session.

Command Syntax

```
description LINE
no description
```

Parameters

LINE

Enter the description string

Default

No default value is specified.

Command Mode

Monitor Session mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#description “port mirror rx”
(config-monitor)#no description
```

© 2026 IP Infusion Inc. Proprietary

destination interface

Use this command to configure a mirror-to port per local monitor session. A destination port can be a physical port or a trunk port.

Use the `no` parameter to remove the destination port from a local monitor session.

Note: For the monitor sessions, the destination interface should be an switchport with no service attached. This port will not participate in L2/L3 packet forwarding.

Command Syntax

```
destination interface IFNAME
no destination interface IFNAME
```

Parameters

IFNAME
Interface name

Default

No default value is specified

Command Mode

Monitor Session mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe3
(config-if)#switchport
(config-if)#exit
(config)#monitor session 1
(config-monitor)#destination interface xe3
(config-monitor)#no destination interface xe3
```

© 2026 IP Infusion Inc. Proprietary

filter

Use this command to add filters to the monitor session. Filters can be applied only in case of ingress mirroring. The configuration of sequence identifier for each rule is optional, but even if it is not configured explicitly, it will always be generated and in steps of 10.

Use the `no` parameter to remove the filter from monitor session.

Note: To add or update or delete any filters in monitor session, session needs to be in shut state.

Command Syntax

```
(<1-268435453>/<1-4294967294> |) filter {vlan VLAN_RANGE| cos <0-7> | dest-mac (host XXXX.XXXX.XXXX |
XXXX.XXXX.XXXX XXXX.XXXX.XXXX) | src-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX XXXX.XXXX.XXXX) |
frame-type (ETHTYPE | arp (req | resp|) (sender-ip A.B.C.D|) (target-ip A.B.C.D|) | ipv4 (src-ip
(A.B.C.D | A.B.C.D/M)|) (dest-ip (A.B.C.D | A.B.C.D/M)|) | ipv6 (src-ip X:X::X:X/M |) (dest-ip
X:X::X:X/M |))}

no (<1-268435453>/<1-4294967294>) filter
```

Parameters

(<1-268435453>/<1-4294967294> |)
Sequence identifier for each rule.

<2-4094>
VLAN identifier

<0-7>
COS number

XXXX.XXXX.XXXX
MAC address

ETHTYPE
Ethertype

arp
ARP frames

req
Request frames

resp
Response frames

A.B.C.D
Single IP address

A.B.C.D/M
IP addresses with mask

X:X::X:X/M
IPv6 addresses with mask

Default

No default value is specified.

© 2026 IP Infusion Inc. Proprietary

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#filter dest-mac host 0000.0001.2421 frame-type ipv4
(config-monitor)#filter cos 3 frame-type arp req sender-ip 2.2.2.1
(config-monitor)#35 filter vlan 200
(config-monitor)#no 10 filter
(config-monitor)#no 20 filter
(config-monitor)#no 35 filter
```

© 2026 IP Infusion Inc. Proprietary

monitor session

Use this command to create a local or remote monitor session. By default, a local monitor session is created.

A monitor session consists of:

- A single destination interface, referred to as a mirror-to port or a single remote destination
- One or more source interfaces (egress, ingress, or both)
- One or more VLAN sources in the ingress direction
- One or more filters that can be applied to filter the mirrored packets

Use the `no` parameter to delete a monitor session.

Command Syntax

```
monitor session <1-18> ( | type ( local | remote ))
no monitor session ( <1-18> | all )
```

Parameters

<1-18>
Session number

local
Create a local session

remote
Create a remote source node session

all
All sessions

Default

By default, monitor session type is local and will not be active by default

Command Mode

Monitor Session mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#monitor session 1
(config-monitor)#exit
(config)#monitor session 3 type remote
(config-monitor)#exit
(config)#no monitor session 1
```

© 2026 IP Infusion Inc. Proprietary

monitor session shut

Use this command to deactivate one monitor session.

Use the `no` parameter to activate one monitor session.

Command Syntax

```
monitor session <1-18> shut
no monitor session <1-18> shut
```

Parameters

<1-18>
Session number

Default

Monitor session will not be active by default

Command Mode

Monitor Session mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#monitor session 3 shut

(config)#no monitor session 3 shut
```

© 2026 IP Infusion Inc. Proprietary

no shut

Use this command to activate a monitor session

Command Syntax

```
no shut
```

Parameters

None

Default

Monitor session will not be active by default.

Command Mode

Monitor Session mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#no shut
```

© 2026 IP Infusion Inc. Proprietary

remote destination

Use this command to configure a destination VLAN and the reflector port for the remote monitor session.

Use the `no` parameter to remove a destination from a remote monitor session.

Command Syntax

```
destination remote vlan <2-4094> reflector-port IFNAME
no destination remote
```

Parameters

<2-4094>
VLAN identifier

IFNAME
Interface name

Default

No default value is specified

Command Mode

Monitor Session mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#no vlan 900 bridge 1
(config)#interface xe3
(config-if)#switchport
(config)#monitor session 1
(config-monitor)#destination remote vlan 900 reflector-port xe3
(config-monitor)#no destination remote
```

© 2026 IP Infusion Inc. Proprietary

show filter

Use this command to display filters for one or more monitor sessions.

Command Syntax

```
show monitor session (<1-18>|all|(range RANGE)) filter
```

Parameters

<1-18>
Session number

all
All sessions

RANGE
Session number range (n1-n2)

Command Mode

Execution mode or Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor session 1 filter
session 1
---------------
filter count : 3
---------------

match set 1
---------------
destination mac address : 0000.0002.4451 (host)
source mac address : 0000.0012.2288 (host)
---------------

match set 2
---------------
frame type : arp
sender ip address : 2.2.2.5
target ip addres : 2.2.2.8
---------------

match set 3
---------------
destination mac address : 0000.0001.1453 (host)
frame type : ipv4
source ip address : 3.3.3.5
#
```

© 2026 IP Infusion Inc. Proprietary

show monitor

Use this command to display states of all monitor sessions. If a session is down, the reason is displayed.

Command Syntax

```
show monitor
```

Parameters

None

Command Mode

Execution mode or Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor
Session   State          Reason               Description
------- ----------- --------------------- --------------------------------
1       down        No sources configured
2       down        Dst in wrong mode
```

show monitor running configuration

Use this command to display the mirror-related running configuration.

Command Syntax

```
show running-config monitor (all|)
```

Parameters

all
Show running configuration with defaults

Command Mode

Execution mode or Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config monitor
!
monitor session 1
 source interface xe10 rx
 destination interface po1
 no shut
#
```

© 2026 IP Infusion Inc. Proprietary

show monitor session

Use this command to display the configuration details of one or more monitor sessions.

Command Syntax

```
show monitor session (<1-18>|all|(range RANGE)) (brief|)
```

Parameters

<1-18>
Session number

all
All sessions

RANGE
Session number range (n1-n2)

brief
Brief information

Command Mode

Execution mode or Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor session 1
session 1
---------------
type              : local
state             : down (Session admin shut)
source intf       :
tx                : xe1 xe3 xe4
rx                : xe2 xe3 xe4
both              : xe3 xe4
source VLANs      :
rx                : 2,5-10,15,18-20
destination ports : xe5
filter count      :

Legend: f = forwarding enabled, l = learning enabled
#
```

Table 21 Explains the show command output fields

Table 21. Show monitor session output fields

Field	Description
Type	Type of monitor session.

Field	Description
State	State of the security flow filter.
Rx	Incoming flow (source and destination IP addresses).
Tx	Reverse flow (source and destination IP addresses).
Both	Incoming and reverse flow (source and destination IP address)
Destination Port	Name of the destination port to be matched.
Source intf	Number of maximum intf central source session.
Source VLANs	Number of maximum VLANs central source session.
Filter count	Used to count number of lines in a file or table.

© 2026 IP Infusion Inc. Proprietary

shut

Use this command to de-activate a monitor session.

Command Syntax

```
shut
```

Parameters

None

Default

Monitored session is not active by default.

Command Mode

Monitor Session mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#shut
```

© 2026 IP Infusion Inc. Proprietary

source interface

Use this command to configure a source port per monitor session in either ingress or egress or both directions. Source port can be physical interface or a trunk port.

Use the `no` parameter to remove the source port.

Note: The behavior is changed when the configuration is edited in the current release: For example, if you have configured as follows

```
source interface xe10 rx → running-config/backend: source interface xe10 rx
source interface xe10 tx → running-config/backend: source interface xe10 both
```

its direction is changed to as follows

```
source interface xe10 rx → running-config/backend: source interface xe10 rx
source interface xe10 tx → running-config/backend: source interface xe10 tx
```

Command Syntax

```
source interface IFNAME ( rx | tx | both | )
no source interface IFNAME
```

Parameters

IFNAME
Interface name

rx
Ingress direction

tx
Egress direction

both
Both directions

Default

Source port will be mirrored for both directions if the direction is not specified

Command Mode

Monitor Session mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 1
```

```
(config-monitor)#source interface xe1 both
(config-monitor)#no source interface xe1
```

source vlan

Use this command to configure one or more VLANs as source per monitor session. A VLAN as source will be mirrored only in the ingress direction. Up to 32 VLANs can be configured as source per monitor session.

Use the `no` parameter to remove vlan source from monitor session.

Note: To add or update or delete source VLAN in monitor session, session needs to be in shut state.

Command Syntax

```
source vlan VLAN_RANGE
no source vlan VLAN_RANGE
```

Parameters

VLAN_RANGE
VLAN identifier or VLAN identifier range

Default

A trunk port is a member of all VLANs by default.

Command Mode

Monitor Session mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 1
(config-monitor)#source vlan 2
(config-monitor)#source vlan 4-10
(config-monitor)#no source vlan 2-5,10
```

© 2026 IP Infusion Inc. Proprietary

VLAN and Private VLAN Commands

This section has the commands used to manage VLANs and Private VLANs. A private VLAN contains switch ports that cannot communicate with each other, but can access other networks. This section includes the following commands:

feature vlan classifier 562
global-bridge-vlan-check enable 563
private-vlan association 564
private-vlan community 565
private-vlan isolated 566
private-vlan primary 567
show dtag vlan 568
show vlan 569
show vlan access-map 571
show vlan brief 572
show vlan classifier 573
show vlan-reservation 575
switchport access 577
switchport hybrid 578
switchport mode 580
switchport mode access ingress-filter 581
switchport mode hybrid acceptable-frame-type 582
switchport mode hybrid ingress-filter 583
switchport mode private-vlan 584
switchport mode trunk disable-native-vlan 585
switchport mode (trunk) disable-native-vlan 586
switchport mode trunk ingress-filter 587
switchport private-vlan association-trunk 588
switchport mode trunk ingress-filter 589
switchport private-vlan host-association 590
switchport private-vlan mapping 591
switchport trunk allowed 592
switchport trunk allowed vlan dtag 594
switchport trunk native 595
vlan classifier activate 596
vlan classifier group 597
vlan classifier rule ipv4 598
vlan classifier rule mac 599
vlan classifier rule proto 600

© 2026 IP Infusion Inc. Proprietary

vlan database 602
vlan database 603
vlan VLAN_RANGE bridge 604
vlan VLAN_RANGE type customer 605
vlan VLAN_RANGE type service 606

feature vlan classifier

Use this command to enable the feature VLAN classifier.

Use `no` form of this command to disable the feature VLAN classifier.

Command Syntax

```
feature vlan classifier
no feature vlan classifier
```

Parameters

classifier
VLAN Classifier Service

Default

By default, feature vlan classifier is enable

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#feature vlan classifier
(config)#no feature vlan classifier
```

© 2026 IP Infusion Inc. Proprietary

global-bridge-vlan-check enable

Use this command to establish a VLAN in the global VLAN database, ensuring that the same VLAN is not permitted to be encapsulated on a sub-interface.

Command Syntax

```
global-bridge-vlan-check enable
no global-bridge-vlan-check enable
```

Parameters

enable
Enable VLAN check validations

Default

Disabled.

Command Mode

Configure mode

Applicability

This command is introduced from OcNOS version 6.5.1.

Example

1. Validating sub-interface encap VLANs should not be overlapped with bridge VLANs.

```
#(config)#bridge 1 protocol rstp vlan-bridge
(config)#vlan 2-10 bridge 1
(config)#commit
(config)#
(config)#global-bridge-vlan-check enable
(config)#commit
(config)#
(config)#int xe2.2 switchport
(config-if)#encapsulation dot1q 2
(config-if)#commit
```

Bridge VLAN ids cannot be used for L2 sub-interface's encaps

Failed to commit. As error(s) encountered during commit operation.

2. Configure sub-interface encap VLANs when not overlapping with bridge VLAN IDs.

```
#(config)#int xe5.5 switchport
(config-if)#encapsulation dot1q 11
(config-if)#commit
(config-if)#exit
(config)#end
```

© 2026 IP Infusion Inc. Proprietary

private-vlan association

Use this command to associate a secondary VLAN to a primary VLAN. Only one isolated VLAN can be associated to a primary VLAN. Multiple community VLANs can be associated to a primary VLAN.

Use the no form of this command to remove association of all the secondary VLANs to a primary VLAN.

Command Syntax

```
private-vlan association add VLAN_RANGE
private-vlan association remove VLAN_RANGE
no private-vlan association
```

Parameters

add
Add a VLAN to private VLAN list.

remove
Removes values associated with a single VLAN.

VLAN_RANGE
Specify VLAN ID 1-4094 or range(s): 1-5, 10 or 2-5,7-19 of the private VLANs to be configured

Default

By default, functionality is disabled

Command Mode

VLAN mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan association add 3-4
(config-vlan)#private-vlan association remove 3-4
(config-vlan)#no private-vlan association
```

© 2026 IP Infusion Inc. Proprietary

private-vlan community

Use this command to set a VLAN type for a private (community) VLAN.

Use the no form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> community bridge <1-32>
no private-vlan <2-4094> bridge <1-32>
```

Parameters

<2-4094>
Specify a private VLAN identifier.

bridge
Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 4 community bridge 1
```

© 2026 IP Infusion Inc. Proprietary

private-vlan isolated

Use this command to create an isolated private VLAN.

Use the no form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> isolated bridge <1-32>
no private-vlan <2-4094> bridge <1-32>
```

Parameters

<2-4094>
Specify a private VLAN identifier.

bridge
Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 3 isolated bridge 1
```

© 2026 IP Infusion Inc. Proprietary

private-vlan primary

Use this command to create a primary VLAN.

Use the no form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> primary bridge <1-32>
no private-vlan <2-4094> bridge <1-32>
```

Parameters

<2-4094>
Specify a private VLAN identifier.

bridge
Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 2 primary bridge 1
```

© 2026 IP Infusion Inc. Proprietary

show dtag vlan

Use this command to display information about VLAN double tagging.

Command Syntax

```
show dtag vlan DTAG_VLAN_ID
```

Parameters

DTAG-VLAN-IDs

Outer-VLAN identifier and inner-VLAN identifier in the format 100.200, where 100 is the outer tag and 200 is the inner tag

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh vlan all bridge 1
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                      (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Up         xe2(u) xe10(u)
1       2       vlan2            ACTIVE  Up         xe10(t)
1       10      VLAN0010         ACTIVE  Up         xe2(t) xe10(t)
1       20      VLAN0020         ACTIVE  Up         xe2(t) xe10(t)
1       30      VLAN0030         ACTIVE  Up         xe10(t)
1       40      VLAN0040         ACTIVE  Up         xe10(t)
1       50      VLAN0050         ACTIVE  Up         xe10(t)
1       60      VLAN0060         ACTIVE  Up         xe10(t)
#
```

Table 22 Explains the show command output fields.

Table 22. show vlan output fields

Field	Description
Bridge	Number of bridge in the interface.
VLAN ID	VLAN identifier of the VLAN listed.
Name	Name of the VLAN.
State	Indicates whether the physical link is operational and can pass packets.
H/W Status	Indicates that the hardware is operational.
Member ports	The tagged interfaces to which a VLAN is associated.

© 2026 IP Infusion Inc. Proprietary

show vlan

Use this command to display information about static, dynamic or all VLANs.

Command Syntax

```
show vlan (all|static|dynamic|auto) bridge <1-32>
```

Parameters

<1-32>
Displays the bridge group ID.

all
Displays all VLANs (static and dynamic).

static
Displays static VLANs.

dynamic
Displays dynamic VLANs.

auto
Displays auto configured VLANs.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh vlan all bridge 1
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                      (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== =========================
1       1       default          ACTIVE  Up         xe2(u) xe10(u)
1       2       vlan2            ACTIVE  Up         xe10(t)
1       10      VLAN0010         ACTIVE  Up         xe2(t) xe10(t)
1       20      VLAN0020         ACTIVE  Up         xe2(t) xe10(t)
1       30      VLAN0030         ACTIVE  Up         xe10(t)
1       40      VLAN0040         ACTIVE  Up         xe10(t)
1       50      VLAN0050         ACTIVE  Up         xe10(t)
1       60      VLAN0060         ACTIVE  Up         xe10(t)
#
```

Table 23 Explains the show command output fields.

Table 23. show vlan output fields

Field	Description
Bridge	Number of bridge in the interface.
VLAN ID	VLAN identifier of the VLAN listed.
Name	Name of the VLAN.
State	Indicates whether the physical link is operational and can pass packets.
H/W Status	Indicates that the hardware is operational.
Member ports	The tagged interfaces to which a VLAN is associated.

© 2026 IP Infusion Inc. Proprietary

show vlan access-map

Use this command to display information for VLAN access maps.

Command Syntax

```
show vlan access-map
```

Parameters

None

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vlan access-map
Vlan access-map myMap 10
       match ip: myMap
       action: drop
```

show vlan brief

Use this command to display brief VLAN information for all bridges.

Command Syntax

```
show vlan (brief | <2-4094>)
```

Parameters

None

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3. Added the `Total Vlans` field in the command output in OcNOS version 7.0.0.

Example

The following is a sample output from this command.

```
OcNOS#show vlan brief
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                      (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Success    eth1(u)
1       2       VLAN0002         ACTIVE  Success
1       3       VLAN0003         ACTIVE  Success
1       4       VLAN0004         ACTIVE  Success
1       5       VLAN0005         ACTIVE  Success
1       10      VLAN0010         ACTIVE  Success

Total VLANs: 6
```

Table 24 Explains the show command output fields.

Table 24. show vlan brief output fields

Field	Description
Bridge	Number of bridge in the interface.
VLAN ID	VLAN identifier of the VLAN listed.
Name	Name of the VLAN.
State	Indicates whether the physical link is operational and can pass packets.
H/W Status	Indicates that the hardware is operational.
Member ports	The tagged interfaces to which a VLAN is associated.
Total VLANs	Displays the total number of VLANs currently configured on the device.

© 2026 IP Infusion Inc. Proprietary

show vlan classifier

Use this command to display information on configured VLAN classifier groups, interfaces configured for a VLAN group or all the groups, or all configured VLAN classifier rules.

If either a group ID or rule ID is not specified, all configured VLAN classifier rules are shown. If either a group ID or rule ID is specified, a specific configured VLAN classifier rule is shown.

Command Syntax

```
show vlan classifier group interface IFNAME
show vlan classifier group (<1-16>|)
show vlan classifier interface group (<1-16>|)
show vlan classifier rule(<1-256>|)
```

Parameters

group
Displays group activated information.

<1-16>
Displays the group ID

interface
Displays interface information.

interface
Displays interface group information.

group
Displays group activated information.

<1-16>
Displays the group ID.

rule
Displays VLAN classifier rule ID.

<1-256>
Displays rule ID information.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example displays groups for VLAN classifier groups:

```
#show vlan classifier group 1
vlan classifier group 1 add rule 1
```

This example displays interfaces for all VLAN classifier groups:

© 2026 IP Infusion Inc. Proprietary

```
#show vlan classifier interface group
vlan classifier group 1 interface fe2
vlan classifier group 1 interface fe3
vlan classifier group 2 interface fe5
vlan classifier group 3 interface fe7
```

This example displays interfaces for VLAN classifier group 1:

```
#show vlan classifier interface group 1
vlan classifier group 1 interface fe2
vlan classifier group 1 interface fe3
```

This example displays interfaces for VLAN classifier rule 1:

```
#show vlan classifier rule 1
vlan classifier rule 1 mac 0011.2222.3333 vlan 2
```

© 2026 IP Infusion Inc. Proprietary

show vlan-reservation

Use this command to display reserved vlans that are configured via vlan-reservation configuration on the switch.

Command Syntax

```
show vlan-reservation
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 5.1.

Example

```
OcNOS#show vlan-reservation
VLAN ID         Status
=======         ======
500             free
501             free
502             free
503             free
504             free
505             free
506             free
507             free
508             free
509             free
510             free
OcNOS#
```

If user enables port breakout on any of the interface

```
OcNOS(config)#interface xe54/1
OcNOS(config-if)#port breakout enable
OcNOS(config-if)#commit
```

Each subsidiary ports 54/2, 54/3, 54/4 will get vlan-id from the vlan-reservation pool and the status of vlan-id changes to "allocated".

```
OcNOS#show vlan-reservation
VLAN ID         Status
=======         ======
500             allocated
501             allocated
502             allocated
503             free
504             free
505             free
506             free
507             free
```

© 2026 IP Infusion Inc. Proprietary

```
508             free
509             free
510             free
OcNOS#
```

Note: From OcNOS version 5.1, it is mandatory to configure vlan-reservation prior to port breakout configuration.

switchport access

Use this command to change the default VLAN on the current interface.

Note: IP Infusion Inc. does not recommend using VLAN identifier 1 because of interoperability issues with other vendors' equipment.

Use the `no` parameter to remove an existing VLAN.

Command Syntax

```
switchport access vlan <2-4094>
no switchport access vlan
```

Parameter

<2-4094>
Specify the VLAN identifier.

Default

The switchport access vlan default value is 3968.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows the steps of a typical VLAN session, creating and destroying a VLAN.

```
#configure terminal
(config)#interface eth0
(config-if)#switchport access vlan 3

(config)#interface eth0
(config-if)#no switchport access vlan
```

© 2026 IP Infusion Inc. Proprietary

switchport hybrid

Use this command to set the switching characteristics of the interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.

For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Use the `no` parameter to turn off allowed hybrid switching.

Command Syntax

```
switchport hybrid allowed vlan all
switchport hybrid vlan <2-4094>
switchport hybrid allowed vlan none
switchport hybrid allowed vlan remove VLAN_ID
switchport hybrid allowed vlan add VLAN_ID
no switchport hybrid
no switchport hybrid vlan
```

Parameters

all
Allow all VLANs to transmit and receive through the interface.

none
Allow no VLANs to transmit and receive through the interface.

remove
Remove these VLANs from the member set.

VLAN_ID
VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.

add
Add these VLANs to the member set.

VLAN_ID
VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.

Default

By default, switchport hybrid is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following shows adding a single VLAN to the member set.

© 2026 IP Infusion Inc. Proprietary

```
(config-if)#switchport hybrid allowed vlan add VLAN_RANGE2
eg switchport hybrid allowed vlan add 2
```

The following shows adding a range of VLANs to the member set.

```
(config-if)#switchport hybrid allowed vlan add VLAN_RANGE2
eg switchport hybrid allowed vlan add 2-4
```

© 2026 IP Infusion Inc. Proprietary

switchport mode

Use this command to set the switching characteristics of the Layer 2 interface.

Note: Customer-Network Port is not supported in Qumran1 (Q1) series platforms.

Command Syntax

```
switchport mode (provider-network|customer-edge|customer-network)
```

Parameters

provider-network
Provider network.

customer-edge
Customer edge.

customer-network
Customer network.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode provider-network
```

switchport mode access ingress-filter

Use this command to set the switching characteristics of the interface to access mode, and classify untagged frames only. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode access ingress-filter (enable|disable)
```

Parameters

ingress-filter
Set the ingress filtering for the received frames.

enable
Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.

disable
Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode access ingress-filter enable
```

© 2026 IP Infusion Inc. Proprietary

switchport mode hybrid acceptable-frame-type

Use this command to set the interface acceptable frame types. This processing occurs after VLAN classification.

Command Syntax

```
switchport mode hybrid acceptable-frame-type (all|vlan-tagged)
```

Parameters

all
Set all frames can be received

vlan-tagged
Accept only classified frames that belong to the port's member set.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode hybrid acceptable-frame-type vlan-tagged
```

© 2026 IP Infusion Inc. Proprietary

switchport mode hybrid ingress-filter

Use this command to set the switching characteristics of the interface as hybrid, and classify both tagged and untagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode hybrid ingress-filter (enable|disable)
```

Parameters

enable
Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.

disable
Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode hybrid ingress-filter enable
```

© 2026 IP Infusion Inc. Proprietary

switchport mode private-vlan

Use this command to make a Layer 2 port a host port, promiscuous port, or trunk port.

Use the no form of this command to remove the configuration.

Command Syntax

```
switchport mode private-vlan (host | promiscuous)
no switchport mode private-vlan
```

Parameters

host

This port type can communicate with all other host ports assigned to the same community VLAN, but it cannot communicate with the ports in the same isolated VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN.

promiscuous

A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN

Default

By default, switchport mode private-vlan is host.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 3.0.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode private-vlan host
(config)#interface eth1
(config-if)#switchport mode private-vlan promiscuous
(config)#interface eth2
(config-if)#no switchport mode private-vlan
```

© 2026 IP Infusion Inc. Proprietary

switchport mode trunk disable-native-vlan

Use this command to create a switchport mode trunk without any default native vlan (i.e. vlan 1).

Use the `no` form of this command to delete the CLI and add vlan-1 back as default-native-vlan (i.e. vlan 1) as untagged.

Command Syntax

```
switchport mode trunk disable-native-vlan
no switchport mode trunk disable-native-vlan
```

Parameters

None

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 5.1.

Example

```
(config)#int xe7
(config-if)#switchport mode trunk disable-native-vlan
```

switchport mode (trunk) disable-native-vlan

Use this command to create switchport mode trunk without any default native vlan (i.e. vlan 1).

Use the `no` form of this command to delete the CLI and add vlan-1 back as default-native-vlan(i.e. vlan 1) as untagged.

Command Syntax

```
switchport mode (trunk) disable-native-vlan
no switchport mode (trunk) disable-native-vlan
```

Parameters

switchport
Set the switching characteristics of interface

mode
Set the mode of the Layer-2 interface

trunk
Set the Layer-2 interface as trunk

disable-native-vlan
Disable native VLAN support

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 5.1.

Example

```
OcNOS(config)#int xe7
OcNOS(config-if)#switchport mode trunk disable-native-vlan
```

© 2026 IP Infusion Inc. Proprietary

switchport mode trunk ingress-filter

Use this command to set the switching characteristics of the interface as trunk, and specify only tagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode trunk ingress-filter (enable|disable)
```

Parameters

ingress-filter
Set the ingress filtering for the received frames.

enable
Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.

disable
Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode trunk ingress-filter enable
```

© 2026 IP Infusion Inc. Proprietary

switchport private-vlan association-trunk

Use this command to associate primary vlan and secondary vlan under "switchport mode trunk" and "switchport mode private-vlan host".

Note: Each secondary VLAN on a host trunk port must be associated with a different primary VLAN. User cannot put two secondary VLANs that are associated with the same primary VLAN on a host trunk port. Each secondary vlan on the same port has to have the same type, ie isolated or community, there cannot be mixed type.

Use the no form of this command to remove the association.

Command Syntax

```
switchport private-vlan association-trunk VLAN_ID VLAN_ ID
no switchport private-vlan association-trunk VLAN_ ID VLAN_ ID
no switchport private-vlan association-trunk
```

Parameters

VLAN_ ID
VLAN ID 2-4094

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.1.

Example

```
#configure terminal
(config)#interface xe2
(config-if)#speed 10g
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan add 10 20
(config-if)#switchport mode private-vlan host
(config-if)#switchport private-vlan association-trunk 100 10
(config-if)#switchport private-vlan association-trunk 200 20
(config-if)#no switchport private-vlan association-trunk 100 10
(config-if)#no switchport private-vlan association-trunk
```

© 2026 IP Infusion Inc. Proprietary

switchport mode trunk ingress-filter

Use this command to set the switching characteristics of the interface as trunk, and specify only tagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode trunk ingress-filter (enable|disable)
```

Parameters

ingress-filter
Set the ingress filtering for the received frames.

enable
Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.

disable
Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode trunk ingress-filter enable
```

© 2026 IP Infusion Inc. Proprietary

switchport private-vlan host-association

Use this command to associate a primary VLAN and a secondary VLAN to a host port. Only one primary and secondary VLAN can be associated to a host port.

Use the no form of this command to remove the association.

Command Syntax

```
switchport private-vlan host-association <2-4094> add <2-4094>
no switchport private-vlan host-association
```

Parameters

<2-4094>

VLAN identifier of the primary VLAN.

add

Adds the secondary VLAN.

<2-4094>

VLAN identifier of the secondary VLAN (either isolated or community).

Default

By default, switchport mode private-vlan value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport private-vlan host-association 2 add 3

#configure terminal
(config)#interface eth0
(config-if)#no switchport private-vlan host-association
```

© 2026 IP Infusion Inc. Proprietary

switchport private-vlan mapping

Use this command to associate a primary VLAN and a set of secondary VLANs to a promiscuous port.

Use the no form of this to remove all the association of secondary VLANs to primary VLANs for a promiscuous port.

Command Syntax

```
switchport private-vlan mapping <2-4094> add VLAN_ID
switchport private-vlan mapping <2-4094> remove VLAN_ID
no switchport private-vlan mapping
```

Parameters

<2-4094>

VLAN identifier of the primary VLAN.

add

Adds the secondary VLAN.

remove

Removes the secondary VLAN.

VLAN_ID

VLAN identifier <2-4094> of the secondary VLAN (either isolated or community).

Default

By default, switchport mode private-vlan mapping value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport private-vlan mapping 2 add 3-4
(config-if)#switchport private-vlan mapping 2 remove 3-4

(config-if)#no switchport private-vlan mapping
```

© 2026 IP Infusion Inc. Proprietary

switchport trunk allowed

Use this command to set the switching characteristics of the interface to trunk.

For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Use the `no` parameter to remove all VLAN identifiers configured on this port.

Command Syntax

```
switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add VLAN_ID
switchport trunk allowed vlan except VLAN_ID
switchport trunk allowed vlan remove VLAN_ID
no switchport trunk
```

Parameters

all
Allow all VLANs to transmit and receive through the interface.

none
Allow no VLANs to transmit and receive through the interface.

add
Add these VLANs to the member set.

VLAN_ID
VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.

except
All VLANs except these VLANs are part of the member set.

VLAN_ID
VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.

remove
Remove these VLANs from the member set.

VLAN_ID
VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

© 2026 IP Infusion Inc. Proprietary

Examples

The following shows adding a single VLAN to the port's member set.

```
(config)#interface eth0
(config-if)#switchport trunk allowed vlan add 2
```

The following shows adding a range of VLANs to the port's member set.

```
(config)#interface eth0
(config-if)#switchport trunk allowed vlan add 2-4
```

© 2026 IP Infusion Inc. Proprietary

switchport trunk allowed vlan dtag

Use this command to maintain a mapping between the double-tagged logical interfaces with the physical interfaces for the purpose of enabling VLAN-translation on the port alone.

An example of when to use this command is in a GPON application, where an S-tag uniquely identifies an OLT channel partition and a C-tag uniquely identifies a subscriber/service on that channel partition.

Command Syntax

```
switchport trunk allowed vlan add dtag DTAG-VLAN-IDs
switchport trunk allowed vlan remove dtag DTAG-VLAN-IDs
```

Parameters

add
Add a mapping

remove
Remove a mapping

DTAG-VLAN-IDs
Outer-VLAN identifier and inner-VLAN identifier in the format 100.200, where 100 is the outer tag and 200 is the inner tag

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#int mlag1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan add 100,2000
(config-if)#switchport trunk allowed vlan add dtag 2000.3001
```

© 2026 IP Infusion Inc. Proprietary

switchport trunk native

Use this command to configure native VLANs for this port. The native VLAN is used for classifying the incoming untagged packets.

Use the `no` parameter to revert the native VLAN to the default VLAN identifier 1.

Command Syntax

```
switchport trunk native vlan VLAN_ID
no switchport trunk native vlan
```

Parameter

VLAN_ID

VLAN identifier(s) <1-4094>. You can specify a single VLAN, or a VLAN list.

For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces in between the hyphens or commas.

Default

The default is that ingress filtering is off and all frame types are classified and accepted.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport trunk native vlan 2

(config)#interface eth0
(config-if)#no switchport trunk native vlan
```

© 2026 IP Infusion Inc. Proprietary

vlan classifier activate

Use this command to activate the VLAN classifier.

Use no form of this command to deactivate the VLAN classifier.

Command Syntax

```
vlan classifier activate <1-16> vlan <2-4096>
no vlan classifier activate <1-16>
```

Parameters

<1-16>

Indicates the VLAN classifier activate identifier.

<2-4094>

VLAN identifier of the primary VLAN.

Default

By default, vlan classifier activate value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth2
(config-if)#vlan classifier activate 1 vlan 2

(config-if)#no vlan classifier activate 1
```

© 2026 IP Infusion Inc. Proprietary

vlan classifier group

Use this command to create a subnet-based VLAN classifier group. A group indicates a VLAN classifier group ID.

Command Syntax

```
vlan classifier group <1-16> (add | delete) rule <1-256>
no vlan classifier group <1-16>
```

Parameters

add
Adds a rule to a group.

delete
Deletes a rule from a group.

rule
Indicates the VLAN classifier rule identifier <1-256>.

Default

By default, vlan classifier group value is 1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier group 1 delete rule 1
(config)#no vlan classifier group 1
```

© 2026 IP Infusion Inc. Proprietary

vlan classifier rule ipv4

Use this command to create a subnet-based VLAN classifier rule and map it to a specific VLAN.

Use this command to create a MAC-based VLAN classifier rule and map it to a specific VLAN. If the source IP address matches the IP subnet specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> ipv4 A.B.C.D/M
no vlan classifier rule <1-256>
```

Parameters

A.B.C.D/M
Indicates the IPv4 address classification. Enter the address in A.B.C.D/M format.

Default

By default, vlan classifier rule is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 ipv4 20.20.20.2/24
(config)#no vlan classifier rule 2
```

© 2026 IP Infusion Inc. Proprietary

vlan classifier rule mac

Use this command to create a MAC-based VLAN classifier rule and map it to a specific VLAN.

If the source MAC address matches the MAC specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> mac WORD
no vlan classifier rule <1-256>
```

Parameters

WORD
MAC Address in HHHH.HHHH.HHHH format.

Default

By default, vlan classifier rule value is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 mac 00D0.2331.AA1C
(config)#no vlan classifier rule 2
```

© 2026 IP Infusion Inc. Proprietary

vlan classifier rule proto

Use this command to create an Ethertype-based VLAN classifier rule for a protocol and map it to a specific VLAN. If thesource Ethertype matches the Ethertype specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> proto
(ETHERTYPE|ip|x25|arp|g8bpqx25|ieeepup|ieeeaddrtrans|dec|decdnadumpload|decdnaremoteconsole|decdnarou
ting|declat|decdiagnostics|rarp|atalkddp|atalkaarp|ipx|ipv6|atmmulti|pppdiscovery|pppsession|atmtrans
port)
no vlan classifier rule <1-256>
```

Parameters

ETHERTYPE
Specify an Ethernet protocol number (0x600-0xFFFF)

arp
Address Resolution Protocol (0x0806)

atalkaarp
Appletalk AARP (0x80F3)

atalkddp
Appletalk DDP (0x809B)

atmmulti
MultiProtocol Over ATM (0x884c)

atmtransport
Frame-based ATM Transport (0x8884)

dec
DEC Assigned (0x6000)

decdiagnostics
DEC Diagnostics (0x6005)

decdnadumpload
DEC DNA Dump/Load (0x6001)

decdnaremoteconsole
DEC DNA Remote Console (0x6002)

decdnarouting
DEC DNA Routing (0x6003)

declat
DEC LAT (0x6004)

g8bpqx25
G8BPQ AX.25 (0x08FF)

ieeeaddrtrans
Xerox IEEE802.3 PUP Address Translation (0x0a01)

ieeepup
Xerox IEEE802.3 PUP (0x0a00)

© 2026 IP Infusion Inc. Proprietary

ip
IP (0x0800)

ipv6
IPv6 (0x86DD)

ipx
IPX (0x8137)

pppdiscovery
PPPoE discovery (0x8863)

pppsession
PPPoE session (0x8864)

rarp
Reverse Address Resolution Protocol (0x8035)

x25
CCITT X.25 (0x0805)

Default

By default, vlan classifier rule value is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 proto ip
(config)#no vlan classifier rule 2
(config)#vlan classifier rule 3 proto 0x0805
(config)#no vlan classifier rule 3
```

© 2026 IP Infusion Inc. Proprietary

vlan database

Use this command to enter the VLAN configuration mode to add, delete, or modify values associated with a single VLAN.

Command Syntax

```
vlan database
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, note the change to VLAN configuration mode from Configure mode:

```
#configure terminal
(config)#vlan database
(config-vlan)#
```

© 2026 IP Infusion Inc. Proprietary

vlan database

Use this command to create or delete VLAN reservation pool on the switch.

Notes:

- The user-defined VLAN range must be contiguous with the system-defined VLANs. **Example:** If the system VLAN is `4066-4094`, the user VLAN range must be `4040-4065` and not `4040-4064` or `100-200`.
- Delete the VLAN-reservation range completely for the added user-defined VLAN range, as it is not possible to delete subsets.

Command Syntax

```
vlan-reservation VLAN_RANGE
no vlan-reservation VLAN_RANGE
```

Parameters

VLAN_RANGE

VLAN ID 2-4094 or range(s): 2-5,10 or 2-5,7-19

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 5.0.

Example

In the following example, note the change to VLAN configuration mode from Configure mode:

```
#configure terminal
(config)#vlan database
(config-vlan)#
```

© 2026 IP Infusion Inc. Proprietary

vlan VLAN_RANGE bridge

This command allows you to create a single/range of VLAN's on the VLAN aware bridges.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE bridge <1-32>
vlan <2-4094> bridge <1-32> (state (enable|disable)|)
vlan VLAN_RANGE bridge <1-32> (name WORD|) state (enable | disable)
no vlan VLAN_RANGE bridge <1-32>
```

Parameters

VLAN_RANGE
The vlan-id or range of vlan-id's separated by ','&'-'

bridge
Specify the bridge group ID in the range <1-32>.

state
Indicates the operational state of the VLAN.

enable
Sets VLAN into an enable state.

disable
Sets VLAN into a disable state.

Default

By default, vlan bridge state is disabled

Command Mode

Configure mode

VLAN mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#vlan 3-40,56 bridge 4
(config)#no vlan 2-5 bridge 2
```

© 2026 IP Infusion Inc. Proprietary

vlan VLAN_RANGE type customer

This command allows you to create a single/range of VLAN's of the type Customer VLAN in Provider Edge bridges.

Use the `no` form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE (type (customer)|) bridge <1-32> (name WORD|) (state (disable|enable)|)
no vlan VLAN_RANGE type (customer) bridge <1-32>
no vlan VLAN_RANGE bridge <1-32>
```

Parameters

VLAN_RANGE
VLAN ID 2-4094 or range(s): 2-5,10 or 2-5,7-19

bridge
Specify the bridge group ID in the range <1-32>.

WORD
The ascii name of the VLAN

state
Indicates the operational state of the VLAN.

enable
Sets VLAN into an enable state.

disable
Sets VLAN into a disable state.

customer
Customer VLAN

Default

By default, vlan customer state is disabled

Command Mode

Configure mode

VLAN mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config-vlan)#vlan 15 type customer bridge 1 name abcde state enable
(config-vlan)#vlan 2-10,15 type customer bridge 1 state enable
(config-vlan)#no vlan 2-10,15 type customer bridge 1
(config-vlan)#
(config)#no vlan 2-10,15 br 1
(config)#end
#
```

© 2026 IP Infusion Inc. Proprietary

vlan VLAN_RANGE type service

This command allows you to create a single/range of VLAN's of the type Service VLAN in Provider Edge & provider network bridges.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE type service (point-point|multipoint-multipoint|rooted-multipoint) bridge <1-32>
(state (disable|enable)|)

vlan VLAN_RANGE type service (point-point|multipoint-multipoint|rooted-multipoint) bridge <1-32> name
WORD (state (disable|enable)|)

no vlan VLAN_RANGE type service bridge <1-32>
```

Parameters

VLAN_RANGE
VLAN ID 2-4094 or range(s): 2-5,10 or 2-5,7-19

service
service VLAN

multipoint-multipoint
Service Multipoint to Multipoint Service VLAN

point-point
Service Point-to-Point Service VLAN

rooted-multipoint
Service Rooted Multipoint Service VLAN

bridge
Specify the bridge group ID in the range <1-32>.

WORD
The ascii name of the VLAN

state
Operational state of the VLAN

disable
Disable VLAN status on the bridge

enable
Enable VLAN status on the bridge

Default

By default, with the name WORD this can only be given in "vlan database" mode.

Command Mode

Configure mode

VLAN mode

© 2026 IP Infusion Inc. Proprietary

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#vlan database
(config-vlan)#vlan 100 type service multipoint-multipoint bridge 1 name xxxx state enable
(config-vlan)#vlan 101 type service point-point bridge 1 name afsa state disable

(config-vlan)#vlan 102 type service rooted-multipoint bridge 1 state enable
(config)#vlan 104-107 type service multipoint-multipoint bridge 1 state enable
(config)#vlan 114-117,119 type service multipoint-multipoint bridge 1 state enable
(config)#vlan 124-127,129 type service point-point bridge 1 state enable
(config)#no vlan 114-117,119 type service br 1
```

© 2026 IP Infusion Inc. Proprietary

VLAN Cross-Connect Commands

This chapter contains VLAN cross-connect commands.

cross-connect 609
disable 610
outer-vlan VLAN_RANGE2 (inner-vlan VLAN_RANGE2 |) 612
show cross-connect 613

© 2026 IP Infusion Inc. Proprietary

cross-connect

Use this command to enter VLAN cross-connect mode to configure cross-connect parameters.

Use the `no` form of this command to delete a cross-connect.

Command Syntax

```
cross-connect WORD
no cross-connect WORD
```

Parameters

WORD

Cross-connect name, length <1-255>

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#cross-connect VC1
(config-XC)#

#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#no cross-connect VC1
(config)#
```

© 2026 IP Infusion Inc. Proprietary

disable

Use this command to make a cross-connect administratively disabled or enabled.

Command Syntax

```
disable
no disable
```

Parameters

None

Command Mode

Cross-connect mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
OcNOS#sh cross-connect
Cross-connect name : VC1
EP1:ce24/1     EP2:ce31/1     Admin Status:UP         Oper Status:UP
+=============================================================================================================
==============+
| EP       | OVID     | IVID     | Rx packets    | Rx bytes      | Tx packets    |Tx
bytes       |Interface Status|
+=============================================================================================================
==============+
| EP1      |100       |     -
    |0              |0              |0              |0              |UP             |
| EP2      |100       |     -
    |0              |0              |0              |0              |UP             |
+=============================================================================================================
==============+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
OcNOS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#cross-connect VC1
OcNOS(config-XC)#disable
2021 Mar 22 07:35:30.083 : OcNOS : NSM : CRITI : [VXC_DOWN_2]: Cross_Connect VC1 changed state to
down
OcNOS(config-XC)#end
OcNOS#sh cross-connect
ross-connect name : VC1
EP1:ce24/1     EP2:ce31/1     Admin Status:DOWN       Oper Status:DOWN
+=============================================================================================================
==============+
| EP       | OVID     | IVID     | Rx packets    | Rx bytes      | Tx packets    |Tx
bytes       |Interface Status|
+=============================================================================================================
==============+
| EP1      |     -    |     -
```

```
    |0              |0              |0              |0              |UP             |
| EP2       |     -    |     -
    |0              |0              |0              |0              |UP             |
+=============================================================================================================
==============+

cross-connect summary
Total XC    : 1
Admin Up    : 0
Admin Down  : 1
Total Rules : 0

OcNOS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#cross-connect VC1
OcNOS(config-XC)#no disable
OcNOS(config-XC)#2021 Mar 22 07:35:46.814 : OcNOS : NSM : CRITI : [VXC_UP_2]: Cross_Connect VC1
changed state to up
OcNOS#sh cross-connect
Cross-connect name : VC1
EP1:ce24/1     EP2:ce31/1     Admin Status:UP         Oper Status:UP
+=============================================================================================================
==============+
| EP        | OVID     | IVID     | Rx packets    | Rx bytes      | Tx packets    |Tx
bytes       |Interface Status|
+=============================================================================================================
==============+
| EP1*      |     -    |     -
    |47836          |47836000       |0              |0              |UP             |
| EP2*      |     -    |     -
    |0              |0              |48149          |48149000       |UP             |
+=============================================================================================================
==============+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

outer-vlan VLAN_RANGE2 (inner-vlan VLAN_RANGE2 |)

Use this command to configure parameters for VLAN cross-connect.

Command Syntax

```
outer-vlan VLAN_ID inner-vlan VLAN_ID ep1 IFNAME ep2 IFNAME
```

Parameters

outer-vlan
Outer-VLAN associated with the cross-connect

VLAN ID
VLAN ID <2 - 4094>

inner-vlan
Inner-VLAN associated with the cross-connect

VLAN ID
VLAN ID <2 - 4094>

ep1
Interface for cross-connect endpoint 1

IFNAME
Interface name for endpoint 1

ep2
Interface for cross-connect endpoint 2

IFNAME
Interface name for endpoint 2

Command Mode

Cross-connect mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#conf t
Enter configuration commands, one per line.   End with CNTL/Z. (config)#cross-connect VC1
(config-XC)#vlan ep1 ce25/1 ep2 ce16/1
(config-VXC)#outer-vlan 10 inner-vlan 20
(config-VXC)#
```

© 2026 IP Infusion Inc. Proprietary

show cross-connect

Use this command to display the VLAN cross-connect configuration.

Command Syntax

```
show cross-connect
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
OcNOS#sh cross-connect
Cross-connect name : VC1
EP1:ce25/1     EP2:ce16/1     Admin Status:UP         Oper Status:UP
+=============================================================================================================
==============+
| EP       | OVID     | IVID     | Rx packets    | Rx bytes      | Tx packets    |Tx
bytes       |Interface Status|
+=============================================================================================================
==============+
| EP1      |100       |     -
    |0              |0              |0              |0              |UP             |
| EP2      |100       |     -
    |0              |0              |0              |0              |UP             |
+=============================================================================================================
==============+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

802.1x Commands

This section describes the 802.1X commands.

auth-mac 615
auth-mac dynamic-vlan-creation 616
auth-mac mac-aging 617
auth-mac mode 618
auth-mac system-auth-ctrl 619
auth-port 620
dot1x port-control 621
dot1x protocol-version 622
dot1x quiet-period 623
dot1x reauthentication 624
dot1x reauthMax 625
dot1x system-auth-ctrl 626
dot1x timeout re-authperiod 627
dot1x timeout server-timeout 628
dot1x timeout supp-timeout 629
dot1x timeout tx-period 630
ip radius source-interface 631
key-string 632
key-string encrypted 633
radius-server dot1x host 634
retransmit 635
show debugging dot1x 636
show dot1x 637

© 2026 IP Infusion Inc. Proprietary

auth-mac

Use this command to enable MAC based authentication standalone on the interface level.

Use the `no` form of this command to disable/remove the auth-MAC from interface level.

Command Syntax

```
auth-mac
no auth-mac
```

Parameters

None.

Default

Command message will not be displayed and disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac
(config-if)#commit

#configure terminal
(config)#interface eth0
(config-if)#no auth-mac
(config-if)#commit
(config-if)#end
```

© 2026 IP Infusion Inc. Proprietary

auth-mac dynamic-vlan-creation

Use this command to enable dynamic VLAN creation after successful MAC authentication.

Use the `no` parameter of the command to disable dynamic VLAN creation.

Command Syntax

```
auth-mac dynamic-vlan-creation
no auth-mac dynamic-vlan-creation
```

Parameters

None

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#no auth-mac dynamic-vlan-creation

#configure terminal
(config)#interface eth0
(config-if)#auth-mac dynamic-vlan-creation
```

© 2026 IP Infusion Inc. Proprietary

auth-mac mac-aging

Use this command to enable MAC aging. When enabled, a MAC entry is added to the forwarding database, with aging time equal to the bridge aging time. Otherwise, the MAC entry will not be aged out.

If MAC aging is disabled, the MAC entry will not be aged out.

Use the `no` parameter of this command to disable MAC aging.

Command Syntax

```
auth-mac mac-aging
no auth-mac mac-aging
```

Parameters

None

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#no auth-mac mac-aging

#configure terminal
(config)#interface eth0
(config-if)#auth-mac mac-aging
```

© 2026 IP Infusion Inc. Proprietary

auth-mac mode

Use this command to enable MAC authentication mode on an interface.

Use the `no` parameter with this command to disable MAC authentication mode on an interface.

Command Syntax

```
auth-mac mode (filter|shutdown)
no auth-mac mode
```

Parameters

filter
Filter the frames for the MAC when in an unauthorized state.

shutdown
Shut down the interface when the MAC is unauthenticated.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac mode filter
(config-if)#commit

#configure terminal
(config)#interface eth0
(config-if)#no auth-mac mode
(config-if)#commit
```

© 2026 IP Infusion Inc. Proprietary

auth-mac system-auth-ctrl

Use this command to enable MAC authentication globally. If MAC authentication is not enabled, other MAC authentication related commands throw an error when issued.

Use the `no` parameter with this command to disable MAC authentication globally.

Command Syntax

```
auth-mac system-auth-ctrl
no auth-mac system-auth-ctrl
```

Parameters

None

Default

Authentication system messages are not displayed.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#auth-mac system-auth-ctrl

(config)#no auth-mac system-auth-ctrl
```

© 2026 IP Infusion Inc. Proprietary

auth-port

Use this command to specify a port for Radius authentication.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
auth-port <1-65535>
no auth-port
```

Parameters

<0-65535>
Port number.

Default

The default port number is 1812.

Command Mode

Configure Radius server mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Examples

```
#configure terminal
(config)#radius-server dot1x host 1.1.1.1
(config-radius-server)#auth-port 1233
(config-radius-server)#no auth-port
```

© 2026 IP Infusion Inc. Proprietary

dot1x port-control

Use this command to force a port state.

Use the `no` parameter with this command to remove a port from the 802.1x management.

Command Syntax

```
dot1x port-control (force-unauthorized|force-authorized|auto)
no dot1x port-control
```

Parameters

auto
Specify to enable authentication on port.

force-authorized
Specify to force a port to always be in an authorized state.

force-unauthorized
Specify to force a port to always be in an unauthorized state.

Default

The dot1x port-control default is active.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x port-control auto

(config)#interface eth0
(config-if)#no dot1x port-control
```

© 2026 IP Infusion Inc. Proprietary

dot1x protocol-version

Use this command to set the protocol version of dot1x to 1 or 2. The protocol version must be synchronized with the Xsupplicant being used in that interface.

Use the `no` parameter with this command to set the protocol version to the default value (2).

Command Syntax

```
dot1x protocol-version <1-2>
no dot1x protocol-version
```

Parameters

<1-2>
Indicates the EAP Over LAN (EAPOL) version.

Default

The default dot1x protocol version is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x protocol-version 2

(config)#interface eth0
(config-if)#no dot1x protocol-version
```

© 2026 IP Infusion Inc. Proprietary

dot1x quiet-period

Use this command to set the quiet-period time interval.

When a switch cannot authenticate a client, the switch remains idle for a quiet-period interval of time, then tries again. By administratively changing the quiet-period interval, by entering a lower number than the default, a faster response time can be provided.

Use the `no` parameter with this command to set the configured quiet period to the default (60 seconds).

Command Syntax

```
dot1x quiet-period <1-65535>
no dot1x quiet-period
```

Parameter

<1-65535>
Seconds between the retrial of authentication.

Default

The default dot1x quiet-period is 60.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x quiet-period 200
```

© 2026 IP Infusion Inc. Proprietary

dot1x reauthentication

Use this command to enable reauthentication on a port.

Use the `no` parameter to disable reauthentication on a port.

Command Syntax

```
dot1x reauthentication
no dot1x reauthentication
```

Parameters

None

Default

The dot1x reauthentication default is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x reauthentication
```

© 2026 IP Infusion Inc. Proprietary

dot1x reauthMax

Use this command to set the maximum reauthentication value, which sets the maximum number of reauthentication attempts after which the port will be unauthorized.

Use the `no` parameter with this command to set the reauthentication maximum to the default value (2).

Command Syntax

```
dot1x reauthMax <1-10>
no dot1x reauthMax
```

Parameter

<1-10>

Indicates the maximum number of reauthentication attempts after which the port will be unauthorized.

Default

The default is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following sets the maximum reauthentication value to 5.

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x reauthMax 5
```

The following sets the reauthentication maximum to the default value.

```
#configure terminal
(config)#interface eth0
(config-if)#no dot1x reauthMax
```

© 2026 IP Infusion Inc. Proprietary

dot1x system-auth-ctrl

Use this command to enable globally authentication.

Use the `no` parameter to disable globally authentication.

Command Syntax

```
dot1x system-auth-ctrl
no dot1x system-auth-ctrl
```

Parameters

None

Default

Authentication is off by default.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#dot1x system-auth-ctrl
```

© 2026 IP Infusion Inc. Proprietary

dot1x timeout re-authperiod

Use this command to set the interval between reauthorization attempts.

Use the `no` parameter to disable the interval between reauthorization attempts.

Command Syntax

```
dot1x timeout re-authperiod <1-4294967295>
no dot1x timeout re-authperiod
```

Parameter

<1-4294967295>
Specify the seconds between reauthorization attempts.

Default

Default time is 3600 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout re-authperiod 25
```

© 2026 IP Infusion Inc. Proprietary

dot1x timeout server-timeout

Use this command to set the authentication sever response timeout.

Use the `no` parameter to disable the authentication sever response timeout.

Command Syntax

```
dot1x timeout server-timeout <1-65535>
no dot1x timeout server-timeout
```

Parameter

<1-65535>
Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout server-timeout 555

(config)#interface eth0
(config-if)#no dot1x timeout server-timeout
```

© 2026 IP Infusion Inc. Proprietary

dot1x timeout supp-timeout

Use this command to set the interval for a supplicant to respond.

Use the `no` parameter to disable the authentication sever response timeout.

Command Syntax

```
dot1x timeout supp-timeout <1-65535>
no dot1x timeout supp-timeout
```

Parameter

<1-65535>
Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout supp-timeout 40

(config)#interface eth0
(config-if)#no dot1x timeout supp-timeout
```

© 2026 IP Infusion Inc. Proprietary

dot1x timeout tx-period

Use this command to set the interval between successive attempts to request an ID.

Use the `no` parameter to disable the interval between successive attempts to request an ID.

Command Syntax

```
dot1x timeout tx-period <1-65535>
no dot1x timeout tx-period
```

Parameter

<1-65535>
Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout tx-period 34

(config)#interface eth0
(config-if)#no dot1x timeout tx-period
```

© 2026 IP Infusion Inc. Proprietary

ip radius source-interface

Use this command to set the local address sent in packets to the radius server.

Use the `no` parameter to clear the local address.

Command Syntax

```
ip radius source-interface A.B.C.D <1-65535>
no ip radius source-interface
```

Parameters

A.B.C.D
IPv4 address of the RADIUS server.

<1-65535>
Port number.

Default

The default port number is 1812.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip radius source-interface 12.12.12.1 1812
(config)#no ip radius source-interface
```

© 2026 IP Infusion Inc. Proprietary

key-string

Use this command to define a password in plain text.

The password is stored as encrypted and is displayed in encrypted text when the `show running-config` command is executed.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
key-string WORD
no key-string
```

Parameter

WORD
A string of characters to use as a password (1-64 characters).

Default

By default, the password is not configured.

Command Mode

Configure Radius server mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Examples

```
#configure terminal
(config)#radius-server dot1x host 1.1.1.1
(config-radius-server)#key-string 1234567890
(config-radius-server)#no key-string
```

© 2026 IP Infusion Inc. Proprietary

key-string encrypted

Use this command to define a password in encrypted format.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
key-string encrypted WORD
no key-string
```

Parameter

WORD

A string of characters to use as a password (18-130 characters).

Default

By default, password is not configured.

Command Mode

Configure Radius server mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Examples

```
#configure terminal
(config)#radius-server dot1x host 1.1.1.1
(config-radius-server)#key-string encrypted 0x16176d21cc1688d995
(config-radius-server)#no key-string
```

© 2026 IP Infusion Inc. Proprietary

radius-server dot1x host

Use this command to specify the IP address of the remote radius server host and assign authentication and accounting destination port numbers. Multiple radius-server host commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified.

If no host-specific auth-port (page 620), timeout, retransmit (page 635), key-string (page 632), or key-string encrypted (page 633) values are specified, the global default values apply to that host.

Use the `no` form of the command to unconfigure a specified radius-server.

Command Syntax

```
radius-server dot1x host (A.B.C.D)
no radius-server dot1x host (A.B.C.D)
```

Parameters

dot1x
IEEE 802.1X Port-Based Access Control.

A.B.C.D
IPv4 address of the RADIUS server.

Default

The default value of auth-port is 1812.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server dot1x host 1.1.1.1
(config-radius-server)#
(config)#no radius-server dot1x host 1.1.1.1
```

© 2026 IP Infusion Inc. Proprietary

retransmit

Use this command to specify the number of times to transmit each Radius request to the server before giving up.

Use the `no` form of this command to disable retransmission.

Command Syntax

```
retransmit <0-100>
no retransmit
```

Parameter

<0-100>
Number of times to transmit each Radius request (0-100).

Default

The default value is 3.

Command Mode

Configure Radius server mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Examples

```
#configure terminal
(config)#radius-server dot1x host 1.1.1.1
(config-radius-server)#retransmit 12
(config-radius-server)#no retransmit
```

© 2026 IP Infusion Inc. Proprietary

show debugging dot1x

Use this command to display the status of the debugging of the 802.1x system.

Command Syntax

```
show debugging dot1x
```

Parameters

None

Command Mode

Privileged execution mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

```
#show debugging dot1x
802.1X debugging status:
```

show dot1x

Use this command to display the state of the whole system.

Command Syntax

```
show dot1x
show dot1x all
show dot1x host
show dot1x diagnostics interface IFNAME
show dot1x interface IFNAME
show dot1x sessionstatistics (interface IFNAME|)
show dot1x statistics interface IFNAME
```

Parameters

all
Display all information.

host
Show operational radius-server dot1x host information for a specific host (IPv4 address) or for all hosts.

diagnostics
Display diagnostics information.

interface
Display diagnostics interface information.

interface
Display interface information.

sessionstatistics
Display session statistics.

interface
Display session statistics interface information.

statistics
Display statistics information.

interface
Display statistics interface information.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Displayed Output

The following tables describes the output for the show dot1x all command and the show dot1x interface command.

© 2026 IP Infusion Inc. Proprietary

Table 25. Port variables

Entry	Description
portEnabled	Interface operational status (Up-true/down-false)
portControl	Current control status of the port for 802.1x control
portStatus	802.1x status of the port (authorized/unauthorized)
reAuthenticate	Reauthentication enabled/disabled status on port
reAuthPeriod	Value holds meaning only if reAuthentication is enabled

Table 26. Supplicant PAE related global variables

Entry	Description
abort	Indicates that authentication should be aborted when set to true
fail	Indicates failed authentication attempt when set to false
start	Indicates authentication should be started when set to true
timeout	Indicates authentication attempt timed out when set to true
success	Indicates authentication successful when set to true

Table 27. 802.1x Operational State of Interface

Entry	Description
mode	Configured 802.1x mode
reAuthCount	Reauthentication count
quietperiod	Time between reauthentication attempts
reAuthMax	Maximum reauthentication attempts

Table 28. Backend Authentication state machine variables and constants

Entry	Description
state	State of the state machine
reqCount	Count of requests sent to server
suppTimeout	Supplicant timeout
serverTimeout	Server timeout
maxReq	Maximum requests to be sent

Table 29. Controlled Directions State machine

Entry	Description
adminControlledDirections	Administrative value (Both/In)
operControlledDirections	Operational Value (Both/In)

© 2026 IP Infusion Inc. Proprietary

Table 30. KR -- Key receive state machine

Entry	Description
rxKey	True when EAPOL-Key message is received by supplicant or authenticator. false when key is transmitted

Table 31. Key Transmit State machine

Entry	Description
keyAvailable	False when key has been transmitted by authenticator, true when new key is available for key exchange
keyTxEnabled	Key transmission enabled/disabled status

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is an output of this command displaying the state of the system.

```
#show dot1x
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.mySite.com.12103
% Next radius message id: 0
```

The following is an output of this command displaying detailed information for all ports.

```
#show dot1x all
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.mySite.com.12103
% Next radius message id: 0
% Dot1x info for interface eth1 - 3
%  portEnabled: true - portControl: auto
%  portStatus: unauthorized - currentId: 11
%  reAuthenticate: disabled
%  abort:F fail:F start:F timeout:F success:F
%  PAE: state: connecting - portMode: auto
%  PAE: reAuthCount: 2 - rxRespId: 0
%  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
%  BE: state: idle - reqCount: 0 - idFromServer: 0
%  BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2
%  CD: adminControlledDirections: in - operControlledDirections: in
%  CD: bridgeDetected: false
%  KR: rxKey: false
%  KT: keyAvailable: false - keyTxEnabled: false
```

© 2026 IP Infusion Inc. Proprietary

Layer 2 Control Protocols Tunneling Commands

This section is a reference for the Layer 2 Control Protocols (L2CP) tunneling commands:

clear l2protocol interface counters 641
l2protocol 642
l2protocol encapsulation dest-mac 644
show l2protocol interface counters 646
show l2protocol processing interface 647

© 2026 IP Infusion Inc. Proprietary

clear l2protocol interface counters

This command allows you to clear the counters for numbers of packets peered, discarded and tunneled.

Command Syntax

```
clear l2protocol interface (IFNAME|) counters (peer|discard|tunnel|tunnel-discard|)
```

Parameters

peer
Clear stats for Peer protocol packets.

discard
Clear stats for Tunnel protocol packets.

tunnel
Clear stats for Tunnel protocol packets.

tunnel-discard
Clear stats for Tunnel discard protocol packets.

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
# clear l2protocol interface xe1 counters peer
```

© 2026 IP Infusion Inc. Proprietary

l2protocol

This command allows you to change the process of protocol to peer/discard/tunnel.

Command Syntax

```
l2protocol (stp|lacp|efm|elmi|lldp|synce)(peer|discard|tunnel)
```

Parameters

stp
Spanning Tree Protocols.

lacp
Link Aggregation (LACP).

efm
Ethernet first mile (Link OAM).

elmi
Ethernet local management interface.

lldp
Link layer discovery protocol.

synce
Link layer discovery protocol.

peer
Act as peer to the customer Device instance of the protocol.

discard
Discard the protocol data unit.

tunnel
Tunnel the Protocol data unit into the SVLAN.

Default

Default process value is peer.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode customer-edge access
(config-if)#l2protocol stp tunnel
```

© 2026 IP Infusion Inc. Proprietary

```
(config-if)#l2protocol stp peer
(config-if)#l2protocol stp discard
```

l2protocol encapsulation dest-mac

Use this command to change destination mac of tunneled l2 protocol packet. Allowed mac are 0100.C2CD.CDD0 or 0104.DFCD.CDD0.

Use the `no` parameter with this command to set default mac 0100.C2CD.CDD0.

Note: This command only applies to provider bridging. For more information, Refer Provider Bridging Configuration.

Command Syntax

```
bridge <1-32> l2protocol encapsulation dest-mac XXXX.XXXX.XXXX
no bridge <1-32> l2protocol encapsulation dest-mac
```

Parameters

bridge
Bridge group for bridging.

<1-32>
<1-32>

l2protocol
Configure Layer2 Protocol Tunneling.

encapsulation
Encapsulation of L2PT packet.

dest-mac
Encapsulation with destination mac.

XXXX.XXXX.XXXX
Destination Mac-address of L2PT tunneling (0100.C2CD.CDD0 or 0104.DFCD.CDD0).

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 3.0.

Examples

```
(config)#bridge 1 l2protocol encapsulation dest-mac ?
XXXX.XXXX.XXXX Destination Mac-address of L2PT tunneling (0100.C2CD.CDD0 or
0104.DFCD.CDD0)
(config)#bridge 1 l2protocol encapsulation dest-mac 0104.DFCD.CDD1
L2PT destination mac should be 0100.C2CD.CDD0 or 0104.DFCD.CDD0
(config)#bridge 1 l2protocol encapsulation dest-mac 0104.DFCD.CDD0
(config)#bridge 1 l2protocol encapsulation dest-mac 0100.C2CD.CDD0
(config)#bridge 1 l2protocol encapsulation dest-mac 0100.C2CD.CDD1
L2PT destination mac should be 0100.C2CD.CDD0 or 0104.DFCD.CDD0
(config)#
```

© 2026 IP Infusion Inc. Proprietary

```
(config)#no bridge 1 l2protocol encapsulation dest-mac
(config)#show running-config | in bridge
bridge 1 protocol provider-rstp edge
vlan 2-10 type customer bridge 1 state enable
vlan 11-12 type service point-point bridge 1 state enable
cvlan registration table map1 bridge 1
bridge-group 1
bridge-group 1
(config)#
```

© 2026 IP Infusion Inc. Proprietary

show l2protocol interface counters

This command allows you to display the counters for numbers of packets peered, discarded and tunneled.

Notes:

- In case of Provider-Bridging, tunneling will be done via slow path forwarding (via CPU).
- And for other tunneling feature such as L2VPN, EVPN cases, L2protocol will follow hardware forwarding path to be tunneled.
- Except Provider-Bridging feature, for other tunneling feature such as L2VPN/EVPN cases, tunnel counters will not be captured. Peering and discarding decision will be taken at CPU, hence, these counters will be captured with this show command.

Command Syntax

```
show l2protocol interface (IFNAME|) counters (peer|discard|tunnel|tunnel-discard|)
```

Parameters

peer
Display stats for Peer protocol packets.

discard
Display stats for Tunnel protocol packets.

tunnel
Display stats for Tunnel protocol packets.

tunnel-discard
Display stats for Tunnel discard protocol packets.

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
# show l2protocol interface xe1 counters peer
Interface xe1
Peer:     stp:    1

# show l2protocol interface xe1 counters
Interface xe1
Peer:     stp:    1
Discard:  stp:    10
Tunnel:   stp:    5
```

© 2026 IP Infusion Inc. Proprietary

show l2protocol processing interface

This command allows you to display the processing information on Layer 2 protocol interface.

Command Syntax

```
show l2protocol processing interface IFNAME
```

Parameters

IFNAME
Interface name

Command Mode

Execution mode and Privileged execution mode

Applicability

This command is introduced was before OcNOS version 3.0.

Examples

```
#show l2protocol processing interface xe1/1
Bridge    Interface Name                  Protocol       Processing Status
======    ==============                  ========       =================
1         xe1/1                            stp            Tunnel
1         xe1/1                            gmrp           Peer
1         xe1/1                            gvrp           Peer
1         xe1/1                            mmrp           Peer
1         xe1/1                            mvrp           Peer
1         xe1/1                            lacp           Peer
1         xe1/1                            lldp           Peer
1         xe1/1                            efm            Peer
1         xe1/1                            elmi           Peer
1         xe1/1                            ptp            Peer
1         xe1/1                            synce          Peer
```

© 2026 IP Infusion Inc. Proprietary

Provider Bridging Commands

This section describes the Provider Bridging (PB) commands.

IEEE 802.1ad standardizes the architecture and bridged protocols to allow Ethernet frames with multiple VLAN tags. Packets through a provider network are doubly tagged with both an:

- Inner (C-VLAN) tag which is the customer network VLAN identifier
- Outer (S-VLAN) tag which is the service provider network VLAN identifier

bridge protocol provider-mstp 649
bridge protocol provider-rstp 650
cvlan registration table 651
cvlan svlan 652
dot1ad ethertype 654
show cvlan registration table 655
switchport customer-edge 656
switchport customer-edge hybrid 657
switchport customer-edge trunk 658
switchport customer-edge vlan registration 659
switchport customer-network allowed vlan 660
switchport customer-network vlan 661
switchport mode 662
switchport mode customer-edge 663
switchport mode customer-edge hybrid acceptable-frame-type 664
switchport provider-network 665
switchport provider-network isolated-vlan 666
vlan type 667
vlan type customer 668

© 2026 IP Infusion Inc. Proprietary

bridge protocol provider-mstp

Use this command to create a provider multiple spanning-tree protocol (MSTP) bridge. MSTP bridges can have different spanning-tree topologies for different VLANs inside a region of similar MSTP bridges.

Using this command creates an instance of the spanning tree, and associates the VLANs specified with that instance. A bridge created by this command forms its own separate region.

The multiple spanning tree protocol, like the rapid spanning tree protocol, provides rapid reconfiguration features, while providing load-balancing capability.

Command Syntax

```
bridge <1-32> protocol provider-mstp (edge|)
```

Parameters

<1-32>
Bridge identifier.

edge
Configure as an edge bridge.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 2 protocol provider-mstp edge
```

© 2026 IP Infusion Inc. Proprietary

bridge protocol provider-rstp

Use this command to add an IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in interface mode.

Command Syntax

```
bridge <1-32> protocol provider-rstp (edge|)
```

Parameters

<1-32>
Bridge identifier.

edge
Configure as an edge bridge.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 2 protocol provider-rstp edge
```

© 2026 IP Infusion Inc. Proprietary

cvlan registration table

Use this command to create a customer VLAN (CVLAN) registration table that maps between CVLANs and service provider VLANs (SVLANs).

Use the no parameter with this command to delete the CVLAN registration table.

Command Syntax

```
cvlan registration table WORD bridge <1-32>
no cvlan registration table WORD bridge <1-32>
```

Parameters

WORD
Name of the CVLAN registration table.

<1-32>
Specify a bridge ID.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#cvlan registration table customer1
(config-cvlan-registration)#
```

cvlan svlan

Use this command to map one or more customer VLANs (CVLANs) to a service provider VLAN (SVLAN).

To update the optional QoS parameters cos-to-queue and remark-cos, execute the complete command along with the optional parameters. To remove these options, execute the same command by removing the optional parameters.

Refer `qos profile` commands from configuration guide for more details about qos profiles.

Use the `no` forms of this command to delete a mapping.

Command Syntax

```
cvlan VLAN_RANGE2 (cvlan VLAN_ID|) svlan VLAN_ID ({untagged-pep|untagged-cep}|)({cos-to-queue NAME |
remark-cos}|)
no cvlan VLAN_RANGE2  svlan VLAN_ID
```

Parameters

cvlan
CVLAN

VLAN_RANGE2
VLAN identifier <1-4094> or range such as 2-5,10 or 2-5,7-19

cvlan
Translation of CVID

VLAN_ID
Translated CVID <1-4095>

svlan
SVLAN corresponding to the C-VLAN

VLAN_ID
VLAN identifier 1-4094>

untagged-pep
Provider edge port is untagged for this CVLAN

untagged-cep
Customer edge port is untagged for this CVLAN

cos-to-queue
Configure cos-to-queue map for cvlan

NAME
Ingress profile to modify queue/color on basis of c-cos

remark-cos
Remark Egress COS

Command Mode

CVLAN Registration mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 3.0.

© 2026 IP Infusion Inc. Proprietary

Example

```
#configure terminal
(config)#cvlan registration table customer1 bridge 1
(config-cvlan-registration)#cvlan 2 svlan 3
(config-cvlan-registration)#cvlan 3 svlan 3 cos-to-queue c1 remark-cos
(config-cvlan-registration)#cvlan 100 cvlan 101 svlan 200 cos-to-queue p1 remark-cos
(config-cvlanregistration)#cvlan 3 svlan 3 remark-cos
(config-cvlan-registration)#cvlan 4 svlan 5 untagged-pep
(config-cvlan-registration)#cvlan 5 svlan 6 untagged-cep
(config-cvlan-registration)#no cvlan 3 svlan 3
(config-cvlan-registration)#cvlan 23 svlan 31 untagged-pep untagged-cep cos-to-queue p1 remark-cos
(config-cvlan-registration)#cvlan 15-16 svlan 18 untagged-cep remark-cos
```

© 2026 IP Infusion Inc. Proprietary

dot1ad ethertype

Use this command to change the TPID for a port.

Use the no form of this command to set the TPID to its default value.

Command Syntax

```
dot1ad ethertype (0x8100 | 0x88a8 | 0x9100 | 0x9200)
no dot1ad ethertype
```

Parameters

0x8100
IEEE 802.1Q VLAN-tagged frame

0x88a8
IEEE 802.1ad Provider Bridging Service VLAN tag identifier (S-Tag)

0x9100
Supported for interoperability with legacy devices

0x9200
Supported for interoperability with legacy devices

Default

The default TPID value is 8100.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
(config)#interface xe1
(config-if)#dot1ad ethertype 0x9100
(config-if)#exit
(config)#interface xe1
(config-if)#no dot1ad ethertype
(config-if)#exit
```

© 2026 IP Infusion Inc. Proprietary

show cvlan registration table

Use this command to display the CVLAN registration table.

Command Syntax

```
show cvlan registration table (WORD|bridge <1-32>|WORD bridge <1-32>|)
```

Parameters

WORD
CVLAN registration table name.

<1-32>
Bridge identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh cvlan registration table bridge 1
Bridge          Table Name       Port List
======          ==========       =========
  1               map              xe17

CVLAN ID      T-CVLAN ID     SVLAN ID     Profile Name    Egress remark-Cos
 ========    ==========      ========    =============    =================
 100             101             200          p1              Yes
```

Table 32 explains the output fields.

Table 32. show cvlan registration table output

Entry	Description
Bridge	ID number of the bridge associated with the Customer VLAN (CVLAN).
Table Name	ID of the CVLAN registration table.
Port List	List of ports used by this CVLAN (including Link aggregators).
CVLAN ID	ID number of the CVLAN.
T-CVLAN ID	Translation CVLAN ID.
SVLAN ID	ID number of the Service VLAN (SVLAN) associated with the CVLAN.
Profile Name	cos-to-queue profile name.
Egress remark-Cos	Remark Egress Cos

© 2026 IP Infusion Inc. Proprietary

switchport customer-edge

Use this command to set the switching characteristics of the layer 2 interface and the default customer VLAN.

Use the no form of this command to remove a customer VLAN.

Command Syntax

```
switchport customer-edge (access|hybrid) vlan <1-4094>
no switchport customer-edge (access|hybrid) vlan
```

Parameters

access
Set the layer 2 interface as access.

hybrid
Set the layer 2 interface as hybrid.

<1-4094>
Set the default VID for the interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport customer-edge access vlan 3
(config)#interface eth0
(config-if)#no switchport customer-edge access vlan
```

© 2026 IP Infusion Inc. Proprietary

switchport customer-edge hybrid

Use this command to set the switching characteristics of the Layer 2 customer-facing interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.

Command Syntax

```
switchport customer-edge hybrid allowed vlan add VLAN_ID
switchport customer-edge hybrid allowed vlan remove VLAN_ID
switchport customer-edge hybrid allowed vlan all
switchport customer-edge hybrid allowed vlan none
```

Parameters

add
Add a VLAN to transmit and receive through the Layer 2 interface.

VLAN_ID
ID of the VLAN <1-4094>.

remove
Remove a VLAN from the member set.

VLAN_ID
ID of the VLAN <1-4094>.

all
Allow all VLANs to transmit and receive through the Layer 2 interface.

none
Allow no VLANs to transmit and receive through the Layer 2 interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#switchport customer-edge hybrid allowed vlan add 2
```

© 2026 IP Infusion Inc. Proprietary

switchport customer-edge trunk

Use this command to set the Layer2 interface as trunk.

Command Syntax

```
switchport customer-edge trunk allowed vlan add VLAN_ID
switchport customer-edge trunk allowed vlan remove VLAN_ID
switchport customer-edge trunk allowed vlan all
switchport customer-edge trunk allowed vlan none
```

Parameters

add
Add a VLAN to the member set.

VLAN_ID
Specify a VLAN ID <2-4094>

remove
Remove a VLAN from the member set.

all
Allow all VLANs to transmit and receive through the Layer 2 interface.

none
Allow no VLANs to transmit and receive through the Layer 2 interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#switchport customer-edge trunk allowed vlan add 12
```

© 2026 IP Infusion Inc. Proprietary

switchport customer-edge vlan registration

Use this command to configure the VLAN registration parameters.

Use the no parameter with this command to delete the mapping from the interface.

Command Syntax

```
switchport customer-edge vlan registration WORD
no switchport customer-edge vlan registration
```

Parameters

WORD
Name of the CVLAN registration table.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#switchport customer-edge vlan registration customer1
```

switchport customer-network allowed vlan

Use this command to add SVLAN IDs to the Customer Network Port.

Customer-Network Port Command Syntax

```
switchport customer-network allowed vlan add VLAN_RANGE
```

Parameters

VLAN_RANGE
VLAN identifier <1-4094> or range such as 2-5,10 or 2-5,7-19.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 6.2.0.

Examples

In this example, the xe1 interface allows S-TAG 100-200 and 400 traffic from customer.

```
(config)#interface xe1
(config-if)#switchport
(config-if)#dot1ad ethertype 0x88a8
(config-if)#bridge-group 1
(config-if)#switchport mode customer-network
(config-if)#switchport customer-network allowed vlan add 100-200,400
```

© 2026 IP Infusion Inc. Proprietary

switchport customer-network vlan

Use this command to set the default SVLAN ID for the Customer Network Port.

Note: Customer-Network Port is not supported in Qumran1 (Q1) series platforms.

Command Syntax

```
switchport customer-network vlan <2-4094>
no switchport customer-network vlan
```

Parameters

<2-4094>
Set the default VLAN ID for the interface.

Default

Default Customer Network VLAN is 1.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 6.2.0

Examples

In this example, the xe1 interface allows C-TAG/untagged traffic from customers, adding SVLAN ID 100 before forwarding to the provider network. While egressing out, the SVLAN ID 100 will be stripped out.

```
(config)#interface xe1
(config-if)#switchport
(config-if)#dot1ad ethertype 0x88a8
(config-if)#bridge-group 1
(config-if)#switchport mode customer-network
(config-if)#switchport customer-network allowed vlan add 100
(config-if)#switchport customer-network vlan 100
```

© 2026 IP Infusion Inc. Proprietary

switchport mode

Use this command to set the switching characteristics of the Layer 2 interface.

Note: Customer-Network Port is not supported in Qumran1 (Q1) series platforms.

Command Syntax

```
switchport mode (provider-network|customer-edge|customer-network)
```

Parameters

provider-network
Provider network.

customer-edge
Customer edge.

customer-network
Customer network.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode provider-network
```

switchport mode customer-edge

Use this command to set the switching characteristics of the Layer 2 customer facing interface and classify only untagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode customer-edge (access|hybrid|trunk)
switchport mode customer-edge (access|hybrid|trunk)
```

Parameters

access
Set the layer 2 interface as access.

hybrid
Set the layer 2 interface as hybrid.

trunk
Set the layer 2 interface as trunk.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode customer-edge access
```

© 2026 IP Infusion Inc. Proprietary

switchport mode customer-edge hybrid acceptable-frame-type

Use this command to set the layer 2 interface acceptable frames types. This processing occurs after VLAN classification.

Command Syntax

```
switchport mode customer-edge hybrid acceptable-frame-type (all|vlan-tagged)
```

Parameters

all
Set all frames can be received.

vlan-tagged
Set only VLAN-tagged frames can be received.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode customer-edge hybrid acceptable-frame-type vlan-tagged
```

© 2026 IP Infusion Inc. Proprietary

switchport provider-network

Use this command to set the switching characteristics of the provider-network interface.

Command Syntax

```
switchport provider-network allowed vlan add VLAN_RANGE2
switchport provider-network allowed vlan remove VLAN_RANGE2
switchport provider-network allowed vlan except VLAN_RANGE2
switchport provider-network allowed vlan all
switchport provider-network allowed vlan none
```

Parameters

add
Add a VLAN to transmit and receive through the Layer 2 interface.

VLAN_RANGE2
VLAN ID 1-4094 or range(s): 2-5 10 or 2-5 7-20.

remove
Remove a VLAN from the member set.

VLAN_RANGE2
VLAN ID 1-4094 or range(s): 2-5 10 or 2-5 7-20.

Except
All VLANs except these VLANs are part of the member set.

VLAN_RANGE2
VLAN ID 1-4094 or range(s): 2-5 10 or 2-5 7-20.

all
Allow all VLANs to transmit and receive through the Layer 2 interface.

none
Allow no VLANs to transmit and receive through the Layer 2 interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#switchport provider-network allowed vlan add 2
```

© 2026 IP Infusion Inc. Proprietary

switchport provider-network isolated-vlan

Use this command to attach a VLAN as an isolated VLAN for a provider network port.

Using an isolated VLAN for PNP ports on a switch can forward all frames received from the PNP port to all other PNP ports. However, if VLANs are configured to be isolated, they can traverse PNP port without sharing any of their frames.

Use the no form of this command to remove an isolated VLAN for a provider network port.

Command Syntax

```
switchport provider-network isolated-vlan VLAN_RANGE
no switchport provider-network isolated-vlan VLAN_RANGE
```

Parameters

VLAN_RANGE

VLAN identifier <2-4094> or range such as 2-5,10 or 2-5,7-19

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#bridge 1 protocol provider-rstp
(config)#vlan database
(config-vlan)#vlan 2-10 type service point-point bridge 1 state enable
(config-vlan)#exit
(config)#interface xe0
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport provider-network allowed vlan all
(config-if)#switchport provider-network isolated-vlan 2-10
```

© 2026 IP Infusion Inc. Proprietary

vlan type

This command allows you to create a single/range of VLAN's on provide/edge bridge.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE type customer bridge <1-32>
vlan VLAN_RANGE type customer bridge <1-32> name WORD
vlan VLAN_RANGE type customer bridge <1-32> state (enable | disable)
vlan VLAN_RANGE type service point-point bridge <1-32>
vlan VLAN_RANGE type service point-point bridge <1-32> name WORD
vlan VLAN_RANGE type service point-point bridge <1-32> state (enable | disable)
no vlan VLAN_RANGE type customer bridge <1-32>
no vlan VLAN_RANGE type service bridge <1-32>
```

Parameters

VLAN_RANGE
VLAN identifier <2-4094> or range such as 2-5,10 or 2-5,7-19

customer
Identifies the Customer VLAN

bridge
Specify the bridge group ID in the range <1-32>.

name
The ASCII name of the VLAN. Maximum length allowed is 16 characters.

point-point
Sets the VLAN connectivity mode to point-to-point

WORD
ASCII name of the VLAN.

state
Indicates the operational state of the VLAN.

enable
Sets VLAN into an enable state.

disable
Sets VLAN into a disable state.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)vlan 2,4,5-6 customer bridge 2
(config)vlan 10-12 service type point-point bridge 3
```

© 2026 IP Infusion Inc. Proprietary

vlan type customer

Use this command to configure VLANs of type customer, to enable or disable the state of the VLANs, and to configure the name for VLANs.

Use the `no` form of this command to remove the VLAN type.

Command Syntax

```
vlan <2-4094> type customer bridge <1-32>
vlan <2-4094> type customer bridge <1-32> state (enable|disable)
vlan <2-4094> type customer bridge <1-32> name WORD
no vlan <2-4094> type customer bridge <1-32>
```

Parameters

<2-4094>
The VID of the VLAN that will be enabled or disabled on the bridge <2-4094>.

type
Identifies the VLAN as a customer, service, or VLAN.

customer
Identifies the Customer VLAN

bridge
Indicates a Service VLAN <1-32>.

name
The ASCII name of the VLAN. Maximum length allowed is 16 characters.

state
Indicates the operational state of the VLAN.

enable
Sets VLAN into an enable state.

disable
Sets VLAN into a disable state.

WORD
ASCII name of the VLAN.

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#vlan database
(config-vlan)#vlan 12 type customer bridge 1 name new state enable
```

© 2026 IP Infusion Inc. Proprietary

Port Security Commands

This chapter describes the port security commands.

port-security 669
show port-security 669
switchport port-security 670
switchport port-security logging 671
switchport port-security mac-address 672
switchport port-security maximum 673

port-security

Use this command to enable or disable port security globally.

Command Syntax

```
port-security (enable | disable)
```

Parameters

enable
Enable port security globally

disable
Disable port security globally

Default

By default, port security is enabled globally.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS Version SP 4.0.

Example

```
(config)#port-security enable
(config)#
```

show port-security

Use this command to display the port security configuration for all interfaces or for a particular interface.

Command Syntax

```
show port-security (interface IFNAME |)
```

Parameters

IFNAME
Interface name

Default

None

Command Mode

Execution mode

Applicability

This command was introduced in OcNOS Version SP 4.0.

Example

```
#show port-security
Port port-security mode MAC limit CVLAN SVLAN static secure MAC
-----------------------------------------------------------------
ge1  dynamic            3         2           0000.0000.1112
                                   10          0000.0000.3333

#show port-security interface ge1
Port Security Mode : Dynamic
Secure MAC limit : 3
Static Secure MAC list :
CVLAN SVLAN MAC Address
---------------------------
2           0000.0000.1112
10          0000.0000.3333
```

switchport port-security

Use this command to enable port security on an interface.

Use the `no` form of this command to disable port security on an interface. This command removes configured secured MAC, if any, on this interface.

Note: This command is supported for physical, LAG, and MLAG (active) interfaces only. Enabling port security on an interface removes learned MAC addresses of interfaces (whether learned by static or dynamic means), and then relearns the secure MAC addresses. Multicast MAC addresses are not considered as part of the MAC learning limit.

Note: This command is ignored when port security is already enabled on an interface.

Command Syntax

```
switchport port-security (static |)
no switchport port-security
```

Parameters

static
Static mode

Default

By default this feature is disabled; the default mode of port security is to dynamically learn. In dynamic mode, devices learn MAC addresses dynamically. You can program static MACs, however, dynamic MAC learning will not be allowed in static mode for port security.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS Version SP 4.0.

Example

```
#configure terminal
(config)#interface ge1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode hybrid
(config-if)#switchport hybrid allowed vlan all
(config-if)#switchport port-security
```

switchport port-security logging

Use this command to enable violated MAC logging on a port security enabled interface.

Use the `disable` parameter with this command to disable violated mac logging on a port security enabled interface.

Note: This command has no impact, as Qumran does not support unsecured MAC address logging.

Command Syntax

```
switchport port-security logging (enable | disable)
```

Parameters

enable
Enable violated MAC logging

© 2026 IP Infusion Inc. Proprietary

disable
Disable violated MAC logging

Default

By default logging is disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS Version SP 4.0.

Example

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security logging enable
```

switchport port-security mac-address

Use this command to add static secure MAC addresses.

Use the `no` form of this command to remove static secure MAC addresses.

Command Syntax

```
switchport port-security mac-address XXXX.XXXX.XXXX
no switchport port-security mac-address XXXX.XXXX.XXXX

switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094>
no switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094>

switchport port-security mac-address XXXX.XXXX.XXXX svlanId <2-4094>
no switchport port-security mac-address XXXX.XXXX.XXXX svlanId <2-4094>

switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094> svlanId <2-4094>
no switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094> svlanId <2-4094>
```

Parameters

XXXX.XXXX.XXXX
Static secure MAC address

vlanId
VLAN identifier

<2-4094>
VLAN identifier

svlanId
SVLAN identifier

<2-4094>
SVLAN identifier

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS Version SP 4.0.

Example

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security mac-address 0000.0000.1112 vlan 2
(config-if)# no switchport port-security mac-address 0000.0000.1112 vlan 2
(config)#interface ge2
(config-if)#switchport port-security mac-address 0000.1111.2222
(config-if)#no switchport port-security mac-address 0000.1111.2222
(config)#interface ge3
(config-if)#switchport port-security mac-address 0000.2222.3333 svlan 9
(config-if)#no switchport port-security mac-address 0000.2222.3333 svlan 9
(config)#interface ge4
(config-if)#switchport port-security mac-address 0000.2222.3333 vlan 23 svlan 31
(config-if)#no switchport port-security mac-address 0000.2222.3333 vlan 23 svlan 31
```

switchport port-security maximum

Use this command to set the MAC address learning limit for an interface.

Note: This command is supported for physical, LAG, and MLAG (active) interfaces only. When a newly configured maximum learn limit is less than the previous value, you must remove/flush-out the unwanted MACs to stop traffic forwarding from the unwanted source MAC addresses. MAC addresses can be removed using the clear mac address-table command.

Use `no` form cli to set the maximum limit back to default value 1.

Command Syntax

```
switchport port-security maximum <1-1000>
no switchport port-security maximum
```

Parameters

<1-1000>
Maximum MAC address learning limit

Default

The default MAC address learning limit is 1.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS Version SP 4.0.

Example

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security maximum 3

#configure terminal
(config)#interface po1
(config-if)#switchport port-security maximum 3

#configure terminal
(config)#interface mlag1
(config-if)#switchport port-security maximum 3
```

© 2026 IP Infusion Inc. Proprietary

Link Layer Discovery Protocol Commands

This section describes the Link Layer Discovery Protocol (LLDP) commands.

lldp debug 676
lldp (disable|enable) default-agent 677
lldp ip 678
lldp run 679
lldp tlv 680
lldp tlv-select 681
set lldp chassis-id-tlv 683
set lldp disable 684
set lldp enable 685
set lldp locally-assigned 686
set lldp management-address-tlv 687
set lldp msg-tx-hold 688
set lldp timer 689
set lldp too-many-neighbors 690
show lldp 691
snmp restart lldp 692

© 2026 IP Infusion Inc. Proprietary

lldp debug

Use this command to set the debugging functions for LLDP.

Use the `no` form of this command to turn off LLDP debugging functions

Command Syntax

```
lldp debug (event|rx|tx|message)
no lldp debug (event|rx|tx|message)
```

Parameters

event
Enable or disable event debugging

message
Enable or disable NSM message debugging

rx
Enable or disable RX debugging

tx
Enable or disable TX debugging

Command Mode

Execution mode and Privileged execution mode

Examples

```
#lldp debug event
#lldp debug messages
```

© 2026 IP Infusion Inc. Proprietary

lldp (disable|enable) default-agent

Use this command to exclude interface when LLDP enabled globally

Command Syntax

```
lldp (disable|enable) default-agent
```

Parameters

disable
Disables default LLDP agent

enable
Enables default LLDP agent

Command Mode

Interface mode

Applicability

This command is introduced from OcNOS version 5.0

Example

```
#configure terminal
(config)#interface xe1
(config-if)#lldp disable default-agent
(config-if)#lldp enable default-agent
```

lldp ip

Use this command to set the Link Layer Discovery Protocol with an IP address to be used as a chassis and management ID.

Use the `no` form of this command to remove this value.

Command Syntax

```
lldp ip address A.B.C.D
no lldp ip address
```

Parameters

A.B.C.D
Enter the IP address value

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#lldp ip address 1.1.1.1
(config)#no lldp ip address
```

© 2026 IP Infusion Inc. Proprietary

lldp run

Use this command to start the Link Layer Discovery Protocol (LLDP).

Use the `no` parameter of this command to stop LLDP.

Command Syntax

```
lldp run
no lldp run
```

Parameters

None

Command Mode

Configure mode

Example

```
#configure terminal
(config)#lldp run

(config)#no lldp run
```

lldp tlv

Use this command to set the TLVs enabled for transmission on a port. Make sure that the complete set of Type Length Values (TLVs) is specified when giving this command, because TLVs not specified are disabled.

Command Syntax

```
lldp tlv {chassis-id|port-id|ttl|port-description|system-name|system-description|system-
capabilities|management-address|ieee-8021-org-specific|ieee-8023-org-specific}
```

Parameters

chassis-id
Chassis ID type length values (TLV)

port-id
Port ID TLV

ttl
Time to live TLV

port-description
Port description TLV

system-name
System name TLV

system-description
System Description

system-capabilities
System capabilities TLV

management-address
Management address TLV

ieee-8021-org-specific
IEEE 802.1 organizationally-specific TLV

ieee-8023-org-specific
IEEE 802.3 organizationally-specific TLV

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#lldp tlv chassis-id ieee-8021-org-specific ieee-8023-org-specific management-address
port-description port-id system-capabilities system-description system-name ttl
```

© 2026 IP Infusion Inc. Proprietary

lldp tlv-select

Use this command to configure interface LLDP parameters.

This command can be executed globally for all ports (configure mode) or locally for a specific port (interface mode).

When you give this command globally on all ports:

- The `show running-config` command only displays the options in global mode.
- A global configuration overrides an interface-level configuration. For example, if you disable an option on an interface, it is enabled after enabling the same option globally. If the option was enabled previously, the show output is suppressed and only global mode is displayed (to avoid duplicating the same configuration).
- After enabling a global configuration, when a new LLDP agent is configured on a port, it inherits the global TLV configuration. However, show output does not appear per interface/agent.
- After enabling globally, if you disable an option on an interface, the "no" form for this command is shown for that interface.
- Enabling an already enabled option causes an error.

If you disable globally on all ports:

- The option is removed globally, as well as overrides configurations for all interfaces.
- If the option was not enabled globally, it causes an error.

When enabled locally on a port:

- If the same option was enabled globally, it causes an error.
- If not already enabled, the option is enabled for the given interface alone.

When disabled locally on a port

- If the option was not present locally or globally, it causes an error.
- If the option was enabled globally, the option is removed from this interface alone. No command will be displayed in show output.

Use the `no` parameter of this command to remove interface LLDP parameter configurations.

Command Syntax

```
lldp tlv-select (port-description|system-name| system-description|system-capabilities|management-
address| ieee-8021-org-specific | ieee-8023-org-specific)
no lldp tlv-select (port-description|system-name|system-description|system-capabilities|management-
address|ieee-8021-org-specific | ieee-8023-org-specific)
```

Parameters

port-description
Port description TLV

system-name
System name TLV

system-description
System Description

system-capabilities
System capabilities TLV

© 2026 IP Infusion Inc. Proprietary

management-address
Management address TLV

ieee-8021-org-specific
IEEE 802.1 organizationally-specific TLV

ieee-8023-org-specific
IEEE 802.3 organizationally-specific TLV

Command Mode

Configure mode and Interface mode

Example

```
#configure terminal
(config)#lldp tlv-select system-capabilities

#configure terminal
(config)#interface eth2
(config-if)#lldp-agent
(config-if-lldp-agent)#lldp tlv-select system-capabilities
```

© 2026 IP Infusion Inc. Proprietary

set lldp chassis-id-tlv

Use this command to set the chassis ID subtype for the LLDP agent on a port.

Command Syntax

```
set lldp chassis-id-tlv (mac-address | ip-address)
```

Parameters

mac-address
Use the MAC address as the chassis ID

ip-address
Use the management IP address as the chassis ID

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp chassis-id-tlv ip-address
```

set lldp disable

Use this command to disable the LLDP agent on a port.

Command Syntax

```
set lldp disable
```

Parameters

None

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp disable
```

© 2026 IP Infusion Inc. Proprietary

set lldp enable

Use this command to enables an LLDP agent on a port and specifies its type.

Command Syntax

```
set lldp enable (txonly|txrx|rxonly)
```

Parameters

rxonly
Receive-only

txonly
Transmit-only

txrx
Transmit and receive

Default

By default, no LLDP agent is enabled for a port.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp enable rxonly
```

© 2026 IP Infusion Inc. Proprietary

set lldp locally-assigned

Use this command to locally assign the LLDP Port ID and the Chassis ID TLV parameters.

Command Syntax

```
set lldp locally-assigned NAME
```

Parameters

NAME
Name assigned to the port.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp locally-assigned port1
```

set lldp management-address-tlv

Use this command to set the management address subtype for the LLDP agent on a port.

Command Syntax

```
set lldp management-address-tlv (mac-address | ip-address)
```

Parameters

mac-address
Use the MAC address as the chassis ID

ip-address
Use the management IP address as the chassis ID

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp management-address-tlv ip-address
```

© 2026 IP Infusion Inc. Proprietary

set lldp msg-tx-hold

Use this command to set the `msg-tx-hold` parameter that determines the Time To Live (TTL) value for LLDPDUs to be transmitted by the port. The value set with this command is multiplied by the `lldp timer msg-tx-interval` value, which determines the final TTL value.

Command Syntax

```
set lldp msg-tx-hold VALUE
```

Parameters

VALUE
Time in seconds of LLDP msg-tx-hold

Default

The default value of the `lldp msg-tx-hold` parameter is 4 seconds.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config)#set lldp msg-tx-hold 3
```

set lldp timer

Use this command to set the interval at which LLDP frames are transmitted.

Command Syntax

```
set lldp timer msg-tx-interval <5-32768>
set lldp timer reinitDelay VALUE
set lldp timer tx-delay <1-8192>
```

Parameters

msg-tx-interval
Set the message transmit interval value

<5-32768>
Set the message transmit interval value

reinitDelay
Set the reinit delay value

VALUE
Set the reinit delay value

tx-delay
Set the transmit delay value

<1-8192>
Set the transmit delay value in range of:

(1 <= tx-delay <= ((0.25)* msg-tx-interval)

Default

The default value for `msg-tx-interval` is 30 seconds.

The default value for `reinitDelay` is 2 seconds.

The default value of the `tx-delay` is 2 seconds.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp timer msg-tx-interval 40

#configure terminal
(config)#interface eth0
(config-if)#set lldp timer reinitDelay 3

#configure terminal
(config)#interface eth0
(config-if)#set lldp timer tx-delay 3
```

© 2026 IP Infusion Inc. Proprietary

set lldp too-many-neighbors

Use this command to set the action to take when the remote table is full.

Command Syntax

```
set lldp too-many-neighbors limit <1-65535> discard received-info timer <1-65535>
set lldp too-many-neighbors limit <1-65535> discard existing-info MACtimer <1-65535>
```

Parameters

limit
The limit on the number of LLDP neighbors.

<1-65535>
The limit on the number of LLDP neighbors.

received-info
The information received for this neighbor.

timer
The period after which received information is discarded.

<1-65535>
The period in seconds after which received information is discarded.

existing-info
The information for this neighbor.

MAC
Identifies the remote LLDP Agent for which information is discarded.

timer
The period in seconds after which existing information is discarded.

<1-65535>
The period in seconds after which existing information is discarded.

Default

No upper limit is enforced for the number of remote LLDP agents.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#set lldp too-many-neighbors limit 20 disc existing-info 1.1.1.1.1 timer 1

(config)#interface eth1
(config-if)#set lldp too-many-neighbors limit 1 discard received-info timer 1
```

© 2026 IP Infusion Inc. Proprietary

show lldp

Use this command to display LLDP port information.

Command Syntax

```
show lldp port IFNAME
show lldp port IFNAME statistics
```

Parameters

IFNAME
The name of the interface

statistics
Display LLDP port statistics

Command Mode

Execution mode and Privileged execution mode

Example

The following sample output from this command displays detailed information about an LLDP-enabled port.

```
#show lldp port eth0
Remote LLDP
MAC Address: 01:06:29:CF:79:A1
TTL: 60
Network Address: 192.168.1.0
Interface Name: eth1
Interface Locally Assigned String: Port-a
Interface Description: bridge
Interface Number: 2
Port Vlan ID: 1
Protocol ID: 274242030202
AutoNego Support: Supported
AutoNego Capability: 1
Operational MAU Type: 3
Link Aggregation Status: Capable
Link Aggregation Port ID: 0
Max Frame Size: 128
System name:
System Description: bridge
System Capabilities: 4
System Capabilities Enabled: 4
```

The following sample output from this command displays all LLDP statistics for a selected port.

```
#show lldp port eth0 statistics
LLDP Port statistics for eth0
Frames transmitted: 22
Frames Aged out: 0
Frames Discarded: 0
Frames with Error: 0
Frames Received: 5
TLVs discarded: 0
TLVs unrecognized 0
```

© 2026 IP Infusion Inc. Proprietary

snmp restart lldp

Use this command to restart SNMP in Link Layer Discovery Protocol (LLDP)

Command Syntax

```
snmp restart lldp
```

Parameters

None

Command Mode

Configure mode

Examples

```
#snmp restart lldp
```

© 2026 IP Infusion Inc. Proprietary

Unidirectional Link Detection Commands

This section describes the Unidirectional Link Detection (UDLD) commands.

udld 694
udld message-time 695
udld mode 696
udld state 697
show udld 698
show udld interface 699

© 2026 IP Infusion Inc. Proprietary

udld

Use this command to enable the UDLD feature globally.

Use `no` form of this command to disable the UDLD feature globally.

Command Syntax

```
udld  enable
no udld enable
```

Parameters

None

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
(config)#udld enable
(config)#no udld enable
```

udld message-time

Use this command to set the UDLD message interval.

Command Syntax

```
udld message-time <7-90>
```

Parameters

<7-90>
Interval time in seconds

Default

15 seconds

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
config)#udld message-time 50
```

© 2026 IP Infusion Inc. Proprietary

udld mode

Use this command to configure UDLD mode as aggressive or normal.

Command Syntax

```
udld mode (aggressive | normal)
```

Parameters

aggressive
Aggressive mode

normal
Normal mode

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
(config-if)#udld mode aggressive
```

© 2026 IP Infusion Inc. Proprietary

udld state

Use this command to enable or disable the UDLD feature for an interface.

Command Syntax

```
udld state (enable | disable)
```

Parameters

None

Default

Disabled

Command Mode

Interface modeInterface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
(config)#int xe7
(config-if)#udld state enable
```

© 2026 IP Infusion Inc. Proprietary

show udld

Use this command to display UDLD statistic for all interface.

Command Syntax

```
show udld
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#show udld
UDLD                    : Enable
Message Interval(sec)   : 15
Port    UDLD Status     Mode           Link-Status
------------------------------------------------
xe7     Enable          Normal         Bi-Directional
```

Table 33. show udld output fields (page 698)explains the output fields.

Table 33. show udld output fields

Field	Description
UDLD	Whether UDLD is enabled or disabled
Message Interval	Message interval in seconds
Port	Interface name
UDLD Status	Whether UDLD is enabled or disabled on the interface
Mode	Whether the mode is aggressive or normal
Link-Status	State of the link: Unknown Loop-Back Neighbor Mismatch Unidirectional Undetermined Bi-Directional

© 2026 IP Infusion Inc. Proprietary

show udld interface

Use this command to display UDLD settings for particular interface.

Command Syntax

```
show udld interface IFNAME
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#show udld interface xe14
UDLD Status           : Enable
UDLD Mode             : Aggressive
Link-State            : Bi-Directional
#
```

Table 34. show udld interface output fields (page 699) explains the output fields.

Table 34. show udld interface output fields

Field	Description
UDLD Status	Whether UDLD is enabled or disabled
UDLD Mode	Whether the mode is aggressive or normal
Link-State	State of the link: Unknown Loop-Back Neighbor Mismatch Unidirectional Undetermined Bi-Directional

© 2026 IP Infusion Inc. Proprietary

Spanning Tree Protocol Commands

This section provides a description, syntax, and examples of the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) commands. It includes the following commands:

bridge cisco-interoperability 702
bridge-group instance 703
bridge-group instance path-cost 704
bridge-group instance priority 705
bridge-group path-cost 706
bridge-group priority 707
bridge-group spanning-tree 708
bridge instance 709
bridge instance priority 710
bridge instance vlan 711
bridge multiple-spanning-tree 713
bridge protocol ieee 714
bridge protocol mstp 715
bridge protocol rstp 716
bridge rapid-spanning-tree 717
bridge region 718
bridge revision 719
bridge spanning-tree 720
bridge spanning-tree errdisable-timeout 721
bridge spanning-tree force-version 722
bridge spanning-tree pathcost 723
bridge te-msti 724
bridge te-msti vlan 725
clear spanning-tree detected protocols 727
clear spanning-tree statistics 728
customer-spanning-tree customer-edge priority 729
customer-spanning-tree customer-edge path-cost 730
customer-spanning-tree hello-time 731
customer-spanning-tree max-age 732
customer-spanning-tree priority 733
customer-spanning-tree provider-edge path-cost 734
customer-spanning-tree provider-edge priority 735
customer-spanning-tree transmit-holdcount 736
debug mstp 737

© 2026 IP Infusion Inc. Proprietary

show debugging mstp 739
show spanning-tree 740
show spanning-tree mst 744
show spanning-tree statistics 746
snmp restart mstp 748
spanning-tree autoedge 749
spanning-tree edgeport 750
spanning-tree guard 751
spanning-tree instance restricted-role 752
spanning-tree instance restricted-tcn 753
spanning-tree link-type 754
spanning-tree mst configuration 755
spanning-tree restricted-domain-role 756
spanning-tree restricted-role 757
spanning-tree restricted-tcn 758
spanning-tree te-msti configuration 759

© 2026 IP Infusion Inc. Proprietary

bridge cisco-interoperability

Use this command to enable/disable Cisco interoperability for MSTP (Multiple Spanning Tree Protocol).

If Cisco interoperability is required, all OcNOS devices in the switched LAN must be Cisco-interoperability enabled. When OcNOS inter operates with Cisco, the only criteria used to classify a region are the region name and revision level. VLAN-to-instance mapping is not used to classify regions when interoperating with Cisco.

Command Syntax

```
bridge <1-32> cisco-interoperability (enable | disable)
```

Parameters

<1-32>
Specify the bridge group ID

enable
Enable Cisco interoperability for MSTP bridge

disable
Disable Cisco interoperability for MSTP bridge

Default

By default, cisco interoperability is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

To enable Cisco interoperability on a switch for a bridge:

```
#configure terminal
(config)#bridge 2 cisco-interoperability enable
```

To disable Cisco interoperability on a switch for a particular bridge:

```
#configure terminal
(config)#bridge 2 cisco-interoperability disable
```

© 2026 IP Infusion Inc. Proprietary

bridge-group instance

Use this command to assign a Multiple Spanning Tree (MST) instance to a port.

Use the `no` form of this command to remove the interface from the MST instance.

Command Syntax

```
bridge-group (<1-32> | backbone) instance (<1-63> | te-msti)
no bridge-group (<1-32> | backbone) instance (<1-63> | te-msti)
```

Parameters

<1-32>
Bridge identifier.

backbone
Backbone bridge.

<1-63>
Multiple spanning tree instance identifier.

te-msti
Traffic engineering MSTI instance.

For Provider Backbone Bridging (PBB), bridge-group <1-32> refers to the I-component or PB bridge while the <backbone> bridge group refers to the B-component. Usually for a BEB (Backbone Edge Bridge) device, the backbone bridge-group is used for traffic engineering.

For a PB (Provider Bridge) device used as BCB (Backbone Core Bridge), bridge group <1-32> is used for traffic engineering.

Default

By default, the bridge port remains in the listening and learning states for 15 seconds before transitional to the forwarding state.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#bridge-group 1
(config-if)#bridge-group 1 instance te-msti
```

© 2026 IP Infusion Inc. Proprietary

bridge-group instance path-cost

Use this command to set a path cost for a multiple spanning tree instance.

Before you can give this command, you must explicitly add an MST instance to a port using the `bridge-group instance` command.

Use the `no` form of this command to set the path cost to its default which varies depending on bandwidth.

Command Syntax

```
bridge-group (<1-32> | backbone) instance <1-63> path-cost <1-200000000>
no bridge-group ( <1-32> | backbone) instance <1-63> path-cost
```

Parameters

<1-32>
Bridge identifier.

backbone
Specify the backbone bridge.

<1-63>
Set the MST instance identifier.

<1-200000000>
Path cost for a port (a lower path cost means greater likelihood of becoming root).

Default

Assuming a 10 Mb/s link speed, the default value is 200,000.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3 vlan 3
(config-mst)#exit
(config)#interface eth1
(config-if)#bridge-group 4 instance 3
(config-if)#bridge-group 4 instance 3 path-cost 1000
```

© 2026 IP Infusion Inc. Proprietary

bridge-group instance priority

Use this command to set the priority of a multiple spanning tree instance.

The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

Command Syntax

```
bridge-group (<1-32>) instance (<1-63>) priority <0-240>
no bridge-group (<1-32>) instance (<1-63>) priority
```

Parameters

<1-32>
Bridge identifier.

backbone
Backbone bridge.

<1-63>
Multiple spanning tree instance identifier.

<0-240>
Port priority. A lower value means greater likelihood of becoming root. Set the port priority in increments of 16.

Default

By default, the port priority is 128

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth2
(config-if)#bridge-group 2
(config-if)#bridge-group 2 instance 4
(config-if)#bridge-group 2 instance 4 priority 64
```

© 2026 IP Infusion Inc. Proprietary

bridge-group path-cost

Use this command to set the cost of a path. Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the bridge-group instance command.

Use the no parameter with this command to restore the default cost value of the path which varies depending on the bandwidth.

Command Syntax

```
bridge-group <1-32> path-cost <1-200000000>
no bridge-group <1-32> path-cost
```

Parameters

<1-32>

Specify the bridge group ID.

path-cost

Specify the cost of path for a port.

<1-200000000>

Specify the cost of the path (a lower cost means a greater likelihood of the interface becoming root).

Default

Assuming a 10 Mb/s link speed, the default value is 200,000.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3 vlan 3
(config-mst)#exit
(config)#interface eth1
(config-if)#bridge-group 4
(config-if)#bridge-group 4 path-cost 1000
```

© 2026 IP Infusion Inc. Proprietary

bridge-group priority

Use this command to set the port priority for a bridge group.

The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

Command Syntax

```
bridge-group (<1-32> | backbone) priority <0-240>
no bridge-group (<1-32> | backbone) priority
```

Parameters

<1-32>
Specify the bridge group ID.

backbone
Backbone bridge.

<0-240>
Specify the port priority (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

128

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#bridge-group 4 priority 80
```

© 2026 IP Infusion Inc. Proprietary

bridge-group spanning-tree

This command is used to enable or disable the spanning-tree on a configured bridge.

Command Syntax

```
bridge-group <1-32> spanning-tree (disable|enable)
```

Parameters

<1-32>
Specify the bridge group ID.

disable
Disable spanning tree on the interface.

enable
Enable spanning tree on the interface.

Default

By default, spanning-tree is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth1
(config-if)#bridge-group 1 spanning-tree enable
```

© 2026 IP Infusion Inc. Proprietary

bridge instance

Use this command to add an MST instance to a bridge.

Use the `no` form of this command to delete an MST instance identifier from a bridge.

Command Syntax

```
bridge (<1-32> | backbone) instance (<1-62>)
no bridge (<1-32> | backbone) instance (<1-62>)
```

Parameters

<1-32>
Bridge identifier.

backbone
Backbone bridge.

<1-62>
MST instance identifier.

Default

The bridge instance default is 1.

Command Mode

MST Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 4 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3
...
(config-mst)#no bridge 4 instance 3
```

© 2026 IP Infusion Inc. Proprietary

bridge instance priority

Use this command to set the bridge instance priority.

Use the `no` form of this command to reset the priority to its default.

Command Syntax

```
bridge (<1-32> | backbone) instance <1-63> priority <0-61440>
no bridge (<1-32> | backbone) instance <1-63> priority
```

Parameters

<1-32>
Specify the bridge identifier.

backbone
Specifies the backbone bridge.

<1-63>
Specify the instance identifier.

priority
Specify the bridge priority for the instance. The lower the priority of the bridge, the better the chances is of the bridge becoming a root bridge or a designated bridge for the LAN. The priority values can be set only in increments of 4096. The default value is 32768.

<0-61440>
Specify the bridge priority.

Default

By default, bridge instance priority is 32768

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#bridge 4 instance 3 priority 1
```

© 2026 IP Infusion Inc. Proprietary

bridge instance vlan

Use this command to simultaneously add multiple VLANs for the corresponding instance of a bridge.The VLANs must be created before being associated with an MST instance (MSTI). If the VLAN range is not specified, the MSTI will not be created.

Use the `no` form of this command to simultaneously remove multiple VLANs for the corresponding instance of a bridge.

Command Syntax

```
bridge (<1-32> | backbone) instance (<1-63>) vlan VLANID
no bridge (<1-32> | backbone) instance (<1-63>) vlan VLANID
```

Parameters

<1-32>
Bridge identifier.

backbone
Backbone bridge.

<1-63>
MST instance identifier.

VLANID
VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.

For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Default

The bridge instance VLAN ID Interfaces default-switch is VLAN100 100 ae0.0 ae1.0 ae2.0.

Command Mode

MST Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

To associate multiple VLANs, in this case VLANs 10 and 20 to instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 1 instance 1 vlan 10,20
```

To associate multiple VLANs, in this case, VLANs 10, 11, 12, 13, 14, and 15 to instance 1 of bridge 1:

```
#configure terminal
```

© 2026 IP Infusion Inc. Proprietary

```
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 1 instance 1 vlan 10-15
```

To delete multiple VLANs, in this case, VLANs 10 and 11 from instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#no bridge 1 instance 1 vlan 10,11
```

© 2026 IP Infusion Inc. Proprietary

bridge multiple-spanning-tree

Use this command to enable MSTP on a bridge.

Use the `no` form of this command to disable MSTP on the bridge.

Command Syntax

```
bridge <1-32> multiple-spanning-tree enable
no bridge <1-32> multiple-spanning-tree enable (bridge-forward|bridge-block)
```

Parameters

<1-32>
Specify the bridge-group ID.

enable
Enables the spanning tree protocol.

bridge-forward
Puts all ports of the specified bridge into forwarding state.

bridge-block
Puts all ports of the specified bridge into blocking state.

Default

If the bridge-forward option is entered when using the no parameter, the default behavior is to put all bridge ports in forwarding state.

If the bridge-block option is entered when using the no parameter, the behavior is to put all bridge ports in blocking state.

If no options are defined after the command no bridge <1-32> multiple-spanning-tree enable, then the default behavior is same as bridge-block command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 multiple-spanning-tree enable
(config)#no bridge 2 multiple-spanning-tree enable bridge-forward
```

© 2026 IP Infusion Inc. Proprietary

bridge protocol ieee

Use this command to add a IEEE 802.1d Spanning Tree Protocol bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in interface mode.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol ieee (vlan-bridge|)
no bridge <1-32>
```

Parameters

<1-32>
Specify the bridge group ID.

vlan-bridge
Specify this as a VLAN-aware bridge.

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 protocol ieee
(config)#bridge 4 protocol ieee vlan-bridge
```

© 2026 IP Infusion Inc. Proprietary

bridge protocol mstp

Use this command to create a multiple spanning-tree protocol (MSTP) bridge of a specified parameter. This command creates an instance of the spanning tree and associates the VLANs specified with that instance.

The MSTP bridges can have different spanning-tree topologies for different VLANs inside a region of “similar” MSTP bridges. The multiple spanning tree protocol, like the rapid spanning tree protocol, provides rapid reconfiguration capability, while providing load balancing ability. A bridge created with this command forms its own separate region unless it is added explicitly to a region using the `region name` command.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol mstp
no bridge <1-32>
```

Parameters

<1-32>
Specify the bridge group ID.

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 protocol mstp
```

bridge protocol rstp

Use this command to add an IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in Interface mode.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol rstp
bridge <1-32> protocol rstp (vlan-bridge|)
no bridge <1-32>
```

Parameters

<1-32>
Specify the bridge group ID.

vlan-bridge
(Optional) Adds a VLAN-aware bridge.

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 protocol rstp
```

© 2026 IP Infusion Inc. Proprietary

bridge rapid-spanning-tree

Use this command to enable or disable RSTP on a specific bridge. Use the `bridge-forward` option with the `no` form of the command to place all ports on the specified bridge into the forwarding state.

Use the `no` form of the command to disable the Rapid Spanning Tree protocol on a bridge.

Command Syntax

```
bridge <1-32> rapid-spanning-tree enable
no bridge <1-32> rapid-spanning-tree enable (bridge-forward|bridge-block)
```

Parameters

<1-32>
Specify the bridge group ID.

enable
Enables the spanning tree protocol.

bridge-forward
(Optional) Puts all ports of the specified bridge into forwarding state.

bridge-block
(Optional) Puts all ports of the specified bridge into blocking state.

Default

When the `bridge-forward` option is used with the `no` parameter, the default behavior puts all bridge ports in the forwarding state.

If the bridge-block option is entered when using the no parameter, the behavior is to put all bridge ports in blocking state.

If no options are defined after the command no bridge <1-32> rapid-spanning-tree enable, then the default behavior is same as bridge-block command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
# configure terminal
(config)#bridge 2 rapid-spanning-tree enable
(config)#no bridge 2 rapid-spanning-tree enable bridge-forward
```

© 2026 IP Infusion Inc. Proprietary

bridge region

Use this command to create an MST region and specify its name. MST bridges of a region form different spanning trees for different VLANs.

Use the `no` form of the command to disable the Rapid Spanning Tree protocol on a region.

Command Syntax

```
bridge <1-32> region REGION_NAME
no bridge <1-32> region
```

Parameters

<1-32>
Specify the bridge group ID.

REGION_NAME
Specify the name of the region.

Default

By default, each MST bridge starts with the region name as its bridge address. This means each MST bridge is a region by itself, unless specifically added to one.

Command Mode

MST Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 3 region myRegion
(config)#spanning-tree mst configuration
(config-mst)#no bridge 3 region
```

© 2026 IP Infusion Inc. Proprietary

bridge revision

Use this command to specify the number for configuration information.

Command Syntax

```
bridge <1-32> revision <0-65535>
```

Parameters

<1-32>
Specify the bridge group ID in the range of <1-32>.

<0-65535>
Specify a revision number in the range of <0-65535>.

Default

By default, revision number is 0

Command Mode

MST Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 3 revision 25
```

© 2026 IP Infusion Inc. Proprietary

bridge spanning-tree

Use this command to enable the Spanning Tree Protocol on a bridge.

Use the `no` parameter to disable the Spanning Tree Protocol on the bridge.

Command Syntax

```
bridge <1-32> spanning-tree enable
no bridge <1-32> spanning-tree enable (bridge-forward|bridge-block)
```

Parameters

<1-32>
Specify the bridge group ID.

enable
Enables the spanning tree protocol on this bridge.

bridge-forward
Puts all ports of the specified bridge into the forwarding state.

bridge-block
Puts all ports of the specified bridge into the blocking state.

Default

If the bridge-forward option is entered when using the no parameter, the default behavior is to put all bridge ports in forwarding state.

If the bridge-block option is entered when using the no parameter, the behavior is to put all bridge ports in blocking state.

If no options are defined after the command no bridge <1-32> spanning-tree enable, then the default behavior is same as bridge-block command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 spanning-tree enable
(config)#no bridge 2 spanning-tree enable bridge-forward
```

© 2026 IP Infusion Inc. Proprietary

bridge spanning-tree errdisable-timeout

Use this command to enable the error-disable-timeout facility, which sets a timeout for ports that are disabled due to the BPDU guard feature.

The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port. This command associates a timer with the feature such that the port gets enabled back without manual intervention after a set interval.

Use the `no` parameter to disable the error-disable-timeout facility.

Command Syntax

```
bridge <1-32> spanning-tree errdisable-timeout enable
no bridge <1-32> spanning-tree errdisable-timeout enable
```

Parameters

<1-32>
Specify the bridge group ID.

enable
Enable the timeout mechanism for the port to be enabled back

Default

By default, the port is enabled after 300 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 spanning-tree errdisable-timeout enable
```

© 2026 IP Infusion Inc. Proprietary

bridge spanning-tree force-version

Use this command to set the version for the bridge. A version identifier of less than a value of 2 enforces the spanning tree protocol. Although the command supports an input range of 0-4, for RSTP, the valid range is 0-2. When the force-version is set for a bridge, all ports of the bridge have the same spanning tree version set.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree (page 740)).

Use the no parameter with this command to disable the version for the bridge.

Command Syntax

```
bridge <1-32> spanning-tree force-version <0-4>
no bridge <1-32> spanning-tree force-version
```

Parameters

<1-32>
Specify the bridge group ID.

force-version
Specify a force version identifier:

0
STP

1
Not supported

2
RSTP

3
MSTP

Default

By default, spanning tree force version is 0

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

Set the value to enforce the spanning tree protocol:

```
#configure terminal
(config)#bridge 1 spanning-tree force-version 0
(config)#no bridge 1 spanning-tree force-version
```

© 2026 IP Infusion Inc. Proprietary

bridge spanning-tree pathcost

Use this command to set a spanning-tree path cost method.

If the short parameter is used, the switch uses a value for the default path cost a number in the range 1 through 65,535. If the long parameter is used, the switch uses a value for the default path cost a number in the range 1 through 200,000,000. Use the show spanning-tree (page 740) to view the administratively configured and current running pathcost method running on a bridge.

Use the `no` option with this command to return the path cost method to the default setting.

Command Syntax

```
bridge <1-32> spanning-tree pathcost method (short|long)
no bridge <1-32> spanning-tree pathcost method
```

Parameters

<1-32>
Specify the bridge group ID.

method
Method used to calculate default port path cost.

long
Use 16-bit based values for default port path costs.

short
Use 32-bit based values for default port path costs.

Default

By default, path cost method for STP is short and for MSTP/RSTP is long.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 spanning-tree pathcost method short
(config)#no bridge 1 spanning-tree pathcost method
```

© 2026 IP Infusion Inc. Proprietary

bridge te-msti

Use this command to enable or disable a Multiple Spanning Tree Instance (MSTI).

The te-msti always refers to the MST instance indexed by the pre-defined macro constant MSTP_TE_MSTID internally. This is the only MST instance which supports the disabling of spanning trees.

Use the no form of this command to remove the configuration.

Command Syntax

```
bridge (<1-32> | backbone) te-msti
no bridge (<1-32> | backbone) te-msti
```

Parameters

<1-32>
Specify the bridge group ID.

backbone
Identity of the backbone bridge group.

te-msti
MSTI to be the traffic engineering MSTI instance.

Default

By default, bridge te-msti is disabled

Command Mode

TE-MSTI Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#bridge 2 te-msti
(config-te-msti)#no bridge 2 te-msti
```

© 2026 IP Infusion Inc. Proprietary

bridge te-msti vlan

Use this command to enable or disable a Multiple Spanning Tree Instance (MSTI). When an MSTI is shutdown (disabled) each VLAN in the MSTI is set to the forwarding state on all bridge ports which the VLAN as a member of. When and MSTI is enabled (no shutdown), normal MSTP operation is started for the MSTI.

The `te-msti` always refers to the MST instance indexed by the pre-defined macro constant `MSTP_TE_MSTID` internally. This is the only MST instance which supports the disabling of spanning trees. All VLANs that do not want spanning tree topology computation need to be assigned to this `te-msti` instance.

This command is intended for supporting Traffic Engineering (TE) Ethernet tunnels. All VLANs allocated for traffic engineering should be assigned to one MSTI. That MSTI can in turn shutdown the spanning tree operation so that each VLAN path through the network can be manually provisioned.

Use the no form of this command to remove the configuration.

Command Syntax

```
bridge (<1-32> | backbone) te-msti vlan <1-4094>
no bridge (<1-32> | backbone) te-msti vlan <1-4094>
```

Parameters

<1-32>
Specify the bridge group ID.

backbone
Identity of the backbone bridge group.

vlan
Specify a VLAN.

<1-4094>
Specify a VLAN identifier to be associated.

Note: This designated instance is defined in 802.1Qay clause 8.9 to be 0xFFE.

Default

By default, te-msti vlan is vlan1.

Command Mode

TE-MSTI Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
```

```
(config-te-msti)#bridge 2 te-msti vlan 10
(config-te-msti)#no bridge 2 te-msti vlan 10
```

© 2026 IP Infusion Inc. Proprietary

clear spanning-tree detected protocols

Use this command to clear the detected protocols for a specific bridge or interface. This command begins the port migration as per IEEE 802.1w-2001, Section 17.26. After issuing this command, the migration timer is started on the port, only if the force version is RSTP or MSTP (greater versions of RSTP).

Command Syntax

```
clear spanning-tree detected protocols bridge <1-32>
```

Parameters

<1-32>
Specify the bridge group ID.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear spanning-tree detected protocols bridge 2
```

© 2026 IP Infusion Inc. Proprietary

clear spanning-tree statistics

Use this command to clear all STP BPDU statistics.

Command Syntax

```
clear spanning-tree statistics bridge <1-32>
clear spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <1-4094>) bridge <1-32>
clear spanning-tree statistics (interface IFNAME| (instance (<1-63>)| vlan <2-4094>)) bridge <1-32>
```

Parameters

<1-32>
Specify the bridge identifier.

IFNAME
Specify the name of the interface on which protocols have to be cleared.

<1-63>
MST instance ID.

<1-4094>
VLAN identifier where spanning tree is located <2-4094>

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear spanning-tree statistics bridge 32
```

© 2026 IP Infusion Inc. Proprietary

customer-spanning-tree customer-edge priority

Use this command to set the port priority for a customer-edge port in the customer spanning tree.

Command Syntax

```
customer-spanning-tree customer-edge priority <0-240>
```

Parameters

priority
Specify the port priority.

<0-240>
Specify the port priority range (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree customer-edge priority 100
```

© 2026 IP Infusion Inc. Proprietary

customer-spanning-tree customer-edge path-cost

Use this command to set the cost of a path associated with a customer edge port on a customer edge spanning tree.

Use the `no` form of this command to remove the cost of a path associated with a customer edge port on a customer edge spanning tree.

Command Syntax

```
customer-spanning-tree customer-edge path-cost <1-200000000>
no customer-spanning-tree customer-edge path-cost
```

Parameters

path-cost
Specify the path-cost of a port.

<1-200000000>
Specify the cost to be assigned to the group.

Default

Assuming a 10 Mb/s link speed, the default value is 200,000

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree customer-edge path-cost 1000
```

© 2026 IP Infusion Inc. Proprietary

customer-spanning-tree hello-time

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). Avoid a very low value of this parameter as this can lead to excessive traffic on the network; a higher value delays the detection of topology change. This value is used by all instances.

Use the `no` option with this command to restore the default value of the hello-time.

Command Syntax

```
customer-spanning-tree hello-time <1-10>
no customer-spanning-tree hello-time
```

Parameters

<1-10>
Specify the hello BPDU interval in seconds.

Default

By default, level is 2 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree hello-time 3
(config-if)#no customer-spanning-tree hello-time
```

© 2026 IP Infusion Inc. Proprietary

customer-spanning-tree max-age

Use this command to set the max-age for a bridge.

Max-age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of max-age should be greater than twice the value of hello-time plus one, but less than twice the value of forward delay minus one. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by a root can be propagated to the leaf nodes without exceeding the max-age.

Use the `no` parameter with this command to restore the default value of max-age.

Command Syntax

```
customer-spanning-tree max-age <6-40>
no customer-spanning-tree max-age
```

Parameters

<6-40>

Specify the maximum time in seconds to listen for the root bridge.

Default

By default, bridge max-age is 20 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree max-age 12
(config-if)#no customer-spanning-tree max-age
```

© 2026 IP Infusion Inc. Proprietary

customer-spanning-tree priority

Use this command to set the bridge priority for the spanning tree on a customer edge port. Using a lower priority indicates a greater likelihood of the bridge becoming root. This command must be used to set the priority of the customer spanning tree running on the customer edge port.

Use the `no` form of the command to reset it to the default value.

Command Syntax

```
customer-spanning-tree priority <0-61440>
no customer-spanning-tree priority
```

Parameters

<0-61440>

Specify the bridge priority in the range <0-61440>. Priority values can be set only in increments of 4096.

Default

By default, priority is 61440

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree priority 4096
(config-if)#no customer-spanning-tree priority
```

© 2026 IP Infusion Inc. Proprietary

customer-spanning-tree provider-edge path-cost

Use this command to set the cost of a path associated with a provider edge port on a customer edge spanning tree.

Use the `no` form of this command to remove the cost of a path associated with a provider edge port on a customer edge spanning tree.

Command Syntax

```
customer-spanning-tree provider-edge svlan <1-4094> path-cost <1-200000000>
no customer-spanning-tree provider-edge svlan <1-4094> path-cost
```

Parameters

<1-4094>
Specify the SVLAN identifier of provider edge port.

<1-200000000>
Specify the cost to be assigned to the group.

Default

Assuming a 10 Mb/s link speed, the default value is 200,000

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree provider-edge svlan 2 path-cost 1000
(config-if)#no customer-spanning-tree provider-edge svlan 2 path-cost
```

© 2026 IP Infusion Inc. Proprietary

customer-spanning-tree provider-edge priority

Use this command to set the port priority for a provider-edge port in the customer spanning tree.

Command Syntax

```
customer-spanning-tree provider-edge svlan <1-4094> priority <0-240>
```

Parameters

<1-4094>
Specify the SVLAN identifier of provider edge port.

<0-240>
Specify the port priority (a lower priority means greater likelihood of the interface becoming root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree provider-edge svlan 2 priority 0
```

© 2026 IP Infusion Inc. Proprietary

customer-spanning-tree transmit-holdcount

Use this command to set the transmit-holdcount for a bridge.

Use the `no` parameter with this command to restore the default value of `transmit-holdcount`.

Command Syntax

```
customer-spanning-tree transmit-holdcount <1-10>
no customer-spanning-tree transmit-holdcount
```

Parameters

<1-10>
Specify the maximum number that can be transmitted per second.

Default

By default, bridge transmit hold count is 6

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree transmit-holdcount 3
(config-if)#no customer-spanning-tree transmit-holdcount
```

© 2026 IP Infusion Inc. Proprietary

debug mstp

Use this command to turn on, and turn off, debugging and echoing data to the console, at various levels.

Note: This command enables MSTP, RSTP, and STP debugging.

Use the `no` parameter with this command to turn off debugging.

Command Syntax

```
debug mstp all
debug mstp cli
debug mstp packet rx
debug mstp packet tx
debug mstp protocol
debug mstp protocol detail
debug mstp timer
debug mstp timer detail
no debug mstp all
no debug mstp cli
no debug mstp packet rx
no debug mstp packet tx
no debug mstp protocol
no debug mstp protocol detail
no debug mstp timer
no debug mstp timer detail
```

Parameters

all
Echoes all spanning-tree debugging levels to the console.

cli
Echoes spanning-tree commands to the console.

packet
Echoes spanning-tree packets to the console.

rx
Received packets.

tx
Transmitted packets.

protocol
Echoes protocol changes to the console.

detail
Detailed output.

timer
Echoes timer start to the console.

detail
Detailed output.

Command Mode

Execution mode, Privileged execution mode, and Configure mode

© 2026 IP Infusion Inc. Proprietary

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug mstp all
(config)#debug mstp cli
(config)#debug mstp packet rx
(config)#debug mstp protocol detail
(config)#debug mstp timer
```

© 2026 IP Infusion Inc. Proprietary

show debugging mstp

Use this command to display the status of debugging of the MSTP system.

Command Syntax

```
show debugging mstp
```

Parameters

None

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging mstp
MSTP debugging status:
MSTP debugging status:
 MSTP timer debugging is on
 MSTP protocol debugging is on
 MSTP detailed protocol debugging is on
 MSTP cli echo debugging is on
 MSTP transmitting packet debugging is on
 MSTP receiving packet debugging is on
#
```

© 2026 IP Infusion Inc. Proprietary

show spanning-tree

Use this command to show the state of the spanning tree for all STP or RSTP bridge-groups, including named interface and VLANs.

Command Syntax

```
show spanning-tree
show spanning-tree interface IFNAME
show spanning-tree mst
show spanning-tree mst config
show spanning-tree mst interface IFNAME
show spanning-tree mst detail
show spanning-tree mst detail interface IFNAME
show spanning-tree mst instance (<1-63>) interface IFNAME
show spanning-tree mst instance (<1-63> | te-msti)
show spanning-tree statistics bridge <1-32>
show spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <2-4094>) bridge <1-32>
show spanning-tree statistics (interface IFNAME | (instance (<1-63>) | vlan <1-4094>)) bridge <1-32>
show spanning-tree vlan range-index
```

Parameters

interface
Display interface information

mst
Display MST information

statistics
Display statistics of the BPDUs

vlan range-index
Display a VLAN range-index value

config
Display configuration information

detail
Display detailed information

instance
Display instance information

<1-63>
Specify the instance identifier

te-msti
Display Traffic Engineering MSTI instance

<1-32>
Specify the bridge identifier

IFNAME
Display the interface name

<2-4094>
Specify a VLAN identifier, associated with the instance

© 2026 IP Infusion Inc. Proprietary

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command displaying spanning tree information.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%eth2: Ifindex 5 - Port Id 8005 - Role Designated - State Forwarding
%eth2: Designated Path Cost 0
%eth2: Configured Path Cost 200000 - Add type Explicit ref count 1
%eth2: Designated Port Id 8005 - Priority 128 -
%eth2: Root 80000002b328530a
%eth2: Designated Bridge 80000002b328530a
%eth2: Message Age 0 - Max Age 20
%eth2: Hello Time 2 - Forward Delay 15
%eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%eth2: forward-transitions 4
%eth2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%eth2: No portfast configured - Current portfast off
%eth2: portfast bpdu-guard default - Current portfast bpdu-guard off
%eth2: portfast bpdu-filter default - Current portfast bpdu-filter off
%eth2: no root guard configured   - Current root guard off
%eth2: Configured Link Type point-to-point - Current point-to-point
%eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
%eth1: Designated Path Cost 0
%eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
%eth1: Designated Port Id 8004 - Priority 128 -
%eth1: Root 80000002b328530a
%eth1: Designated Bridge 80000002b328530a
%eth1: Message Age 0 - Max Age 20
%eth1: Hello Time 2 - Forward Delay 15
%eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%eth1: forward-transitions 4
%eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%eth1: No portfast configured - Current portfast off
%eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
%eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
%eth1: no root guard configured   - Current root guard off
%eth1: Configured Link Type point-to-point - Current point-to-point
%
%
```

The following is a sample output of this command displaying the state of the spanning tree for interface eth1.

```
#show spanning-tree interface eth1
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
```

```
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
% eth1: Designated Path Cost 0
% eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
% eth1: Designated Port Id 8004 - Priority 128 -
% eth1: Root 80000002b328530a
% eth1: Designated Bridge 80000002b328530a
% eth1: Message Age 0 - Max Age 20
% eth1: Hello Time 2 - Forward Delay 15
% eth1: forward-transitions 4
% eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
% eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
% eth1: no root guard configured   - Current root guard off
```

Explains the show command output fields.

Table 35. show spanning-tree interface output fields

Field	Description
Bridge up	A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments.
Root Path Cost	Root cost for the interface.
Root Port	Interface that is the current elected root port for this bridge.
Bridge Priority	Used for the common instance.
Forward Delay	Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hello Time	Configured number of seconds between transmissions of configuration BPDUs.
Max Age	Maximum age of received protocol BPDUs.
Port Id	Logical interface identifier configured to participate in the MSTP instance.
Role Designated	Designated role for the packets in the interface.
State Forwarding	State of the forwarding packets in the interface.
Designated Path Cost	Designated cost for the interface.
Configured Path Cost	Configured cost for the interface.
Designated Port Id	Port ID of the designated port for the LAN segment this interface is attached to.
Priority	Specify the port priority.
Message Age	Number of seconds elapsed since the most recent BPDU was received.
Forward Timer	The forward delay timer is the time interval that is spent in the listening and learning state.
Msg Age Timer	The message age contains the length of time that has passed since the root bridge initially

© 2026 IP Infusion Inc. Proprietary

Field	Description
	originated the BPDU.
Received RSTP	Number of times the received the RSTP.
Send RSTP	Number of times transmitted the RSTP.

© 2026 IP Infusion Inc. Proprietary

show spanning-tree mst

Use this command to display the filtering database values. This command displays the number of instances created, and VLANs associated with it.

Command Syntax

```
show spanning-tree mst
show spanning-tree mst config
show spanning-tree mst detail
show spanning-tree mst detail interface IFNAME
show spanning-tree mst instance (<1-63>) interface IFNAME
show spanning-tree mst instance (<1-63> | te-msti)
show spanning-tree mst interface IFNAME
```

Parameters

config
Display configuration information.

detail
Display detailed information.

interface
Display interface information.

instance
Display instance information.

<1-63>
Specify the instance identifier.

te-msti
Traffic Engineering MSTI instance.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000002b328530a
% 1: CIST Reg Root Id 80000002b328530a
% 1: CIST Bridge Id 80000002b328530a
% 1: 2 topology change(s) - last topology change Wed Nov 19 22:43:21 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
```

© 2026 IP Infusion Inc. Proprietary

```
% 1: portfast errdisable timeout interval 300 sec%
% Instance VLAN
% 0:        1
% 2:        3-4
```

Explains the show command output fields.

Table 36. show spanning-tree mst output fields

Field	Description
Bridge up	A network bridge is networking process that creates a single aggregate network from multiple communication networks or network segments.
CIST Root Path Cost	Calculated cost to reach the regional root bridge from the bridge where the command is entered.
CIST Root Port	Interface that is the current elected CIST root port for this bridge.
CIST Bridge	A CIST bridge is networking process that creates a single aggregate network from multiple communication networks.
Priority	Specify the port priority.
Forward Delay	Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hello Time	Configured number of seconds between transmissions of configuration BPDUs.
Max Age	Maximum age of received protocol BPDUs.
Max-hops	Configured maximum number of hops a BPDU can be forwarded in the MSTP region.

© 2026 IP Infusion Inc. Proprietary

show spanning-tree statistics

Use this command to display detailed BPDU statistics for a spanning tree instance.

Command Syntax

```
show spanning-tree statistics bridge <1-32>
show spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <2-4094>) bridge <1-32>
show spanning-tree statistics (interface IFNAME | (instance (<1-63>) | vlan <1-4094>)) bridge <1-32>
```

Parameters

<1-32>
Bridge identifier.

<1-63>
MST instance identifier.

IFNAME
Displays the interface name.

<2-4094>
Specify a VLAN identifier, associated with the instance.

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, bridge-group 1 is configured for IEEE on the eth2 interface.

```
#show spanning-tree statistics interface eth2 bridge 1

                Port number = 4 Interface = eth2
                ================================
% BPDU Related Parameters
% ----------------------
% Port Spanning Tree                 : Enable
% Spanning Tree Type                 : Spanning Tree Protocol
% Current Port State                 : Forwarding
% Port ID                            : 8004
% Port Number                        : 4
% Path Cost                          : 19
% Message Age                        : 0
% Designated Root                    : 80:00:52:54:00:b2:49:c1
% Designated Cost                    : 0
% Designated Bridge                  : 80:00:52:54:00:b2:49:c1
% Designated Port Id                 : 0x8004
% Top Change Ack                     : FALSE
% Config Pending                     : FALSE

% PORT Based Information & Statistics
% ----------------------------------
% Config Bpdu's xmitted              : 54327
```

```
% Config Bpdu's received             : 0
% TCN Bpdu's xmitted                 : 50
% TCN Bpdu's received                : 3
% Forward Trans Count                : 1

% STATUS of Port Timers
% ---------------------
% Hello Time Configured              : 2
% Hello timer                        : ACTIVE
% Hello Time Value                   : 0
% Forward Delay Timer                : INACTIVE
% Forward Delay Timer Value          : 0
% Message Age Timer                  : INACTIVE
% Message Age Timer Value            : 0
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0

% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 0
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 3
% Next State                         : Discard/Blocking
% Topology Change Time               : 0


% Other Bridge information & Statistics
  -------------------------------------
% STP Multicast Address              : 01:80:c2:00:00:00
% Bridge Priority                    : 32768
% Bridge Mac Address                 : 80:00:52:54:00:b2
% Bridge Hello Time                  : 2
% Bridge Forward Delay               : 15
% Topology Change Initiator          : 5
% Last Topology Change Occured       : Wed Feb 17 09:39:58 2021
% Topology Change                    : FALSE
% Topology Change Detected           : FALSE
% Topology Change Count              : 5
% Topology Change Last Recvd from    : 00:00:00:00:00:00
```

Explains the show command output fields.

Table 37. show spanning-tree statistics output fields

Field	Description
BPDU Related Parameters	Details of the BPDU related parameters.
PORT Based Information & Statistics	Information of the port and interface for which the statistics are being displayed.
STATUS of Port Timers	Status of the port timers.
Other Port-Specific Info	Specific information about the port.
Other Bridge information & Statistics	Information about bridge and statistics being displayed.

snmp restart mstp

Use this command to restart SNMP in Multiple Spanning Tree Protocol (MSTP).

Command Syntax

```
snmp restart mstp
```

Parameters

None

Default

No default value is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#snmp restart mstp
```

© 2026 IP Infusion Inc. Proprietary

spanning-tree autoedge

Use this command to assist in automatic identification of the edge port.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
spanning-tree autoedge
no spanning-tree autoedge
```

Default

By default, spanning-tree autoedge is disabled

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree autoedge
```

© 2026 IP Infusion Inc. Proprietary

spanning-tree edgeport

Use this command to set a port as an edge-port and to enable rapid transitions.

Use the `no` parameter with this command to set a port to its default state (not an edge-port) and to disable rapid transitions.

Note: This command is an alias to the spanning-tree portfast command. Both commands can be used interchangeably.

Command Syntax

```
spanning-tree edgeport
no spanning-tree edgeport
```

Default

By default, spanning-tree edgeport is disabled

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree edgeport
```

© 2026 IP Infusion Inc. Proprietary

spanning-tree guard

Use this command to enable the root guard feature for the port. This feature disables reception of superior BPDUs.

The root guard feature makes sure that the port on which it is enabled is a designated port. If the root guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

Use the no parameter with this command to disable the root guard feature for the port.

Command Syntax

```
spanning-tree guard root
no spanning-tree guard root
```

Parameters

root

Set to disable reception of superior BPDUs

Default

By default, spanning-tree guard root is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree guard root
```

© 2026 IP Infusion Inc. Proprietary

spanning-tree instance restricted-role

Use this command to set the restricted role value for the instance to TRUE.

Use the `no` parameter with this command to set the restricted role value for the instance to FALSE.

Command Syntax

```
spanning-tree instance <1-63> restricted-role
no spanning-tree instance <1-63> restricted-role
```

Parameters

<1-63>
Specify the instance ID range.

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree instance 2 restricted-role
```

© 2026 IP Infusion Inc. Proprietary

spanning-tree instance restricted-tcn

Use this command to set the restricted TCN value for the instance to TRUE.

Command Syntax

```
spanning-tree instance <1-63> restricted-tcn
no spanning-tree instance <1-63> restricted
```

Parameters

<1-63>
Specify the instance ID range.

Default

By default, restricted TCN value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree instance 2 restricted-tcn
```

spanning-tree link-type

Use this command to enable or disable point-to-point or shared link types.

RSTP has a backward-compatible STP mode, `spanning-tree link-type shared`. An alternative is the `spanning-tree force-version 0`.

Use the `no` parameter with this command to disable rapid transition.

Command Syntax

```
spanning-tree link-type auto
spanning-tree link-type point-to-point
spanning-tree link-type shared
no spanning-tree link-type
```

Parameters

auto
Sets to either point-to-point or shared based on duplex state.

point-to-point
Enables rapid transition.

shared
Disables rapid transition.

Default

By default, spanning-tree link-type is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree link-type point-to-point
(config-if)#no spanning-tree link-type
```

© 2026 IP Infusion Inc. Proprietary

spanning-tree mst configuration

Use this command to enter the Multiple Spanning Tree Configuration mode.

Command Syntax

```
spanning-tree mst configuration
```

Parameters

None

Default

No default value is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#
```

© 2026 IP Infusion Inc. Proprietary

spanning-tree restricted-domain-role

Use this command to set the restricted-domain-role value of the port to TRUE.

Use the `no` parameter with this command to set the restricted-domain-role value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-domain-role
no spanning-tree restricted-domain-role
```

Parameters

None

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-domain-role
```

© 2026 IP Infusion Inc. Proprietary

spanning-tree restricted-role

Use this command to set the restricted-role value of the port to TRUE.

Use the `no` parameter with this command to set the restricted-role value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-role
no spanning-tree restricted-role
```

Parameters

None

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-role
```

spanning-tree restricted-tcn

Use this command to set the restricted TCN value of the port to TRUE.

Use the `no` parameter with this command to set the restricted TCN value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-tcn
no spanning-tree restricted-tcn
```

Parameters

None

Default

By default, restricted TCN value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-tcn
```

© 2026 IP Infusion Inc. Proprietary

spanning-tree te-msti configuration

This command is used to put the terminal into the `te-msti` configuration mode.

After creating a bridge instance and adding VLAN to that bridge instance, use this command to enter `te-msti` configuration mode.

Command Syntax

```
spanning-tree te-msti configuration
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#
```

© 2026 IP Infusion Inc. Proprietary

Errdisable Commands

This section describes the errdisable commands.

errdisable cause 761
errdisable link-flap-setting 763
errdisable mac-move-limit 764
errdisable storm-control 765
errdisable timeout 767
link-flap errdisable 768
mac-move-limit priority 769
show errdisable details 770
show interface errdisable status 771

© 2026 IP Infusion Inc. Proprietary

errdisable cause

Use this command to globally shut down a port when certain errors happen:

- BPDU guard puts an interface configured for Spanning Tree Protocol (STP) Port Fast into the ErrDisable state upon receipt of a STP BPDU to avoid a potential bridging loop.
- If one side of a link-access group (LAG) is configured as a static LAG and the other side as a dynamic LAG, the ports on the side receiving LACP BPDUs go into the ErrDisable state

Note: When link-flap ErrDisable is enabled globally, then all interfaces are enabled. Link-flap ErrDisable can be enabled globally, but disabled for a specific interface with the no link-flap errdisable command.

Note: Stp-Bpdu-Guard is enabled by default on the global level configuration.

Use `no` form of this command to not shut down a port when certain errors happen.

Command Syntax

```
errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap|mac-move-limit}
no errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap|mac-move-limit}
```

Parameters

stp-bpdu-guard
ErrDisable on stp-bpdu-guard

lag-mismatch
ErrDisable on lag-mismatch

link-flap
ErrDisable on link-flap

mac-move-limit
Enable or Disable Mac-Move-Limit

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

© 2026 IP Infusion Inc. Proprietary

Examples

```
#configure terminal
(config)#errdisable cause lag-mismatch
```

errdisable link-flap-setting

Use this command to configure the link-flap errdisable feature:

- An interface should change state as up-down to complete one cycle of a link flap.
- The LED does not glow when an interface is in the errdisable state.
- Errdisable is supported only on physical interfaces.
- A LAG interface does not go into the errdisable state when all of its member ports are in the errdisable state
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. If the accumulated link flap count reaches the maximum flap count for a particular sliding window, a link flap error disable fault is triggered.

Note: Any previous flapping accumulated is flushed when you execute this command.

Command Syntax

```
errdisable link-flap-setting max-flaps <1-100> time <1-1800>
```

Parameters

<1-100>
Maximum flap count

<1-1800>
Sliding window size in seconds

Default

Five flaps in ten seconds:

Maximum flap count: 5

Sliding window size: 10 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable link-flap-setting max-flaps 5 time 20
```

errdisable mac-move-limit

Use this command to set the ErrDisable mac movement limit.

Command Syntax

```
errdisable mac-move-limit <1-1000>
no errdisable mac-move-limit
```

Parameters

<1-1000>
Allowed Mac movement in 5 seconds

Default

By default, mac-move-limit is 1000

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
#configure terminal
(config)#errdisable mac-move-limit 50
(config)#no errdisable mac-move-limit
```

© 2026 IP Infusion Inc. Proprietary

errdisable storm-control

Use this command to configure the storm-control errdisable. Following are the limitation:

- An interface discards BUM traffic during the specified interval to complete one discard-hit cycle.
- The LED does not glow when an interface is in the errdisable state.
- Errdisable is supported only on physical interfaces.
- A LAG interface does not go into the errdisable state when all of its member ports are in the errdisable state.
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. Every 5 seconds, a discard hit count increases if there is BUM traffic being dicarded in that period. If the accumulated discard hit count reaches the maximum count for a particular configurable sliding window, a storm control error disable fault is triggered.

Note: Any previous discard hits accumulated are flushed when you execute this command.

Command Syntax

```
errdisable storm-control discard-hit <1-100> time <1-1800>
no errdisable cause storm-control
```

Parameters

`discard-hit <1-100>`
The maximum number of times that BUM traffic can hit the configured bandwidth threshold in an interface within a certain time window before disabling the interface. During continuous storm control discards, this counter is increased approximately every 5 seconds. Default value is 1.

`time <1-1800>`
Sliding window size in seconds. The time window in seconds in which to consider storm control threshold hits for the purposes of disabling the interface if the discard-hit is overcome during that time. This value must have a minimum value of 6 times discard-hit. Default value is 5 seconds.

Default

- One hit: ten seconds
- Maximum discard hit count: 1
- Sliding window size: 5 seconds

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.5.1

© 2026 IP Infusion Inc. Proprietary

Examples

```
#configure terminal
(config)#errdisable storm-control discard-hit 3 time 20
```

© 2026 IP Infusion Inc. Proprietary

errdisable timeout

Use this command to set the ErrDisable auto-recovery timeout interval.

Command Syntax

```
errdisable timeout interval <10-1000000>
```

Parameters

<10-1000000>
Timeout interval in seconds

Default

By default, zero: timer is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable timeout interval 1000
```

© 2026 IP Infusion Inc. Proprietary

link-flap errdisable

Use this command to shut down the interface when it continually goes up and down.

The link-flap ErrDisable feature must be enabled globally with the errdisable cause (page 761) command.

Note: When link-flap ErrDisable is enabled globally, then all interfaces are enabled. Link-flap ErrDisable can be enabled globally, but disabled for a specific interface with the `no link-flap errdisable` command.

Note: This feature is supported only on physical ports.

Use the `no` form of this command to disable this behavior.

Command Syntax

```
link-flap errdisable
no link-flap errdisable
```

Parameter

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#link-flap errdisable
```

© 2026 IP Infusion Inc. Proprietary

mac-move-limit priority

Use this command to set a priority value to an interface during MAC movement events. The system uses this priority to decide which interface to bring down when MAC movement exceeds the configured limit.

Note:

- The interface with the lower priority goes down first.
- If multiple interfaces have the same priority, the interface with the lower index goes down.

Command Syntax

```
mac-move-limit priority <0-255>
```

Parameters

<0–255>
Specifies the MAC movement limit priority range. A higher value indicates a higher priority. Interfaces with a higher priority value remain active longer during MAC move events.

Default

The default priority of each interface is zero.

Command Mode

Interface mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
OcNOS(config)#interface ce2
OcNOS(config-if)#mac-move-limit priority 250
OcNOS(config-if)#commit

OcNOS#show running-config interface ce2
!
interface ce2
 mac-move-limit priority 250
!
OcNOS#
```

© 2026 IP Infusion Inc. Proprietary

show errdisable details

Use this command to display ErrDisable settings.

Command Syntax

```
show errdisable details
```

Parameters

None

Default

None

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show errdisable details
```

© 2026 IP Infusion Inc. Proprietary

show interface errdisable status

Use this command to display ErrDisable conditions for an interface.

Command Syntax

```
show interface errdisable status
```

Parameters

None

Default

None

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface errdisable status
ge1 lag-mismatch-errdisable
ge2 stp-bpdu-guard-errdisable
```

© 2026 IP Infusion Inc. Proprietary

RPVST+ Commands

This section contains the commands used for Rapid Per VLAN Spanning Tree (RPVST+). RPVST+ enables a bridge to inter-operate with Cisco RPVST+ switches.

RPVST+ uses the Multiple Spanning Tree Protocol (MSTP) with a single VLAN for each Multiple Spanning Tree instance (MSTI). The MST bridges can have different spanning-tree topologies for different VLANs inside a region of similar MST bridges. MSTP, like the Rapid Spanning Tree Protocol (RSTP), provides rapid reconfiguration capabilities and supports load balancing.

This section includes the following commands:

bridge-group vlan 773
bridge protocol rpvst+ 774
bridge rapid-pervlan-spanning-tree 775
bridge vlan 776
bridge vlan priority 777
show spanning-tree rpvst+ 778
spanning-tree rpvst+ configuration 782
spanning-tree vlan restricted-role 783
spanning-tree vlan restricted-tcn 784

© 2026 IP Infusion Inc. Proprietary

bridge-group vlan

Use this command to assign a Rapid Per-VLAN Spanning Tree (RPVST+) instance to a port.

RPVST+ uses port priority as a tiebreaker to determine which port should forward frames for a particular LAN, or which port should be the root port for a VLAN. A lower value implies a better priority. In the case of the same priority, the interface index serves as the tiebreaker, with a lower-numbered interface being preferred over others.

Use the `no` parameter with this command to remove an RPVST+ instance from this port.

Command Syntax

```
bridge-group <1-32> vlan <2-4094>
bridge-group <1-32> vlan <2-4094> path-cost <1-200000000>
bridge-group <1-32> vlan <2-4094> priority <0-240>
no bridge-group <1-32> vlan <2-4094>
no bridge-group <1-32> vlan <2-4094> path-cost
no bridge-group <1-32> vlan <2-4094> priority
```

Parameters

<1-32>
Bridge group identifier.

<2-4094>
VLAN identifier.

<1-200000000>
Cost of a path associated with the interface.

<0-240>
Port priority. A lower priority indicates greater likelihood of the interface becoming a root. Set the priority only in increments of 16.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 1 vlan 10

(config)#interface eth1
(config-if)#bridge-group 1 vlan 10 path-cost 1000

(config-if)#no bridge-group 1 vlan 10 path-cost

(config)#interface eth1
(config-if)#bridge-group 1 vlan 10 priority 240

(config-if)#no bridge-group 1 vlan 10 priority
```

© 2026 IP Infusion Inc. Proprietary

bridge protocol rpvst+

Use this command to enable Rapid Per-VLAN Spanning Tree on a bridge.

Command Syntax

```
bridge <1-32> protocol rpvst+
```

Parameter

<1-32>
Bridge identifier.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 1 protocol rpvst+
```

© 2026 IP Infusion Inc. Proprietary

bridge rapid-pervlan-spanning-tree

Use this command to enable RPVST+ functionality on a bridge.

Use the `no` form of this command to disable RPVST+ functionality on a bridge.

Command Syntax

```
bridge <1-32> rapid-pervlan-spanning-tree enable
no bridge <1-32> rapid-pervlan-spanning-tree enable (bridge-forward|)
```

Parameters

<1-32>
Bridge identifier.

enable
Enable the spanning tree protocol.

bridge-forward
Put all ports of the specified bridge into forwarding state.

Default

When the `bridge-forward` option is used with the `no` parameter, the default behavior is to put all bridge ports in the blocking state.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 rapid-pervlan-spanning-tree enable

(config)#no bridge 1 rapid-pervlan-spanning-tree enable bridge-forward
```

© 2026 IP Infusion Inc. Proprietary

bridge vlan

This command creates or deletes a mapping between an MSTI (Multiple Spanning Tree Instance) and a VLAN for RPVST+ operation. There can be only one VLAN per MST instance if the bridge is configured to run in RPVST+ mode.

The VLAN must have already been created. Spanning tree is enabled on each configured VLAN, and one instance of spanning-tree runs on each configured VLAN.

Use the `no` form of the command to disable this functionality.

Command Syntax

```
bridge <1-32> vlan <2-4094>
no bridge <1-32> vlan <2-4094>
```

Parameters

<1-32>
Bridge identifier.

<2-4094>
VLAN identifier.

Command Mode

RPVST+ Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree rpvst+ configuration
(config-rpvst+)#bridge 1 vlan 2
(config-rpvst+)#no bridge 1 vlan 2
```

© 2026 IP Infusion Inc. Proprietary

bridge vlan priority

This command sets the priority value for the spanning-tree on the bridge. The lower the priority of the VLAN on a bridge, the better the chances of the bridge becoming a root bridge, or a designated bridge for the VLAN.

Use the `no` form of this command to set the priority to its default (32,768).

Command Syntax

```
bridge <1-32> vlan <2-4094> priority <0-61440>
no bridge <1-32> vlan <2-4094> priority
```

Parameters

<1-32>
Bridge identifier.

<2-4094>
VLAN identifier.

<0-61440>
Bridge priority for the common instance. Set the priority in increments of 4096. A lower priority indicates greater likelihood of becoming root.

Default

By default, priority for each VLAN is 32,768

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 vlan 2 priority 80
(config)#no bridge 1 vlan 10 priority
```

© 2026 IP Infusion Inc. Proprietary

show spanning-tree rpvst+

Use this command to display RPVST information.

Command Syntax

```
show spanning-tree rpvst+
show spanning-tree rpvst+ config
show spanning-tree rpvst+ detail
show spanning-tree rpvst+ detail interface IFNAME
show spanning-tree rpvst+ interface IFNAME
show spanning-tree rpvst+ vlan <1-4094>
show spanning-tree rpvst+ vlan <1-4094> interface IFNAME
```

Parameters

config
Display configuration information.

detail
Display detailed information.

IFNAME
Display interface information.

<1-4094>
Display VLAN information

Command Mode

Execution mode and Privileged execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following displays output of this command without any parameters.

```
#show spanning-tree rpvst+
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8001525400b092de
% 1: Bridge Id 8001525400b092de
% 1: last topology change Wed Mar 28 02:31:50 2018
% 1: 1 topology change(s)  - last topology change Wed Mar 28 02:31:50 2018

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 2
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 8001525400b092de
%   eth1: Designated Bridge 8001525400b092de
```

```
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 3 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%
%
%   Instance        VLAN
%   0:              1, 4-10
%   1:              2
%   2:              3
```

The following displays output of this command with the `config` parameter.

```
#show spanning-tree rpvst+ config
%
%  RPVST Configuration Information for bridge 1 :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : Default
%  Revision Level : 0
%  Digest         : 0xB41829F9030A054FB74EF7A8587FF58D
%-------------------------------------------------------

##show spanning-tree rpvst+ detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80015254000be278
% 1: Bridge Id 80015254000be278
% 1: last topology change Tue Jul  6 10:51:37 2021
% 1: 6 topology change(s)  - last topology change Tue Jul  6 10:51:37 2021

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 20000000  - Add type Explicit ref count 3
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 80015254000be278
%   eth1: Designated Bridge 80015254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 2
%   eth1: Restricted-role OFF
%   eth1: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State Forwarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 0
%   eth3: Configured Path Cost 20000000  - Add type Explicit ref count 3
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 80015254000be278
%   eth3: Designated Bridge 80015254000be278
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
```

```
%   eth3: forward-transitions 1
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%

% Instance  1:  Vlans: 2
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 20000000
%   eth1: Configured External Path cost 20000000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 80025254000be278
%   eth1: Designated Bridge 80025254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

% Instance  1:  Vlans: 2
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 20000000
%   eth3: Configured External Path cost 20000000
%   eth3: Configured Internal Priority 128
%   eth3: Configured External Priority 128
%   eth3: Designated Root 80025254000be278
%   eth3: Designated Bridge 80025254000be278
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

% Instance  2:  Vlans: 3
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 20000000
%   eth1: Configured External Path cost 20000000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 80035254000be278
%   eth1: Designated Bridge 80035254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

% Instance  2:  Vlans: 3
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 20000000
%   eth3: Configured External Path cost 20000000
%   eth3: Configured Internal Priority 128
%   eth3: Configured External Priority 128
%   eth3: Designated Root 80035254000be278
%   eth3: Designated Bridge 80035254000be278
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b092de
% 1: Bridge Id 8002525400b092de
```

```
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b092de
%   eth1: Designated Bridge 8002525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%


%
#show spanning-tree rpvst+ vlan 2 interface eth1
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b092de
% 1: Bridge Id 8002525400b092de
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b092de
%   eth1: Designated Bridge 8002525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

spanning-tree rpvst+ configuration

Use this command to enter RPVST+ configuration mode after creating a bridge and adding a VLAN to that bridge. Internally, an RSTP Instance is created for each configured VLAN.

Command Syntax

```
spanning-tree rpvst+ configuration
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#spanning-tree rpvst+ configuration
(config-rpvst+)#
```

spanning-tree vlan restricted-role

Use this command to restrict the role of the interface.

Use the `no` form of this command to not restrict the role of the interface.

Command Syntax

```
spanning-tree vlan <2-4094> restricted-role
no spanning-tree vlan <2-4094> restricted-role
```

Parameters

<2-4094>
VLAN identifier.

Default

The default is to not restrict the role of the interface

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree vlan 10 restricted-role
```

© 2026 IP Infusion Inc. Proprietary

spanning-tree vlan restricted-tcn

Use this command to restrict propagating topology change notifications (TCNs) from the interface.

Use the `no` form of this command to not restrict propagating TCNs from the interface.

Command Syntax

```
spanning-tree vlan <2-4094> restricted-tcn
no spanning-tree vlan <2-4094> restricted_tcn
```

Parameters

<2-4094>
VLAN identifier.

Default

The default is to not restrict propagating TCNs

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree vlan 10 restricted-tcn
(config-if)#no spanning-tree vlan 10 restricted_tcn
```

© 2026 IP Infusion Inc. Proprietary

CROSS-CONNECT (XC) CONFIGURATION

Cross-Connect (XC) Resiliency 786
Topology 786
LFPT (Link-Fault-Pass-Through) 786
Revertive 786
Validation 790
VLAN Cross-Connect (XC) 795
Overview 795
Topology 795
Configuration - Single-tagged VLAN 796
Double-tagged VLAN 799
Cross-Connect (XC) 803
Topology 803
Configuration using Topology-1 803
Configuration using Topology-2 810
Configuring Cross connect using Static lag interfaces 812
CFM over xConnect Configuration 816
Topology 816
Configuration 816
Validation 821

© 2026 IP Infusion Inc. Proprietary

Cross-Connect (XC) Resiliency

This section contains the cross-connect resiliency configuration example.

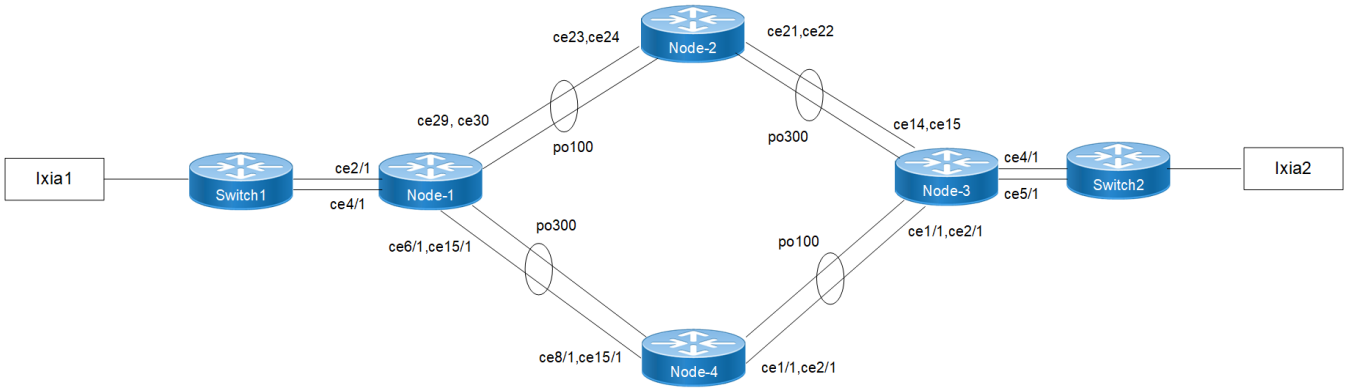
This feature provides resiliency support for port level cross connect when primary link goes down. Whenever, any of the endpoint (EP) of cross-connect goes down, pre-configured backup EP will be chosen and cross-connect will be up with backup EP. Same backup EP cannot be used in another cross-connect link.

This following are the types of EPs supported as backup EPs.

1. Native Ethernet interface
2. LAG interface

Topology

Figure 50. Cross-connect Resiliency Topology



LFPT (Link-Fault-Pass-Through)

If one endpoint goes down, other endpoint of the link is notified and port status is shown as DOWN.

Example: If po100 interface of Node-1 goes down, then Node-2 will inform to Node-3 via LFPT to down the po300 interface.

Revertive

When primary EP comes up, then traffic need to switch from backup EP to Primary EP.

Example: Suppose po100 is down on Node-1, the traffic flow is send to backup EP po300. Whenever the po100 comes up on Node-1 then the traffic flow is switched from backup EP po300 to primary EP po100.

Node-1

`#configure terminal`	Enter configure mode
`(config)#hostname Node-1`	Configure the hostname

`(config)#interface po100`	Create port channel interface
`(config-if)#switchport`	Configure switchport on LAG port
`(config-if)#exit`	Exit the interface level
`(config)#interface ce29`	Enter interface level
`(config-if)#channel-group 100 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface ce30`	Enter interface level
`(config-if)#channel-group 100 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface po300`	Create port channel interface
`(config-if)#switchport`	Configure switchport on LAG interface
`(config-if)#exit`	Exit the interface level
`(config)#interface ce6/1`	Enter interface level
`(config-if)#channel-group 300 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface ce15/1`	Enter interface level
`(config-if)#channel-group 300 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface ce2/1`	Enter interface level
`(config-if)#switchport`	Configure switchport
`(config)#interface ce4/1`	Enter interface level
`(config-if)#switchport`	Configure switchport
`(config-if)#exit`	Exit the interface level
`(config)#cross-connect sample`	Create cross-connect by providing the name
`(config-XC)#ep1 po100 ep2 ce2/1`	Add end-points end-point1 and end-point2
`(config-XC)#backup ep1 po300`	Add backup end-point1
`(config-XC)#backup ep2 ce4/1`	Add backup end-point2
`(config-XC)#cross-connect switchover type revertive`	Configure revertive mode
`(config-XC)#link-fault-pass-through enable`	Configure LFPT

Node-2

`#configure terminal`	Enter configure mode

(config)#hostname Node-2	Configure the hostname
(config)#interface po100	Create port channel interface
(config-if)#switchport	Configure switchport on LAG port
(config-if)#exit	Exit the interface level
(config)#interface ce23	Enter interface level
(config-if)#channel-group 100 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce24	Enter interface level
(config-if)#channel-group 100 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface po300	Create port channel interface
(config-if)#switchport	Configure switchport on LAG interface
(config-if)#exit	Exit the interface level
(config)#interface ce21	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce22	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#cross-connect sample2	Create cross-connect by providing the name
(config-XC)#ep1 po100 ep2 po300	Add end-points end-point1 and end-point2
(config-XC)#link-fault-pass-through enable	Configure LFPT

Node-3

#configure terminal	Enter configure mode
(config)#hostname Node-3	Configure the hostname
(config)#interface po300	Create port channel interface
(config-if)#switchport	Configure switchport on LAG port
(config-if)#exit	Exit the interface level
(config)#interface ce13	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short

© 2026 IP Infusion Inc. Proprietary

(config-if)#exit	Exit the interface level
(config)#interface ce14	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface po100	Create port channel interface
(config-if)#switchport	Configure switchport on LAG interface
(config-if)#exit	Exit the interface level
(config)#interface ce1/1	Enter interface level
(config-if)#channel-group 100 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce2/1	Enter interface level
(config-if)#channel-group 100 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce4/1	Enter interface level
(config-if)#switchport	Configure switchport
(config)#interface ce5/1	Enter interface level
(config-if)#switchport	Configure switchport
(config-if)#exit	Exit the interface level
(config)#cross-connect sample3	Create cross-connect by providing the name
(config-XC)#ep1 po300 ep2 ce4/1	Add end-points end-point1 and end-point2
(config-XC)#backup ep1 po100	Add backup end-point1
(config-XC)#backup ep2 ce5/1	Add backup end-point2
(config-XC)#cross-connect switchover type revertive	Configure revertive mode
(config-XC)#link-fault-pass-through enable	Configure LFPT

Node-4

#configure terminal	Enter configure mode
(config)#hostname Node-4	Configure the hostname
(config)#interface po100	Create port channel interface
(config-if)#switchport	Configure switchport on LAG port
(config-if)#exit	Exit the interface level
(config)#interface ce1/1	Enter interface level
(config-if)#channel-group 100 mode active	Add member port to the port channel interface

© 2026 IP Infusion Inc. Proprietary

(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce2/1	Enter interface level
(config-if)#channel-group 100 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface po300	Create port channel interface
(config-if)#switchport	Configure switchport on LAG interface
(config-if)#exit	Exit the interface level
(config)#interface ce8/1	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce15/1	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#cross-connect sample4	Create cross-connect by providing the name
(config-XC)#ep1 po300 ep2 po100	Add end-points end-point1 and end-point2
(config-XC)#link-fault-pass-through enable	Configure LFPT

Validation

Cross-connect using Dynamic LAG on Node-1

```
Node-1#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: LayeNode-2
  Admin Key: 0100 - Oper Key 0100
     Link: ce29 (5073) sync: 1
     Link: ce30 (5074) sync: 1
--------------------------------------
  Aggregator po300 100300
  Aggregator Type: LayeNode-2
  Admin Key: 0300 - Oper Key 0300
     Link: ce6/1 (5005) sync: 1
     Link: ce15/1 (5006) sync: 1

Node-1#sh running-config cross-connect
!
cross-connect sample
 ep1 po100 ep2 ce2/1
 cross-connect switchover type revertive
 link-fault-pass-through enable
 backup ep1 po300
 backup ep2 ce4/1
!
```

```
Node-1#sh cross-connect
Codes: EP - Endpoint, Bkp_EP - Backup endpoint
       *  - Active Endpoint, none - not configured
Cross-connect name : sample
EP1:po100      EP2:ce2/1       Revertive:Yes        Bkp_EP1:po300      Bkp_EP2:ce4/1      Admin
Status:UP         Oper Status:UP
+=============================================================================================================
==============+
| EP       | OVID     | IVID     | Rx packets    | Rx bytes      | Tx packets    |Tx
bytes       |Interface Status|
+=============================================================================================================
==============+
| EP1*     |     -    |     -
    |0              |0              |5974137342     |764688374912   |UP             |
| EP2*     |     -    |     -
    |5973605019     |764619747456   |0              |0              |UP             |
| bkp_EP1  |     -    |     -
    |5973879754     |764654827904   |0              |0              |UP             |
| bkp_EP2  |     -    |     -
    |0              |0              |0              |0              |UP             |
+=============================================================================================================
==============+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

Cross-connect using Dynamic LAG on Node-2

```
Node-2#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: LayeNode-2
  Admin Key: 0100 - Oper Key 0100
     Link: ce23 (5067) sync: 1
     Link: ce24 (5068) sync: 1
-------------------------------------
  Aggregator po300 100300
  Aggregator Type: LayeNode-2
  Admin Key: 0300 - Oper Key 0300
     Link: ce21 (5063) sync: 1
     Link: ce22 (5064) sync: 1

Node-2#show running-config cross-connect
!
cross-connect sample2
!
cross-connect sample2
 ep1 po100 ep2 po300
 link-fault-pass-through enable
!

Node-2#sh cross-connect
Codes: EP - Endpoint, Bkp_EP - Backup endpoint
       *  - Active Endpoint, none - not configured
Cross-connect name : sample2
EP1:po100      EP2:po300       Revertive:No         Bkp_EP1:None       Bkp_EP2:None       Admin
Status:UP         Oper Status:UP
+=============================================================================================================
==============+
| EP       | OVID     | IVID     | Rx packets    | Rx bytes      | Tx packets    |Tx
bytes       |Interface Status|
+=============================================================================================================
==============+
| EP1*     |     -    |     -
    |3710           |470780         |723            |90626          |UP             |
| EP2*     |     -    |     -
```

```
    |72             |6468           |14             |1548           |UP             |
+=============================================================================================================
==============+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

Cross-connect using Dynamic LAG on Node-3

```
Node-3#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: LayeNode-2
  Admin Key: 0100 - Oper Key 0100
     Link: ce1/1 (5005) sync: 1
     Link: ce2/1 (5006) sync: 1
--------------------------------------
  Aggregator po300 100300
  Aggregator Type: LayeNode-2
  Admin Key: 0300 - Oper Key 0300
     Link: ce13 (5011) sync: 1
     Link: ce14 (5012) sync: 1

Node-3#sh running-config cross-connect
!
cross-connect sample3
 ep1 po300 ep2 ce4/1
 cross-connect switchover type revertive
 link-fault-pass-through enable
 backup ep1 po100
 backup ep2 ce5/1
!

Node-3#sh cross-connect
Codes: EP - Endpoint, Bkp_EP - Backup endpoint
       *  - Active Endpoint, none - not configured
Cross-connect name : sample3
EP1:po300     EP2:ce4/1      Revertive:Yes        Bkp_EP1:po100     Bkp_EP2:ce5/1      Admin
Status:UP         Oper Status:UP
+=============================================================================================================
==============+
| EP       | OVID     | IVID     | Rx packets    | Rx bytes      | Tx packets    |Tx
bytes       |Interface Status|
+=============================================================================================================
==============+
| EP1*     |     -    |     -    |201            |13536          |83318167485    |10664725404928
|UP             |
| EP2*     |     -    |     -    |93501105144    |11968141426060
|2              |128            |UP             |
| bkp_EP1  |     -    |     -
    |0              |0              |10171776397    |1301987373312  |UP             |
| bkp_EP2  |     -    |     -    |93501187674    |11968152089344
|0              |0              |UP             |
+=============================================================================================================
==============+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

Cross-connect using Dynamic LAG on Node-4

```
Node-4#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: LayeNode-2
  Admin Key: 0100 - Oper Key 0100
     Link: ce1/1 (5005) sync: 1
     Link: ce2/1 (5006) sync: 1
--------------------------------------
  Aggregator po300 100300
  Aggregator Type: LayeNode-2
  Admin Key: 0300 - Oper Key 0300
     Link: ce8/1 (5009) sync: 1
     Link: ce15/1 (5012) sync: 1

Node-4#sh running-config cross-connect
!
 cross-connect sample4
 ep1 po300 ep2 po100
 link-fault-pass-through enable
!
```

Disable the Cross-connect on Node-1

`#configure terminal`	Enter configure mode
`(config)#cross-connect sample`	Enter into cross-connect mode
`(config-XC)#disable`	Disabling the cross-connect
`(config-XC)#exit`	Exit the cross-connect

Validation

```
Node-1#sh cross-connect
Codes: EP - Endpoint, Bkp_EP - Backup endpoint
       *  - Active Endpoint, none - not configured
Cross-connect name : sample
EP1:po100      EP2:ce2/1       Revertive:Yes        Bkp_EP1:po300      Bkp_EP2:ce4/1      Admin
Status:DOWN         Oper Status:DOWN
+=============================================================================================================
==============+
| EP       | OVID     | IVID     | Rx packets    | Rx bytes      | Tx packets    |Tx
bytes       |Interface Status|
+=============================================================================================================
==============+
| EP1*     |     -    |     -
    |0              |0              |5974137342     |764688374912   |UP             |
| EP2*     |     -    |     -
    |5973605019     |764619747456   |0              |0              |UP             |
| bkp_EP1  |     -    |     -
    |5973879754     |764654827904   |0              |0              |UP             |
| bkp_EP2  |     -    |     -
    |0              |0              |0              |0              |UP             |
+=============================================================================================================
==============+

cross-connect summary
Total XC    : 1
Admin Up    : 0
Admin Down  : 1
Total Rules : 0
```

Disable the cross-connect on Node-1

Enable the Cross-connect Node-1

`#configure terminal`	Enter configure mode
`(config)#cross-connect sample`	Enter into cross-connect mode
`(config-XC)#no disable`	Enable the cross-connect
`(config-XC)#exit`	Exit the cross-connect

Validation

Cross-connect after enable on Node-1

```
Node-1#sh cross-connect
Codes: EP - Endpoint, Bkp_EP - Backup endpoint
       *  - Active Endpoint, none - not configured
Cross-connect name : sample
EP1:po100      EP2:ce2/1       Revertive:Yes        Bkp_EP1:po300      Bkp_EP2:ce4/1      Admin
Status:UP         Oper Status:UP
+=============================================================================================================
==============+
| EP       | OVID     | IVID     | Rx packets    | Rx bytes      | Tx packets    |Tx
bytes       |Interface Status|
```

VLAN Cross-Connect (XC)

Overview

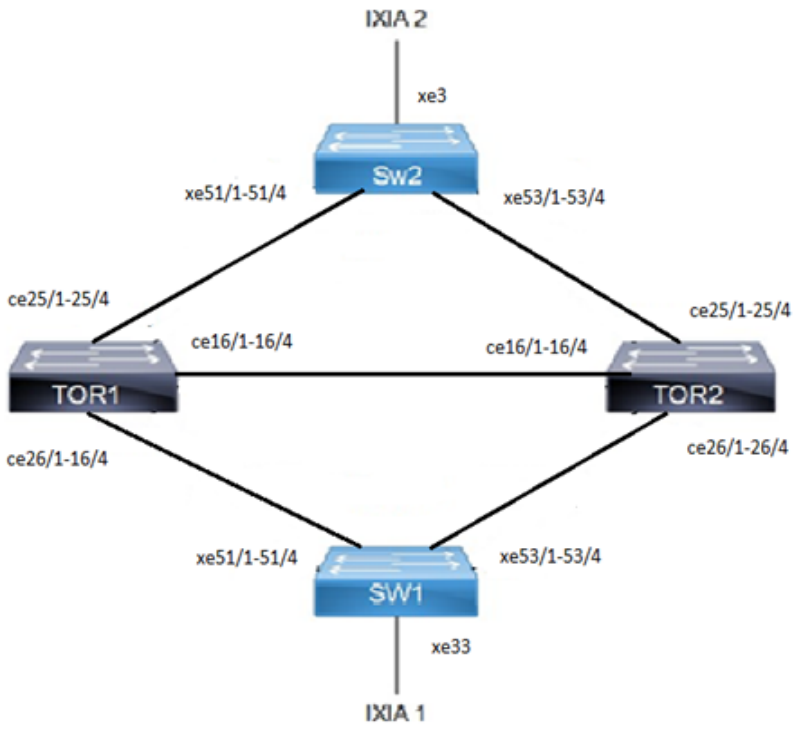
VLAN cross connect creates a L2 bridge between two given endpoints on the same device. Once configured, every packets arriving at one of the endpoints with specific VLAN tag will be sent to another endpoint directly. In current implementation it matches VLAN tag as per configuration in device. If device is configured to match single tag then only outer most tagged will be matched whether packet is double tagged. If device is configured to match double tag then outer tag as well as inner tag will match If the packet is double tagged.

Notes:

- End point or source point could be a physical (Native Ethernet) port or logical port (po, vlan etc).
- Same Vlan ID cannot be used in 2 cross connects.
- Different type of L2, L3 and subscriber services are supported over cross.
- The XC implementation will forward all packets and MAC address learning is disabled.

Topology

Figure 51. Cross-connect topology



Configuration - Single-tagged VLAN

TOR1

#configure terminal	Enter Configure mode.
(config)#interface ce25/1	Enter Interface mode
(config-if)#switchport	Configure interface as a layer 2 port
(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit interface mode
(config)#interface ce16/1	Enter Interface mode
(config-if)#switchport	Configure interface as a layer 2 port
(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit interface mode
(config)#cross-connect VC1	Create cross-connect (XC)
(config-XC)# vlan ep1 ce25/1 ep2 ce16/1	Add Endpoints to XC
(config-VXC)# outer-vlan 100	Outer-vlanId associated with the XC
(config-VXC)#commit	Commit candidate configuration to be running configuration
(config-VXC)#end	Return to privilege mode

TOR2

#configure terminal	Enter Configure mode.
(config)#interface ce16/1	Enter Interface mode
(config-if)#switchport	Configure interface as a layer 2 port
(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit interface mode
(config)#interface ce26/1	Enter Interface mode
(config-if)#switchport	Configure interface as a layer 2 port
(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit interface mode
(config)#cross-connect VC1	Create cross-connect (XC)
(config-XC)# vlan ep1 ce16/1 ep2 ce26/1	Add Endpoints to XC
(config-VXC)# outer-vlan 100	Outer-vlanId associated with the XC
(config-VXC)#commit	Commit candidate configuration to be running

	configuration
(config-VXC)#end	Return to privilege mode

SW2

#configure terminal	Enter Configure mode.
(config)#bridge 1 protocol mstp	Add a bridge (1) to the multiple spanning tree table
(config)#vlan database	Enter the VLAN configuration mode
(config-vlan)#vlan 100 bridge 1 state enable	Enable the state of VLAN 100 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 100 on bridge 1
(config-vlan)#commit	Commit candidate configuration to be running configuration
(config-vlan)#exit	Exit the VLAN configuration mode
(config)#interface xe51/1	Enter Interface mode
(config-if)#switchport	Configure interface as a layer 2 port
(config-if)#bridge-group 1	Associating the interface to bridge-group 1
(config-if)#switchport mode trunk	set the switching characteristics of the Layer 2 interface
(config-if)#switchport trunk allowed vlan all	Allow all VLANs to transmit and receive through the interface
(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit interface mode
(config)#interface xe3	Enter Interface mode
(config-if)#switchport	Configure interface as a layer 2 port
(config-if)#bridge-group 1	Associating the interface to bridge-group 1
(config-if)#switchport mode trunk	set the switching characteristics of the Layer 2 interface
(config-if)#switchport trunk allowed vlan all	Allow all VLANs to transmit and receive through the interface
(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit interface mode

SW1

#configure terminal	Enter Configure mode.
(config)#bridge 1 protocol mstp	Add a bridge (1) to the multiple spanning tree table
(config)#vlan database	Enter the VLAN configuration mode
(config-vlan)#vlan 100 bridge 1 state enable	Enable the state of VLAN 100 on bridge 1. Specifying

	an enable state allows forwarding of frames over VLAN 100 on bridge 1
(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit the VLAN configuration mode
(config)#interface xe53/1	Enter Interface mode
(config-if)#switchport	Configure interface as a layer 2 port
(config-if)#bridge-group 1	Associating the interface to bridge-group 1
(config-if)#switchport mode trunk	set the switching characteristics of the Layer 2 interface
(config-if)#switchport trunk allowed vlan all	Allow all VLANs to transmit and receive through the interface
(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit interface mode
(config)#interface xe33	Enter Interface mode
(config-if)#switchport	Configure interface as a layer 2 port
(config-if)#bridge-group 1	Associating the interface to bridge-group 1
(config-if)#switchport mode trunk	set the switching characteristics of the Layer 2 interface
(config-if)#switchport trunk allowed vlan all	Allow all VLANs to transmit and receive through the interface
(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit interface mode

Validation

TOR1

```
#show cross-connect
Cross-connect name : VC1
EP1:ce25/1              EP2:ce16/1         Admin Status:UP            OperStatus:UP
+=============================================================================================+
| EP  | OVID     | IVID     | Rx packets  | Rx bytes    | Tx packets  | Tx bytes     |
+=============================================================================================+
| EP1 |100       |     -    |6572258      |9858387000  |0            |0             |
| EP2 |100       |     -    |0            |0           |6572224      |9858336000    |
+=============================================================================================+
Cross-connect summary Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

TOR2

```
#show cross-connect
Cross-connect name : VC1
```

```
EP1:ce16/1              EP2:ce26/1         Admin Status:UP            OperStatus:UP
+=============================================================================================+
| EP  | OVID     | IVID     | Rx packets  | Rx bytes    | Tx packets  | Tx bytes     |
+=============================================================================================+
| EP1 |100       |     -    |616588       |924882000    |0            |0             |
| EP2 |100       |     -    |0            |0            |618615       |927922500     |
+=============================================================================================+
Cross-connect summary Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

Double-tagged VLAN

TOR1

`#configure terminal`	Enter Configure mode.
`(config)#interface ce25/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#commit`	Commit candidate configuration to be running configuration
`(config-if)#exit`	Exit interface mode
`(config)#interface ce16/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#commit`	Commit candidate configuration to be running configuration
`(config-if)#exit`	Exit interface mode
`(config)#cross-connect VC2`	Create cross-connect (XC)
`(config-XC)# vlan ep1 ce25/1 ep2 ce16/1`	Add Endpoints to XC
`(config-VXC)# outer-vlan 200-300 inner-vlan 20-30`	Outer-vlanId and Inner-vlanId with range associated with the XC
`(config-VXC)#commit`	Commit candidate configuration to be running configuration
`(config-VXC)#end`	Return to privilege mode

TOR2

`#configure terminal`	Enter Configure mode.
`(config)#interface ce16/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#commit`	Commit candidate configuration to be running configuration
`(config-if)#exit`	Exit interface mode
`(config)#interface ce26/1`	Enter Interface mode

© 2026 IP Infusion Inc. Proprietary

`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#commit`	Commit candidate configuration to be running configuration
`(config-if)#exit`	Exit interface mode
`(config)#cross-connect VC2`	Create cross-connect (XC)
`(config-XC)# vlan ep1 ce16/1 ep2 ce26/1`	Add Endpoints to XC
`(config-VXC)# outer-vlan 200-300 inner-vlan 20-30`	Outer-vlanId and Inner-vlanId with range associated with the XC
`(config-VXC)#commit`	Commit candidate configuration to be running configuration
`(config-VXC)#end`	Return to privilege mode

SW2

`#configure terminal`	Enter Configure mode.
`(config)#bridge 1 protocol mstp`	Add a bridge (1) to the multiple spanning tree table
`(config)#vlan database`	Enter the VLAN configuration mode
`(config-vlan)#vlan 200-300 bridge 1 state enable`	Enable the state of VLANs 200-300 on bridge 1. Specifying an enable state allows forwarding of frames over VLANs 200-300 on bridge 1
`(config-vlan)#commit`	Commit candidate configuration to be running configuration
`(config-vlan)#exit`	Exit the VLAN configuration mode
`(config)#interface xe51/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`(config-if)#switchport mode trunk`	set the switching characteristics of the Layer 2 interface
`(config-if)#switchport trunk allowed vlan all`	Allow all VLANs to transmit and receive through the interface
`(config-if)#commit`	Commit candidate configuration to be running configuration
`(config-if)#exit`	Exit interface mode
`(config)#interface xe3`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`(config-if)#switchport mode trunk`	set the switching characteristics of the Layer 2 interface
`(config-if)#switchport trunk allowed vlan all`	Allow all VLANs to transmit and receive through the interface

© 2026 IP Infusion Inc. Proprietary

(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit interface mode

SW1

#configure terminal	Enter Configure mode.
(config)#bridge 1 protocol mstp	Add a bridge (1) to the multiple spanning tree table
(config)#vlan database	Enter the VLAN configuration mode
(config-vlan)#vlan 200-300 bridge 1 state enable	Enable the state of VLANs 200-300 on bridge 1. Specifying an enable state allows forwarding of frames over VLANs 200-300 on bridge 1
(config-vlan)#commit	Commit candidate configuration to be running configuration
(config-vlan)#exit	Exit the VLAN configuration mode
(config)#interface xe53/1	Enter Interface mode
(config-if)#switchport	Configure interface as a layer 2 port
(config-if)#bridge-group 1	Associating the interface to bridge-group 1
(config-if)#switchport mode trunk	Set the switching characteristics of the Layer 2 interface
(config-if)#switchport trunk allowed vlan all	Allow all VLANs to transmit and receive through the interface
(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit nterface mode
(config)#interface xe33	Enter Interface mode
(config-if)#no shutdown	Bring interface up
(config-if)#switchport	Configure interface as a layer 2 port
(config-if)#bridge-group 1	Associating the interface to bridge-group 1
(config-if)#switchport mode trunk	Set the switching characteristics of the Layer 2 interface
(config-if)#switchport trunk allowed vlan all	Allow all VLANs to transmit and receive through the interface
(config-if)#commit	Commit candidate configuration to be running configuration
(config-if)#exit	Exit interface mode

Validation

TOR1

```
#show cross-connect
```

```
Cross-connect name : VC2
EP1:ce25/1              EP2:ce16/1         Admin Status:UP            OperStatus:UP
+=============================================================================================+
| EP  | OVID     | IVID     | Rx packets  | Rx bytes    | Tx packets  | Tx bytes    |
+=============================================================================================+
| EP1 |200-300   |20-30     |442089       |663133500    |0            |0            |
| EP2 |200-300   |20-30     |0            |0            |444123       |666184500    |
+=============================================================================================+
Cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

TOR2

```
#show cross-connect
Cross-connect name : VC2
EP1:ce16/1              EP2:ce26/1         Admin Status:UP            OperStatus:UP
+=============================================================================================+
| EP  | OVID     | IVID     | Rx packets  | Rx bytes    | Tx packets  | Tx bytes    |
+=============================================================================================+
| EP1 |200-300   |20-30     |267607       |401410500    |0            |0            |
| EP2 |200-300   |20-30     |0            |0            |269640       |404460000    |
+=============================================================================================+
Cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

Cross-Connect (XC)

This section contains the cross-connect configuration examples to connect the two cross connection ports.

The cross connect is bi-directional. The traffic which is received on the first interface is transmitted out to the second interface and the traffic which is received on the second interface is transmitted out to the first interface.

It is point-to-point and same end points (EP) cannot be used for another cross connect.

This following are the types of end points supported by this port based on cross connect.

a. Native Ethernet interface

b. LAG interface

Topology

Figure 52. Cross-connect Topology-1

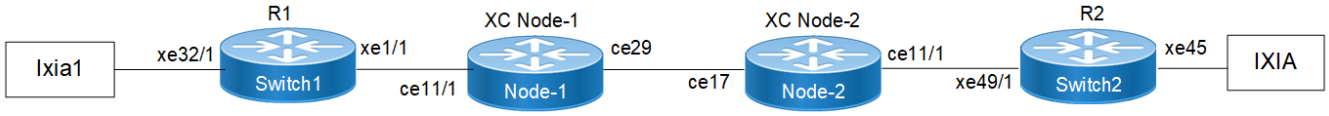
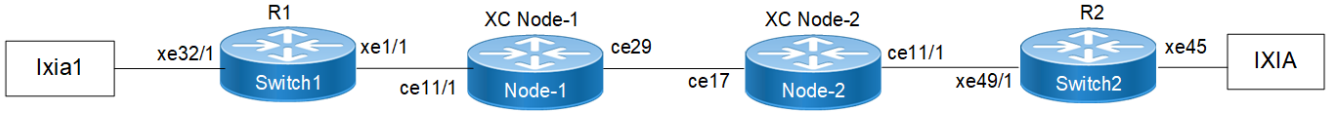


Figure 53. Cross-connect Topology-2



Configuration using Topology-1

The following configuration example will illustrate OSPF, BFD and BGP session establishments via Cross-connect:

R1

`OcNOS#configure terminal`	Enter into configure terminal
`OcNOS(config)#hostname R1`	Configure the host name
`R1(config)#in xe1/1`	Enter into interface level
`R1(config-if)#ip address 10.10.10.1/24`	Configure ip address to the interface
`R1(config-if)#exit`	Exiting from interface level
`R1(config)#in xe32/1`	Enter into interface mode
`R1(config-if)#ip address 20.20.20.1/24`	Configure ip address to the interface
`R1(config-if)#exit`	Exiting from interface level
`R1(config)#interface lo`	Enter into loop-back interface
`R1(config-if)#ip address 1.1.1.1/24 secondary`	Configuring secondary ip address
`R1(config-if)#`	Exiting the loop-back interface level

© 2026 IP Infusion Inc. Proprietary

`R1(config)#bfd interval 3 minrx 3 multiplier 3`	Configuring bfd options
`R1(config)#router ospf 10`	Configuring OSPF process
`R1(config-router)#router-id 1.1.1.1`	Configuring router-id
`R1(config-router)#network 10.10.10.0 0.0.0.255 area 0`	Configuring Network id and Area id
`R1(config-router)#redistribute connected`	Configuring redistribute connected
`R1(config-router)#bfd all-interfaces`	Configuring bfd on all-interfaces
`R1(config-router)#exit`	Exiting the OSPF process
`R1(config)#router bgp 100`	Configuring bgp process
`R1(config-router)#neighbor 10.10.10.2 remote-as 200`	Configuring neighbor details
`R1(config-router)#end`	Exiting from the bgp process

XC Node-1

`OcNOS#configure terminal`	Entering into the configure terminal mode
`OcNOS(config)#hostname Xc Node-1`	Configuring the hostname
`Xc Node-1(config)#interface ce29`	Entering into interface level
`Xc Node-1(config-if)#switchport`	Configuring switchport
`Xc Node-1(config-if)#exit`	Exiting the interface level
`Xc Node-1(config)#in ce11/1`	Entering the interface level
`Xc Node-1(config-if)#switchport`	Configuring the switchport
`Xc Node-1(config-if)#exit`	Exiting the interface level
`Xc Node-1(config)#cross-connect OSPF_BFD_BGP`	Configuring the Cross-connect
`Xc Node-1(config-XC)#ep1 ce11/1 ep2 ce29`	Creating endpoints
`Xc Node-1(config-XC)#end`	Exiting cross-connect mode

Xc Node-2

`OcNOS#configure terminal`	Entering into the configure terminal mode
`OcNOS(config)#hostname Xc Node-2`	Configuring the hostname
`Xc Node-2(config)#interface ce17`	Entering into interface level
`Xc Node-2(config-if)#switchport`	Configuring switchport
`Xc Node-2(config-if)#exit`	Exiting the interface level
`Xc Node-2(config)#interface ce11/1`	Entering the interface level
`Xc Node-2(config-if)#switchport`	Configuring the switchport
`Xc Node-2(config-if)#exit`	Exiting the interface level
`Xc Node-2(config)#cross-connect OSPF_BFD_BGP-1`	Configuring the Cross-connect
`Xc Node-2(config-XC)#ep1 ce17 ep2 ce11/1`	Creating endpoints
`Xc Node-2(config-XC)#end`	Exiting cross-connect mode

© 2026 IP Infusion Inc. Proprietary

R2

OcNOS#conf terminal	Enter into configure terminal
OcNOS(config)#hostname R2	Configure the host name
R2(config)#in xe49/1	Enter into interface level
R2(config-if)#ip address 10.10.10.2/24	Configure ip address to the interface
R2(config-if)#exit	Exiting from interface level
R2(config)#int xe45	Enter into interface mode
R2(config-if)#ip address 30.30.30.1/24	Configure ip address to the interface
R2(config-if)#exit	Exiting from interface level
R2(config)#interface lo	Enter into loop-back interface
R2(config-if)#ip address 2.2.2.2/24 secondary	Configuring secondary ip address
R2(config-if)#exit	Exiting the loop-back interface level
R2(config)#bfd interval 3 minrx 3 multiplier 3	Configuring bfd options
R2(config)#router ospf 10	Configuring OSPF process
R2(config-router)#router-id 2.2.2.2	Configuring router-id
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0	Configuring Network id and Area id
R2(config-router)#redistribute connected	Configuring redistribute connected
R2(config-router)#bfd all-interfaces	Configuring bfd on all-interfaces
R2(config-router)#exit	Exiting the OSPF process
R2(config)#router bgp 200	Configuring bgp process
R2(config-router)#neighbor 10.10.10.1 remote-as 100	Configuring neighbor details
R2(config-router)#end	Exiting from the bgp process

Validation

Cross-connect Validation

```
Xc Node-1#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
OSPF_BFD_BGP       -      -      ce11/1           ce29             UP
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
Xc Node-1#

Xc Node-1#show running-config cross-connect
cross-connect OSPF_BFD_BGP
 ep1 ce11/1 ep2 ce29

Xc Node-2#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
```

```
------------------+------+------+---------------+----------------+------------
OSPF_BFD_BGP-1     -      -      ce17             ce11/1           UP
------------------+------+------+---------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
Xc Node-2#
Xc Node-2#show running-config cross-connect
cross-connect OSPF_BFD_BGP-1
 ep1 ce17 ep2 ce11/1
```

OSPF Validation

```
R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
       Instance ID
2.2.2.2           1   Full/Backup      00:00:37    10.10.10.2      xe1/1
          0
R1#

R2#show ip ospf neighbor
Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
       Instance ID
1.1.1.1           1   Full/Backup      00:00:38    10.10.10.1      xe49/1
          0
R2#
```

BFD Validation

```
R1#show bfd interface xe1/1
Interface:      xe1/1  ifindex: 10001 state:   UP
Interface level configuration: NO ECHO, NO SLOW TMR
Min Tx: 3  Min Rx: 3  Multiplier: 3
R1#

R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================================

Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
      Down-Reason    Remote-Addr
1          1            IPv4         Single-Hop  Up          00:02:54  xe1/1
      NA             10.10.10.2/32
Number of Sessions:    1

R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================================

Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
      Down-Reason    Remote-Addr
1          1            IPv4         Single-Hop  Up          00:02:54  xe1/1
      NA             10.10.10.2/32
Number of Sessions:    1

R1#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
```

```
================================================================================


Session Interface Index : 10001          Interface name :xe1/1
Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.10.10.1/32
Remote Discriminator : 1                 Remote Address : 10.10.10.2/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 3                Min Rx: 3                Multiplier: 3
Neg Tx: 3                Neg Rx: 3                Neg detect mult: 3
Min echo Tx: 1000        Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000117138              Pkt Out : 00000000000000117172
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                               UPTIME : 00:05:42

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
R1#

R2#show bfd interface xe49/1
Interface:     xe49/1  ifindex: 10049 state:   UP
Interface level configuration: NO ECHO, NO SLOW TMR
Min Tx: 3  Min Rx: 3  Multiplier: 3

R2#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================

Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
      Down-Reason    Remote-Addr
1          1            IPv4         Single-Hop  Up          00:04:12  xe49/1
      NA             10.10.10.1/32
Number of Sessions:    1

R2#sh bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================

Session Interface Index : 10049          Interface name :xe49/1
Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.10.10.2/32
Remote Discriminator : 1                 Remote Address : 10.10.10.1/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None
```

```
Timers in Milliseconds :
Min Tx: 3                 Min Rx: 3                 Multiplier: 3
Neg Tx: 3                 Neg Rx: 3                 Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000044905              Pkt Out : 00000000000000044905
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                               UPTIME : 00:02:11

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

BGP Validation

```
R1#sh bgp neighbors
BGP neighbor is 10.10.10.2, remote AS 200, local AS 100, external link
  BGP version 4, local router ID 10.10.10.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:04:00
  Last read 00:00:08, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 12 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.1, Local port: 179
Foreign host: 10.10.10.2, Foreign port: 58033
Nexthop: 10.10.10.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

R2#sh ip bgp neighbors
BGP neighbor is 10.10.10.1, remote AS 100, local AS 200, external link
  BGP version 4, local router ID 2.2.2.2, remote router ID 10.10.10.1
  BGP state = Established, up for 00:00:03
  Last read 00:00:03, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 2 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
```

```
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.2, Local port: 58033
Foreign host: 10.10.10.1, Foreign port: 179
Nexthop: 10.10.10.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
R2#
```

Show interface counters

```
R1#sh interface counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1/1               6.91           13082945      6.91           13082949
 xe32/1              6.91           13082325      6.91           13082325
R1#


Xc Node-1#sh interface counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ce11/1              6.91           13082437      6.91           13082437
 ce29                6.91           13082457      6.91           13082458
Xc Node-1#
Xc Node-1# sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
OSPF_BFD_BGP       -      -      ce11/1           ce29             UP
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
Xc Node-1#

Xc Node-2#sh interface counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ce11/1              6.91           13082428      6.91           13082429
 ce17                6.91           13082381      6.91           13082378

 Xc Node-2#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
OSPF_BFD_BGP-1     -      -      ce17             ce11/1           UP
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
Xc Node-2#

R2#sh interface counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe45                6.91           13081988      6.91           13081988
 xe49/1              6.91           13082339      6.91           13082339
R2#
```

Configuration using Topology-2

The following configuration example illustrates configuration of cross-connect using LAG interfaces on Xc Node:

Configuration on R1 Node

`R1# configure terminal`	Enter configure mode
`R1(config)#interface po100`	Creating port channel interface
`R1(config-if)#exit`	Exit the interface level
`R1(config)#interface xe1/1`	Enter interface level
`R1(config-if)# channel-group 100 mode active`	Adding member port to the port channel interface
`R1(config-if)#exit`	Exit the interface level
`R1(config)#interface xe1/2`	Enter interface level
`R1(config-if)# channel-group 100 mode active`	Adding member port to the port channel interface
`R1(config-if)#exit`	Exit the interface level

Configuring Cross connect using dynamic lag interfaces on XC_node1

`XC_node1# configure terminal`	Enter configure mode
`XC_node1(config)#interface po100`	Creating port channel interface
`XC_node1(config-if)#switchport`	Configuring Switchport to the interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface po200`	Creating port channel interface
`XC_node1(config-if)#switchport`	Configuring Switchport to the interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce11/1`	Enter interface level
`XC_node1(config-if)# channel-group 100 mode active`	Adding member port to the port channel interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce11/2`	Enter interface level
`XC_node1(config-if)# channel-group 100 mode active`	Adding member port to the port channel interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce29`	Enter interface level
`XC_node1(config-if)# channel-group 200 mode active`	Adding member port to the port channel interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce30`	Enter interface level
`XC_node1(config-if)# channel-group 200 mode active`	Adding member port to the port channel interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#cross-connect lag`	Create cross-connect by providing the name

© 2026 IP Infusion Inc. Proprietary

XC_node1(config-XC)#ep1 po100 ep2 po200	Adding end-points ep1 and ep2 as lag interfaces
XC_node1(config-XC)#exit	Exit Cross-connect mode
XC_node1(config)#exit	Exit Configure terminal mode

Configuring Cross connect using dynamic lag interfaces on XC_node2

XC_node2# configure terminal	Enter configure mode
XC_node2(config)#interface po200	Creating port channel interface
XC_node2(config-if)#switchport	Configuring Switchport to the interface
XC_node2(config-if)#exit	Exit the interface level
XC_node2(config)#interface ce29	Enter interface level
XC_node2(config-if)# channel-group 200 mode active	Adding member port to the port channel interface
XC_node2(config-if)#exit	Exit the interface level
XC_node2(config)#interface ce30	Enter interface level
XC_node2(config-if)# channel-group 200 mode active	Adding member port to the port channel interface
XC_node2(config-if)#exit	Exit the interface level
XC_node2(config)#interface ce11/1	Enter interface level
XC_node2(config-if)#Switchport	Configure switchport to the interface
XC_node2(config-if)#exit	Exit the interface level
XC_node2(config)#cross-connect lag	Create cross-connect by providing the name
XC_node2(config-XC)#ep1 po100 ep2 ce11/1	Adding end-points ep1 and ep2 as lag interfaces
XC_node2(config-XC)#exit	Exit Cross-connect mode
XC_node2(config)#exit	Exit Configure terminal mode

Validation

Cross-connect using Dynamic lag on XC_node1

```
XC_node1#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
lag                -      -      po100            po200            UP
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0

XC_node1#sh running-config cross-connect
!
cross-connect lag
 ep1 po100 ep2 po200
!
XC_node1#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: Layer2
  Admin Key: 0100 - Oper Key 0100
     Link: ce11/1 (5073) sync: 1
```

```
     Link: ce11/2 (5074) sync: 1
--------------------------------------
  Aggregator po200 100200
  Aggregator Type: Layer2
  Admin Key: 0200 - Oper Key 0200
     Link: ce30 (5005) sync: 1
     Link: ce29 (5006) sync: 1
```

Cross-connect using Dynamic lag on XC_node2

```
XC_node2#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
lag                -      -      po200           ce11/1            UP
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0

XC Node-2#show running-config cross-connect
!
cross-connect lag
 ep1 po200 ep2 ce11/1

XC Node-2#sh etherchannel summary
  Aggregator po200 100200
  Aggregator Type: Layer2
  Admin Key: 0200 - Oper Key 0200
     Link: ce18 (5009) sync: 1
     Link: ce17 (5010) sync: 1
```

Configuring Cross connect using Static lag interfaces

Configuration on R1 Node

`R1# configure terminal`	Enter configure mode
`R1(config)#interface sa100`	Creating Static lag interface
`R1(config-if)#exit`	Exit the interface level
`R1(config)#interface xe1/1`	Enter interface level
`R1(config-if)# static-channel-group 100`	Adding member port to the static lag interface
`R1(config-if)#exit`	Exit the interface level
`R1(config)#interface xe1/2`	Enter interface level
`R1(config-if)# static-channel-group 100`	Adding member port to the static lag interface
`R1(config-if)#exit`	Exit the interface level

Configuring Cross connect using static lag interfaces on XC_node1

`XC_node1# configure terminal`	Enter configure mode
`XC_node1(config)#interface sa100`	Creating static lag interface

XC_node1(config-if)#switchport	Configuring Switchport to the interface
XC_node1(config-if)#exit	Exit the interface level
XC_node1(config)#interface sa200	Creating static lag interface
XC_node1(config-if)#switchport	Configuring Switchport to the interface
XC_node1(config-if)#exit	Exit the interface level
XC_node1(config)#interface ce11/1	Enter interface level
XC_node1(config-if)# static-channel-group 100	Adding member port to the static lag interface
XC_node1(config-if)#exit	Exit the interface level
XC_node1(config)#interface ce11/2	Enter interface level
XC_node1(config-if)# static-channel-group 100	Adding member port to the static interface
XC_node1(config-if)#exit	Exit the interface level
XC_node1(config)#interface ce29	Enter interface level
XC_node1(config-if)# static-channel-group 200	Adding member port to the static lag interface
XC_node1(config-if)#exit	Exit the interface level
XC_node1(config)#interface ce30	Enter interface level
XC_node1(config-if)# static-channel-group 200	Adding member port to the static lag interface
XC_node1(config-if)#exit	Exit the interface level
XC_node1(config)#cross-connect static-lag	Create cross-connect by providing the name
XC_node1(config-XC)#ep1 sa100 ep2 sa200	Adding end-points ep1 and ep2 as lag interfaces
XC_node1(config-XC)#exit	Exit Cross-connect mode
XC_node1(config)#exit	Exit Configure terminal mode

Configuring Cross connect using static lag interfaces on XC_node2

XC_node2# configure terminal	Enter configure mode
XC_node2(config)#interface sa200	Creating static lag interface
XC_node2(config-if)#switchport	Configuring Switchport to the interface
XC_node2(config-if)#exit	Exit the interface level
XC_node2(config)#interface ce29	Enter interface level
XC_node2(config-if)# static-channel-group 200	Adding member port to the static lag interface
XC_node2(config-if)#exit	Exit the interface level
XC_node2(config)#interface ce30	Enter interface level
XC_node2(config-if)# static-channel-group 200	Adding member port to the static lag interface
XC_node2(config-if)#exit	Exit the interface level
XC_node2(config)#interface ce11/1	Enter interface level
XC_node2(config-if)#Switchport	Configure switchport to the interface
XC_node2(config-if)#exit	Exit the interface level

`XC_node2(config)#cross-connect static-lag`	Create cross-connect by providing the name
`XC_node2(config-XC)#ep1 po200 ep2 ce11/1`	Adding end-points ep1 and ep2 interfaces
`XC_node2(config-XC)#exit`	Exit Cross-connect mode
`XC_node2(config)#exit`	Exit Configure terminal mode

Validation

Cross-connect using Static Lag on XC_node1

```
XC_node1#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
static-lag         -      -      sa100            sa200            UP
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
```

Cross-connect using Static Lag on XC_node2

```
XC_node2#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
static-lag         -      -      sa200            ce11/1           UP
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
```

Disable the Cross-connect on XC node1

`Xc Node-1# configure terminal`	Enter configure mode
`Xc Node-1(config)#cross-connect lag`	Enter into cross-connect mode
`Xc Node-1(config-XC)#disable`	Disable the cross-connect
`Xc Node-1(config-XC)#exit`	Exit the cross-connect

Disable the cross-connect on XC node1

```
Xc Node-1#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
lag                -      -      po100            po200            DOWN
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 0
Down  : 1
```

© 2026 IP Infusion Inc. Proprietary

Enable the Cross-connect XC_node1

`Xc Node-1# configure terminal`	Enter configure mode
`Xc Node-1(config)#cross-connect lag`	Enter into cross-connect mode
`Xc Node-1(config-XC)#no disable`	Enable the cross-connect
`Xc Node-1(config-XC)#exit`	Exit the cross-connect

Cross-connect after enable on XC_node1

```
Xc Node-1#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
-----------------+------+------+----------------+----------------+------------
lag                -      -      po100            po200            UP
-----------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
```

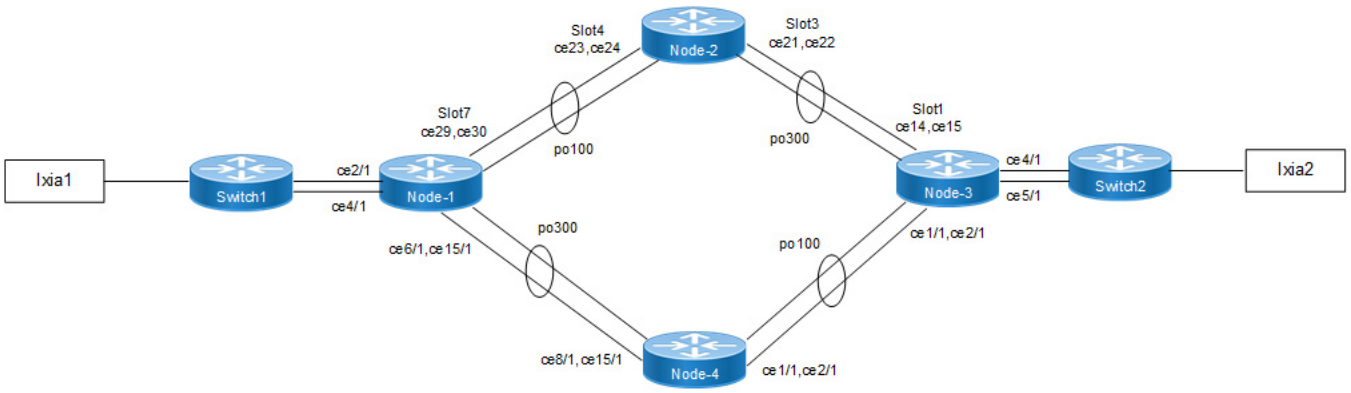
CFM over xConnect Configuration

This section contains a complete example of CFM over xConnect configuration.

The main objective of this feature to achieve L2 resiliency using CFM over xConnect where the traffic is switched to the next available link within xConnect when CFM detects errors or link failure on the monitored link in DC platforms.

Topology

Figure 54. CFM over xConnect Topology



Configuration

Node-1

`#configure terminal`	Enter configure mode
`(config)# hostname Node-1`	Configure the hostname.
`(config)#interface po100`	Create port channel interface.
`(config-if)#switchport`	Configure switchport on LAG port
`(config-if)#exit`	Exit the interface level
`(config)#interface ce29`	Enter interface level
`(config-if)#channel-group 100 mode active`	Add member port to the port channel interface.
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level

© 2026 IP Infusion Inc. Proprietary

`(config)#interface ce30`	Enter interface level
`(config-if)#channel-group 100 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface po300`	Create port channel interface
`(config-if)#switchport`	Configure switchport on LAG interface
`(config-if)#exit`	Exit the interface level
`(config)#interface ce6/1`	Enter interface level
`(config-if)#channel-group 300 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface ce15/1`	Enter interface level
`(config-if)#channel-group 300 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface ce2/1`	Enter interface level
`(config-if)#switchport`	Configure switchport
`(config)#interface ce4/1`	Enter interface level
`(config-if)#switchport`	Configure switchport
`(config-if)#exit`	Exit the interface level
`(config)#cross-connect xc1`	Create cross-connect by providing the name
`(config-XC)#ep1 po100 ep2 ce2/1`	Add end-points end-point1 and end-point2
`(config-XC)#backup ep1 po300`	Add backup end-point1
`(config-XC)#backup ep2 ce4/1`	Add backup end-point2
`(config-XC)#exit`	Exit XC mode
`(config)#ethernet cfm domain-type character-string domain-name mdnam1 level 0 mip-creation none`	Create CFM domain with type as character string with level 0 and set MIP creation criteria to none.
`(config-ether-cfm)#service ma-type string ma-name test1`	Create ma type as string
`(config-ether-cfm-ma)#link-level-ma`	Configure link-level-ma
`(config-ether-cfm-ma)#ethernet cfm mep down mpid 1 active true po100`	Create down MEP on po100
`(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`(config-ether-cfm-ma)#mep crosscheck mpid 2`	Configure crosscheck to remote MEP
`(config-ether-cfm-ma)#cc interval 10ms`	Enable cc interval for 10 millisecond
`(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit ethernet ma mode

© 2026 IP Infusion Inc. Proprietary

`(config-ether-cfm)#exit`	Exit ethernet CFM mode
`(config)#ethernet cfm domain-type character-string domain-name mdnam2 level 0 mip-creation none`	Create CFM domain with type as character string with level 0 and set MIP creation criteria to none.
`(config-ether-cfm)#service ma-type string ma-name test2`	Create MA type as string
`(config-ether-cfm-ma)#link-level-ma`	Configure link-level-ma
`(config-ether-cfm-ma)#ethernet cfm mep down mpid 3 active true po300`	Create down MEP on po300
`(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable CC multicast
`(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet CFM MA-MEP mode
`(config-ether-cfm-ma)#mep crosscheck mpid 4`	Configure crosscheck to remote MEP
`(config-ether-cfm-ma)#cc interval 10ms`	Enable CC interval for 10 millisecond
`(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit ethernet MA mode
`(config-ether-cfm)#exit`	Exit ethernet CFM mode

Node-2

`#configure terminal`	Enter configure mode
`(config)#hostname Node-2`	Configure the hostname
`(config)#interface po100`	Create port channel interface
`(config-if)#switchport`	Configure switchport on LAG port
`(config-if)#exit`	Exit the interface level
`(config)#interface ce23`	Enter interface level
`(config-if)#channel-group 100 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level.
`(config)#interface ce24`	Enter interface level
`(config-if)#channel-group 100 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface po300`	Create port channel interface
`(config-if)#switchport`	Configure switchport on LAG interface
`(config-if)#exit`	Exit the interface level
`(config)#interface ce21`	Enter interface level
`(config-if)#channel-group 300 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface ce22`	Enter interface level

© 2026 IP Infusion Inc. Proprietary

(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#cross-connect xc1	Create cross-connect by providing the name
(config-XC)#ep1 po100 ep2 po300	Add end-points end-point1 and end-point2

Node-3

#configure terminal	Enter configure mode
(config)#hostname Node-3	Configure the hostname
(config)#interface po300	Create port channel interface
(config-if)#switchport	Configure switchport on LAG port
(config-if)#exit	Exit the interface level
(config)#interface ce13	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level.
(config)#interface ce14	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface po100	Create port channel interface
(config-if)#switchport	Configure switchport on LAG interface
(config-if)#exit	Exit the interface level
(config)#interface ce1/1	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce2/1	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce4/1	Enter interface level
(config-if)#switchport	Configure switchport
(config)#interface ce5/1	Enter interface level
(config-if)#switchport	Configure switchport
(config-if)#exit	Exit the interface level

© 2026 IP Infusion Inc. Proprietary

(config)#cross-connect xc1	Create cross-connect by providing the name
(config-XC)#ep1 po300 ep2 ce4/1	Add end-points end-point1 and end-point2
(config-XC)#backup ep1 po100	Add backup end-point1
(config-XC)#backup ep2 ce5/1	Add backup end-point2
(config-XC)#exit	Exit XC mode
(config)#ethernet cfm domain-type character-string domain-name mdnam1 level 0 mip-creation none	Create cfm domain with type as character string with level 0 and set mip creation criteria to none.
(config-ether-cfm)#service ma-type string ma-name test1	Create ma type as string
(config-ether-cfm-ma)#link-level-ma	Configure link-level-ma
(config-ether-cfm-ma)#ethernet cfm mep down mpid 2 active true po100	Create down mep on po100
(config-ether-cfm-ma-mep)#cc multicast state enable	Enable cc multicast
(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit ethernet cfm ma-mep mode
(config-ether-cfm-ma)#mep crosscheck mpid 1	Configure crosscheck to remote MEP
(config-ether-cfm-ma)#cc interval 10ms	Enable cc interval for 10 millisecond
(config-ether-cfm-ma)#exit-ether-ma-mode	Exit ethernet ma mode
(config-ether-cfm)#exit	Exit ethernet CFM mode
(config)#ethernet cfm domain-type character-string domain-name mdnam2 level 0 mip-creation none	Create cfm domain with type as character string with level 0 and set mip creation criteria to none.
(config-ether-cfm)#service ma-type string ma-name test2	Create ma type as string
(config-ether-cfm-ma)#link-level-ma	Configure link-level-ma
(config-ether-cfm-ma)#ethernet cfm mep down mpid 4 active true po300	Create down mep on po300
(config-ether-cfm-ma-mep)#cc multicast state enable	Enable cc multicast
(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit ethernet cfm ma-mep mode
(config-ether-cfm-ma)#mep crosscheck mpid 3	Configure crosscheck to remote MEP
(config-ether-cfm-ma)#cc interval 10ms	Enable cc interval for 10 millisecond
(config-ether-cfm-ma)#exit-ether-ma-mode	Exit ethernet ma mode
(config-ether-cfm)#exit	Exit ethernet CFM mode

Node-4

#configure terminal	Enter configure mode
(config)#hostname Node-4	Configure the hostname
(config)#interface po100	Create port channel interface
(config-if)#switchport	Configure switchport on LAG port
(config-if)#exit	Exit the interface level
(config)#interface ce1/1	Enter interface level

(config-if)#channel-group 100 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level.
(config)#interface ce2/1	Enter interface level
(config-if)#channel-group 100 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface po300	Create port channel interface
(config-if)#switchport	Configure switchport on LAG interface
(config-if)#exit	Exit the interface level
(config)#interface ce8/1	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce15/1	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#cross-connect xc1	Create cross-connect by providing the name
(config-XC)#ep1 po300 ep2 po100	Add end-points end-point1 and end-point2

Validation

Node-1

```
#sh ethernet cfm maintenance-points local mep domain mdnam2 ma-name test2
MPID Dir Lvl VLAN CC-Stat  CC-Intvl MAC-Address    Def Port  MD Name
-------------------------------------------------------------------------------
3    Dn  0   0    Enable  10 ms    34ef.b689.e05a T   po300 mdnam2

#sh ethernet cfm maintenance-points local mep domain mdnam1 ma-name test1
MPID Dir Lvl VLAN CC-Stat  CC-Intvl MAC-Address    Def Port  MD Name
-------------------------------------------------------------------------------
1    Dn  0   0    Enable  10 ms    34ef.b689.e020 F   po100 mdnam1

#sh ethernet cfm maintenance-points remote mpid 3 domain mdnam2
 MEPID     RMEPID     LEVEL     VLAN      Rx CCM    RDI    PEER-MAC        TYPE
-------------------------------------------------------------------------------
 3         4          0         0         Yes       False  5cff.35b7.54b3  Configured

#sh ethernet cfm maintenance-points remote mpid 1 domain mdnam1
 MEPID     RMEPID     LEVEL     VLAN      Rx CCM    RDI    PEER-MAC        TYPE
-------------------------------------------------------------------------------
 1         2          0         0         Yes       False  5cff.35b7.54bb  Configured

#sh ethernet cfm errors domain mdnam1
Domain Name         Level     Vlan     MEPID     Defects
-------------------------------------------------------
```

```
mdnam1              0         0        1         .....

1. defRDICCM    2. defMACstatus  3. defRemoteCCM
4. defErrorCCM  5. defXconCCM

#sh ethernet cfm errors domain mdnam2
Domain Name         Level     Vlan     MEPID     Defects
-----------------------------------------------------------
mdnam2              0         0        3         .....

1. defRDICCM    2. defMACstatus  3. defRemoteCCM
4. defErrorCCM  5. defXconCCM
```

Node-3

```
#sh ethernet cfm maintenance-points local mep domain mdnam1 ma-name test1
MPID Dir Lvl VLAN CC-Stat  CC-Intvl MAC-Address    Def Port  MD Name
-------------------------------------------------------------------------------
2    Dn  0   0    Enable  10 ms    5cff.35b7.54bb F   po300 mdnam1

#sh ethernet cfm maintenance-points local mep domain mdnam2 ma-name test2
MPID Dir Lvl VLAN CC-Stat  CC-Intvl MAC-Address    Def Port  MD Name
-------------------------------------------------------------------------------
4    Dn  0   0    Enable  10 ms    5cff.35b7.54b3 F   po100 mdnam2

#sh ethernet cfm maintenance-points remote mpid 4 domain mdnam2
MEPID     RMEPID     LEVEL     VLAN      Rx CCM    RDI    PEER-MAC        TYPE
-------------------------------------------------------------------------------
4         3          0         0         Yes       False   34ef.b689.e05a Configured

#sh ethernet cfm maintenance-points remote mpid 2 domain mdnam1
MEPID     RMEPID     LEVEL     VLAN      Rx CCM    RDI    PEER-MAC        TYPE
-------------------------------------------------------------------------------
2         1          0         0         Yes       False   34ef.b689.e020 Configured

#sh ethernet cfm errors domain mdnam1
Domain Name         Level     Vlan     MEPID     Defects
-----------------------------------------------------------
mdnam1              0         0        2         .....

1. defRDICCM    2. defMACstatus  3. defRemoteCCM
4. defErrorCCM  5. defXconCCM

#sh ethernet cfm errors domain mdnam2
Domain Name         Level     Vlan     MEPID     Defects
-----------------------------------------------------------
mdnam2              0         0        4         .....

1. defRDICCM    2. defMACstatus  3. defRemoteCCM
4. defErrorCCM  5. defXconCCM
```

DATA CENTER BRIDGING CONFIGURATION

Data Centre Bridging (DCB) is a set of enhancements for Ethernet that enables both LANs and Storage Area Networks (SANs) to utilize a single integrated infrastructure within a data center. The Data Centre Bridging (DCB) technology enables the transportation of Fiber Channel, TCP/IP, and inter-process communication data across a unified Ethernet network. The features of DCB includes the following:

Data Center Bridging 824
- Overview 824
- Protocols Supported for DCBX 824
- DCBX Configuration for PFC via LLDP 825
- Priority-based Flow Control Configuration 826
- PFC with QoS Configuration 829
- PFC Deadlock Detection and Recovery 840
- PFC Frames and ECN Packets Monitoring 855

Data Centre Bridging Capability Exchange Configuration 870
- Overview 870
- DCBX Configuration for PFC via LLDP 870
- Validation 871

© 2026 IP Infusion Inc. Proprietary

Data Center Bridging

Overview

The traditional Ethernet networks are optimized for best-effort traffic, tolerating frame loss, retransmission, packet collisions, and out-of-order delivery. While sufficient for most general-purpose data traffic, this behavior is inadequate for storage traffic, such as Fibre Channel over Ethernet (FCoE), which demands lossless transport across the network.

To address this challenge, the IEEE 802.1 Data Center Bridging (DCB) standard introduced enhancements that enable lossless, low-latency transmission of sensitive data types over Ethernet, making it suitable for converged data center networks.

Data Centre Bridging (DCB) is a set of enhancements for Ethernet that enables both LANs and Storage Area Networks (SANs) to utilize a single integrated infrastructure within a data center. The DCB technology enables the transportation of Fiber Channel, TCP/IP, and inter-process communication data across a unified Ethernet network.

DCB is also essential for AI/ML workload transport. For AI/ML workloads, much of the traffic, such as inference, control, gradient synchronization, activation, and feature map data traffic types are extremely sensitive to latency, bandwidth, and packet loss. Any compromise in these areas directly translates to increased Job Completion Time (JCT), reduced GPU utilization, and training instability. These traffic types are best transported via RoCEv2 over dedicated, L3 routed GPU-to-GPU fabric with ECMP. PFC over Layer 3 enables lossless Ethernet transport across Layer 3 spine-leaf topology-based CLOS fabrics.

Feature Characteristics

Differentiated Traffic Handling

DCB allows multiple traffic types—such as storage, voice, and general data—to coexist and be managed differently on the same physical Ethernet link. This ensures that latency-sensitive or loss-intolerant traffic receives the appropriate level of service.

Lossless Ethernet with Flow Control

To minimize frame loss due to congestion, DCB includes mechanisms that control the flow of traffic at a granular level.

Limitations:

When a switchport (L2) is configured with Priority Flow Control (PFC), applying the no switchport command will also clear the PFC configuration. This behavior is part of the cleanup process triggered by the no switchport command.

Protocols Supported for DCBX

DCBX is primarily used to manage the following DCB protocols:

Priority-based Flow Control (PFC)

Priority-based Flow Control (PFC) (IEEE 802.1Qbb) is a link-level mechanism that enables the selective pausing of traffic based on priority levels (allows separate pause times for each of the eight priority classes) to prevent packet loss, offering granular control over how various traffic classes are managed. While traditionally deployed in Layer 2 (Ethernet) environments, extending PFC to Layer 3 interfaces brings these benefits to routed networks, enhancing

© 2026 IP Infusion Inc. Proprietary

traffic handling across complex topologies. By providing flow control per class, PFC helps minimize packet loss, particularly in congestion-sensitive applications such as storage, AI/ML, and high-performance computing.

PFC is a Layer 2 mechanism — it only works between directly connected neighbors on an Ethernet link. PFC alone can not operate end-to-end on a typical IP-routed (L3) network. However, when the packet is routed hop-by-hop at L3, the actual transmission on each link is L2. Therefore, PFC can still apply at each hop, controlling traffic for a given priority (e.g., for CoS 3 used by RoCEv2). The result is that lossless behavior is preserved link-by-link, provided all hops agree on which priorities to pause, even though the overall path is routed.

Use Cases:

Large-scale model training such as deep learning models like GPT or ResNet involves high-volume east-west traffic between GPUs/TPUs and storage.

High throughput, low congestion, and lossless transport such as RoCEv2 with PFC.

Benefits

Ensures lossless delivery for storage and real-time traffic.

Enhances network convergence by supporting multiple traffic types on one fabric.

Reduces infrastructure cost by eliminating the need for separate SAN and Ethernet networks.

Configuration

The DCB supports the following configurations:

- Priority-based Flow Control Configuration (page 826)
- DCBX Configuration for PFC via LLDP (page 870)
- PFC Configuration for Congestion on Device (page 829)

DCBX Configuration for PFC via LLDP

Configuring PFC parameter exchange typically involves enabling PFC mode, LLDP, activating DCBX, turning on PFC, and allowing the negotiation of control for each traffic priority (priorities 0–7).

Topology

The topology involves two switches SW1 and SW2 directly connected and enabled with DCBx and PFC.

Figure 55. PFC Configuration

Configuration

The following procedure configures PFC parameters and sent them in LLDP messages.

1. Create bridge and enable DCB and PFC on SW1 and SW2.

```
bridge 1 protocol ieee vlan-bridge
data-center-bridging enable bridge
priority-flow-control enable bridge1
```

2. Set interface cd1/1 on SW1 and SW2 to layer 2 and bind it to bridge group.

```
interface cd1/1
 switchport
 bridge-group 1
```

3. Enable LLDP and DCBx on SW1 and SW2. Set LLDP for transmit and receive mode on the interface. Set the TLVs enabled for transmission on the interface to send an IEEE 802.1 organizationally specific TLV set in the packet.

```
!
lldp-agent
 set lldp enable txrx
 lldp tlv ieee-8021-org-specific data-center-bridging select
 dcbx enable
!
```

4. Configure PFC on SW1 and SW2. Set the maximum number of priorities allowed for priority flow control on the interface. Enable PFC on priorities 0,1, and 2

```
!
priority-flow-control mode auto
priority-flow-control cap 3
priority-flow-control link-delay-allowance 65345
priority-flow-control enable priority 0 1 2
!
```

on SW2.

```
!
priority-flow-control mode auto
priority-flow-control cap 6
priority-flow-control link-delay-allowance 5678
priority-flow-control enable priority 5 6 7
!
```

Priority-based Flow Control Configuration

Priority-based Flow Control (PFC) (page 824) feature supports lossless Ethernet for selected traffic classes in congested network environments.

This chapter shows how to:

- Enable PFC on a bridge and interface
- Configure priorities and link delay allowance for PFC

> **Note:** On Tomahawk3 (TH3) platforms and LTSW platforms (Tomahawk4 (TH4) platforms, Tomahawk5 (TH5) platforms and Trident4 (TD4) platforms), performing add, delete, or update operations on PFC will cause a system-wide traffic interruption, resulting in configured session flaps.

Topology

Figure 56. PFC Enabled Bridge

Configuring a Bridge and Interface for PFC

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enables DCB on the bridge
`(config)#priority-flow-control enable bridge 1`	Enables PFC on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv ieee-8021-org-specific data-center-bridging select`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#priority-flow-control mode on`	Configure the advertise flag and start sending DCBX TLVs in LLDP messages

Configuring Priorities and Link Delay Allowance for PFC

`#configure terminal`	Enter Configure Mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enables DCB on the bridge
`(config)#priority-flow-control enable bridge 1`	Enables PFC on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#llldp tlv ieee-8021-org-specific data-center-bridging select`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#priority-flow-control mode on`	Configure the advertise flag and start sending DCBX TLVs in LLDP messages
`(config-if)#priority-flow-control cap 4`	Configure the maximum number of PFC priorities
`(config-if)#priority-flow-control enable priority 2 4 5`	Enable PFC on priorities 2, 4, and 5
`(config-if)#priority-flow-control link-delay-allowance 34567`	Configure the link delay allowance

© 2026 IP Infusion Inc. Proprietary

Validation

1. Verify the default data set.

```
#sh priority-flow-control statistics bridge 1
bridge : 1
interface pri pause sent     pause received
=========================================
eth1        0  00             00
eth1        1  00             00
eth1        2  00             00
eth1     3  00             00
eth1     4  00             00
eth1     5  00             00
eth1     6  00             00
eth1     7  00             00

#sh priority-flow-control details bridge 1

Admin Configuration
interface mode advertise willing  cap   link delay     priorities allowance
================================================================================

eth1       on    on       off      4      34567             2 4 5

Operational Configuration
-------------------------
interface state cap   link delay  priorities allowance
=============================================
eth1     on    4       34567          2 4 5
```

PFC with QoS Configuration

Overview

Priority-based Flow Control (PFC) provides a priority-level flow control mechanism that operates independently for each frame priority. Its primary purpose is to ensure zero packet loss (lossless behavior) during periods of congestion in Data Center Bridging (DCB) networks.

By default, Quality of Service (QoS) functions with a lossy behavior.By default, Class of Service (CoS) priorities are mapped one-to-one with queues. For instance, CoS 0 traffic is assigned to queue 0. If queue 0 is configured as lossless, Priority Flow Control (PFC) will be triggered for that queue.

The objective of this section is to enable PFC support alongside QoS, when congestion occurs on device or peer device node.

Limitation

PFC with QoS functionality is limited to known unicast and tagged traffic.

Benefits

Enable lossless behavior for specific traffic classes while maintaining traffic prioritization by integrating Priority Flow Control (PFC) with Quality of Service (QoS) profiles for designated priorities.

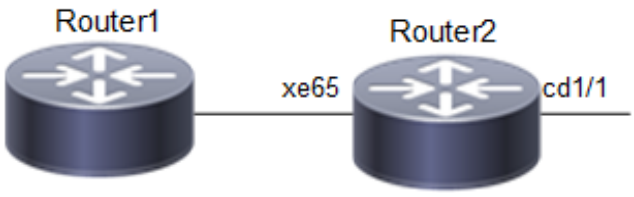
PFC Configuration for Congestion on Device

This section outlines the steps for configuring Priority Flow Control (PFC) and verifying its functionality when congestion occurs on the device (Device1). The setup uses VLAN 100 traffic with CoS priority 0 and ensures proper flow control by applying a shaper on the egress interface of Device1.

Topology

The topology consist of a client that act as Traffic Generator (TG) to send traffic to Device 1 on interface `xe65` Device1.

Figure 57. PFC for Traffic Congestion on Device



Configuration

Use this procedure is to apply PFC when congestion occurs on Device1.

1. Enable Data Center Bridging (DCB) and Priority-based Flow Control (PFC) on the bridge on Device 1.

```
!
bridge 1 protocol ieee vlan-bridge
!
vlan database
 vlan-reservation 4001-4094
```

```
!
 vlan 100 bridge 1 state enable
priority-flow-control enable bridge 1
```

2. Configure queue 0 as lossless with priority enabled in the default queuing policy.

```
!
policy-map type queuing default default-out-policy
 class type queuing default q0
  priority
  lossless
  exit
!
!
interface cd1/1
 shape rate 100 mbps burst 1000
!
```

3. Configure egress port `cd1/1` and ingress `xe65` Interfaces. Following sample commands, configures interface `cd1/1` with rate shaping at 100 Mbps and MTU as 9216 for jumbo frames and interface `xe65` with PFC priority as 0.

```
!
interface cd1/1
 description connected to Router1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 load-interval 30
 mtu 9216
 shape rate 100 mbps burst 1000
!
!
interface xe65
 description connected spirent
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 priority-flow-control mode on
 priority-flow-control enable priority 0
 load-interval 30
 mtu 9216
!
```

4. Configure the Traffic Generator (TG) to send traffic to VLAN-tagged traffic on VLAN 100. Set Class of Service (CoS) to 0. Ensure the TG is connected to interface `xe65` on Device1. Send bidirectional traffic or add a static MAC entry via CLI to ensure unicast forwarding.
5. Send traffic at a rate exceeding the 100 Mbps shaping rate on interface `cd1/1` to create congestion, causing queue 0 to fill up and trigger PFC for priority 0.

Validations

Execute the following command on Device1 to check PFC statistics:

```
#show priority-flow-control statistics bridge  1
bridge : 1
interface pri pause sent     pause received
=========================================
xe65      0  7819702        0
xe65      1  0              0
xe65      2  0              0
```

```
xe65      3  0              0
xe65      40          0
xe65      5  0              0
xe65      6  0              0
xe65      7  0              0
```

Here is the explanation of the "show command" output fields.

Table 38. PFC Parameters Description

Fields	Description
Pause Sent (7819702):	Indicates that the Device 1 has generated PFC frames for priority 0 to notify the peer device to pause traffic.
Pause Received (0):	Indicates that no PFC frames were received from the peer device.

```
#show interface counters rate mbps
+------------------+--------------+-------------+--------------+-------------+
|     Interface    |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+------------------+--------------+-------------+--------------+-------------+
   cd1/1               0.00          1             100.01         97668
   xe65                100.01        97669         1.04           2037
```

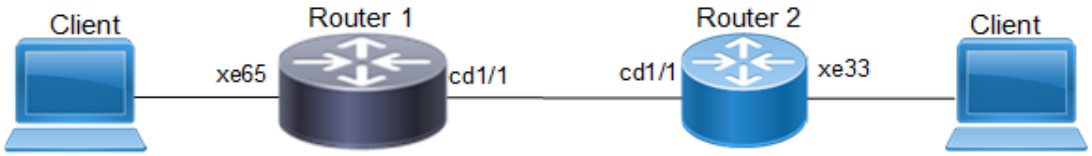
PFC Configuration for Congestion on Peer Device

This section outlines the steps for configuring PFC and verifying its functionality when congestion occurs on the peer device (Device2). The setup uses VLAN 100 traffic with CoS priority 0 and ensures proper flow control by applying a shaper on the egress interface of Device2.

Topology

The topology consist two clients that act as Traffic Generator (TG), Device 1 and 2. The TG client sends VLAN 100 traffic with CoS 0 to simulate congestion. The Device 1 egress interface `cd1/1` is connected to Device2 with PFC for priority 0. On Device2 egress interface `xe33`, the congestion is induced by applying a traffic shaper to the egress interface.

Figure 58. PFC for Congestion on Peer Device



On Router 1

1. Ensure the VLAN is configured and mapped to bridge group 1 and PFC is enabled on Device 1.

```
!
bridge 1 protocol ieee vlan-bridge
!
vlan database
 vlan-reservation 4001-4094
!
 vlan 100 bridge 1 state enable
priority-flow-control enable bridge 1
```

2. Ensure QoS is enabled. Following sample commands, configure queue 0 as lossless with priority enabled in the default queuing policy.

```
!
policy-map type queuing default default-out-policy
 class type queuing default q0
  priority
  lossless
  exit
!
```

3. Configure ingress and egress interfaces for PFC. Following sample commands, configures interface `cd1/1` and `xe65` with MTU as 9216 for jumbo frames, PFC priority as 0 and interface `xe65` with QoS policy as 0 on incoming traffic.

```
 !
interface cd1/1
 description connected to Router1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 priority-flow-control mode on
 priority-flow-control enable priority 0
 load-interval 30
 mtu 9216
!

!
interface xe65
 description connected spirent
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 priority-flow-control mode on
 priority-flow-control enable priority 0
 load-interval 30
 mtu 9216
!
```

On Router 2

1. Login to peer Device 2 and verify VLAN 100 is mapped to bridge group 1. Ensure PFC is enabled.

```
!
bridge 1 protocol ieee vlan-bridge
!
vlan database
 vlan-reservation 4001-4094
vlan 100 bridge 1 state enable
      priority-flow-control enable bridge 1
```

2. Ensure QoS Policy is enabled and configured to assign VLAN 100 traffic with rate shaping at 100 Mbps on egress interface.

```
!
qos enable
qos statistics
interface xe33
 shape rate 100 mbps burst 1000
!
```

3. Configure ingress `cd1/1` and egress `xe33` interfaces. Following sample commands, configures MTU as 9216 for frames, PFC priority as 0 on interface `cd1/1`. And shape rate at 100 Mbps for the incoming traffic from TG on interface `xe33`.

```
!
interface cd1/1
 description connected to Router2
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 priority-flow-control mode on
 priority-flow-control enable priority 0
 load-interval 30
 mtu 9216
!
!
interface xe33
 description connected to spirent
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 load-interval 30
 mtu 9216;
 shape rate 100 mbps burst 1000
!
```

4. Configure the TG to send VLAN 100 traffic with priority 0 to Device2. The TG sends traffic at shaping rate exceeding 100 Mbps to create congestion on the egress `xe33` interface. Ensure the TG is connected to interface `xe33` on Device2. Send bidirectional traffic or add a static MAC entry via CLI to ensure unicast forwarding.
5. Verify the PFC Statistics Device 1 and 2.

Validation

Execute the following command on Device1 to check PFC activity.

```
#show priority-flow-control statistics bridge  1
bridge : 1
interface pri pause sent     pause received
=========================================
xe65      0  190297         0
xe65      1  0              0
xe65      2  0              0
xe65      3  0              0
xe65 4  0              0
xe65      5  0              0
xe65      6  0              0
xe65      7  0              0
cd1/1     0  0              190436
cd1/1     1  0              0
cd1/1     2  0              0
cd1/1     3  0              0
cd1/1 4  0            0
cd1/1     5  0              0
cd1/1     6  0              0
cd1/1     7  0              0
```

Here is the explanation of the "show command" output fields.

Table 39. PFC Parameters Description

Fields	Description
Pause Sent (190297):	Device1 generates PFC pause frames on `xe65` for priority 0 to notify the traffic generator to pause traffic.
Pause Received (190436):	Device1 receives pause frames on `cd1/1` from Device2 for priority 0, indicating congestion on Device2.

```
#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
  cd1/1                0.64           1253          100.02         97671
  xe65                 100.02         97673         0.64           1253
#
```

Execute the following command on Device2 to check PFC activity.

```
#show priority-flow-control statistics bridge  1
show priority-flow-control statistics bridge  1
bridge : 1
interface pri pause sent     pause received
=========================================
cd1/1     0  323455         0
cd1/1     1  0              0
cd1/1     2  0              0
cd1/1     3  0              0
cd1/1     4  0        0
cd1/1     5  0              0
cd1/1     6  0              0
cd1/1     7  0              0
```

Here is the explanation of the "show command" output fields.

Table 40. PFC Parameters Description

Fields	Description
Pause Sent (323455)	Device2 generates PFC pause frames for priority 0 to notify Device1 to slow down traffic due to congestion on `xe33`.

```
#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
   cd1/1                100.01         97669         0.64           1253
   xe33                 0.00           1             100.01         97669
#
```

PFC Configuration for Ingress Service Policy Map

This section outlines the steps for configuring PFC for ingress service policy map.

Topology

Refer to the PFC Configuration for Congestion on Device (page 829) given in PFC Configuration for Congestion on Peer Device (page 831)

Configuration On Device1

1. Ensure the VLAN is configured and mapped to bridge group 1 and PFC is enabled on Device 1.

```
!
bridge 1 protocol ieee vlan-bridge
!
vlan database
 vlan-reservation 4001-4094
!
 vlan 100 bridge 1 state enable
priority-flow-control enable bridge 1
```

2. Ensure QoS is enabled. Configure QoS Polices, class and statistics. Following sample configures Class c1 matches UDP traffic on source port 4791, and policy p1 maps this traffic to queue 4.

```
!
qos enable
qos statistics
!
class-map type qos match-all c1
 match layer4 udp source-port 4791
!
policy-map type qos p1
  class type qos c1
 set queue 4
 exit
!
```

3. Configure queue 4 as lossless with priority enabled in the default queuing policy.

```
!
policy-map type queuing default default-out-policy
 class type queuing default q0
priority
lossless
exit
!
class type queuing default q4
 priority
 lossless
 exit
!
!
interface cd1/1
shape rate 100 mbps burst 1000
!l
interface xe65
service-policy type qos input p1
!
```

4. Configure egress cd1/1 and ingress xe65 Interfaces. Following sample commands, configures interface cd1/1 with rate shaping at 100 Mbps and MTU as 9216 for jumbo frames and interface xe65 with PFC priority as 4 and QoS policy as p1 on incoming traffic.

```
!
interface cd1/1
description connected to Router1
switchport
```

© 2026 IP Infusion Inc. Proprietary

```
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
load-interval 30
mtu 9216
shape rate 100 mbps burst 1000
!
interface xe65
description connected spirent
switchport

bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
priority-flow-control mode on
priority-flow-control enable priority 4
load-interval 30
mtu 9216
service-policy type qos input p1
!
```

5. Configure the Traffic Generator (TG) to send traffic to VLAN-tagged traffic on VLAN 100. Set Class of Service (CoS) to 4. Ensure the TG is connected to interface xe65.
6. Send traffic at a rate exceeding the 100 Mbps shaping rate on interface cd1/1 to create congestion, causing queue 4 to fill up and trigger PFC for priority 4.

Validation

Execute the following command to check PFC statistics

```
#show priority-flow-control statistics bridge  1
bridge : 1
interface           pri    pause sent   pause received
=====================================================
xe65      0  0              0
xe65      1  0              0
xe65      2  0              0
xe65      3  0              0
xe65      4  369553         0
xe65      5  0              0
xe65      6  0              0
xe65      7  0              0
cd1/1     0  0              0
cd1/1     1  0              0
cd1/1     2  0              0
cd1/1     3  0              0
cd1/1     4  0              369172
cd1/1     5  0              0
cd1/1     6  0              0
cd1/1     7  0              0


#show interface counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps   |    Tx mbps  |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 cd1/1               0.64          1253          100.01        97665
 xe65                100.01        97668         0.64          1253


#show policy-map  interface xe65

Interface xe65
```

```
Type QoS statistics status : enabled

Type QoS Ingress policy-map : p1

Class-map (qos): c1 (match all)
 match layer4 udp source-port 4791
 set queue 4
      matched      : 29714724 packets, 3803484672 bytes
      transmitted  : 29714724 packets, 3803484672 bytes


Type Queuing policy-map : default-out-policy

Class-map (queuing): q0
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q1
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q2
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q3
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q4
 priority
 lossless
      output              : 304 packets, 38912 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q5
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q6
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q7
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes

Wred/Tail Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
#
```

Configuration On Device 2

1. Login to peer Device 2 and verify VLAN 100 is mapped to bridge group 1. Ensure PFC is enabled.

```
!
bridge 1 protocol ieee vlan-bridge
!
vlan database
 vlan-reservation 4001-4094
vlan 100 bridge 1 state enable
      priority-flow-control enable bridge 1
```

2. Ensure QoS Policy is enabled and configured to assign VLAN 100 traffic with rate shaping at 100 Mbps on ingress interface.

```
!
qos enable
qos statistics
interface xe33
 shape rate 100 mbps burst 1000
!
```

3. Configure ingress `cd1/1` and egress `xe33` interfaces. Following sample commands, configures MTU as 9216 for frames, PFC priority as 4 on interface `cd1/1. And` shape rate at 100 Mbps for the incoming traffic from TG on interface `xe33`.

```
!
interface cd1/1
 description connected to Router2
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 priority-flow-control mode on
 priority-flow-control enable priority 4
 load-interval 30
 mtu 9216
!
!
interface xe33
 description connected to spirent
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 load-interval 30
 mtu 9216
 shape rate 100 mbps burst 1000
!
```

4. Send bidirectional traffic on the egress xe33 interface.
5. Verify the PFC Statistics on Device 2.

© 2026 IP Infusion Inc. Proprietary

Validation

Execute the following command on Device2 to check PFC activity.

```
#show priority-flow-control statistics bridge  1
bridge : 1
interface           pri    pause sent   pause received
=====================================================
cd1/1     0  0              0
cd1/1     1  0              0
cd1/1     2  0              0
cd1/1     3  0              0
cd1/1     4  519152         0
cd1/1     5  0              0
cd1/1     6  0              0
cd1/1     7  0              0

#show interface counters rate mbps
+------------------+--------------+-------------+--------------+-------------+
|     Interface    |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+------------------+--------------+-------------+--------------+-------------+
 cd1/1               100.01         97666         0.64           1253
 xe33                0.00           1             100.01         97671
#
```

PFC Deadlock Detection and Recovery

Overview

Priority-based Flow Control (PFC) helps manage traffic in networks by pausing specific flows during congestion. However, under certain conditions, a deadlock can occur when cyclical dependencies between flows create a loop of PFC pause events that prevents traffic from making forward progress indefinitely.

Priority Flow Control Pause Frames

PFC uses the standard pause frame mechanism with an additional 14 bytes of padding in the frame. This padding contains a 2-byte value for each of the eight priority classes, specifying the pause time in quanta for that class.

Example for priority pause frame:

```
Pause Frame:
  Control Opcode: 0x0101 (Priority Pause)
  Pause Time (8 priority classes):
    Class 0: 0x0000 (no pause)
    Class 1: 0x1234 (pause time in quanta)
    Class 2: 0x5678 (pause time in quanta)
    ...
    Class 7: 0x9ABC (pause time in quanta)
```

In the example above, the **`pause time in quanta`** field defines if the pause frame has XON or XOFF set for that class:

- **XON (X-On):** A control signal sent from the receiver to the transmitter to indicate readiness to accept data. For example, Class 0 represents a no-pause condition.
- **XOFF (X-Off)**: A control signal sent from the receiver to the transmitter indicating that it cannot accept additional data due to congestion. For example, Classes 1, 2, and 7 above specify a non-zero pause time (in quanta), signaling the transmitter to temporarily halt transmission.

Workflow of PFC Frames

- Transmission: The transmitter sends data to the receiver.
- XOFF: The receiver sends an XOFF signal to the transmitter, indicating that it is congested and cannot process more data.
- Pause: The transmitter pauses sending data to the receiver.
- XON: The receiver sends an XON signal to the transmitter, indicating that it is ready to receive data again.
- Resume: The transmitter resumes sending data to the receiver.

PFC deadlock:

A deadlock may occur when the receiver continuously sends XOFF signals for one or more classes, preventing the transmitter from sending any traffic. This feature is designed to detect such deadlocks and initiate recovery mechanisms.

To handle such critical situation, the OcNOS system provides PFC Deadlock Detection and Recovery capability. This chapter describes how to:

- Enable PFC deadlock detection and recovery on a specific interface
  - Configure Using Timer mode (page 842)
  - PFC State XON mode (page 845)

© 2026 IP Infusion Inc. Proprietary

- Configure the global PFC deadlock detection and recovery action to drop
  - Global Mode (page 846)

Feature Characteristics

Deadlock Detection

- The system monitors PFC queues for extended periods in the XOFF state.
- If a queue remains paused beyond a configurable threshold, a deadlock event is declared.
- An interrupt is raised to inform software of the detected deadlock.

Deadlock Recovery

Once a deadlock is detected, software moves the affected queue into an ignore PFC XOFF state, allowing traffic scheduling to resume.

Recovery can be configured on a per-interface basis and supports three modes:

- **Timer Mode:** Recovery ends automatically after a user-defined time interval. The system then clears the interrupt and restarts the detection timer. It is an automatic recovery method and recovery starts after a configurable detection-multiplier times time-granularity period. During that period, traffic will be allowed by default, but can also be dropped if the configuration priority-flow-control deadlock recovery-action drop is set. Recovery also ends automatically after a optionally configurable recovery-time period.

Note: Traffic will gradually decrease to zero if the `recovery-mode timer` is not configured; otherwise, it will continue indefinitely.

- **PFC-State-XON Mode:** Recovery ends when the interface receives a PFC XON frame, signaling that the pause condition is lifted.
- **Manual Mode:** Recovery requires explicit user action with CLI commands. This option is only valid if no automatic recovery mode is configured.

Limitation:

- Manual recovery mode is not supported in Trident3 (TD3) platforms or Tomahawk3 (TH3) platforms.
- Trident3 (TD3) platforms support deadlock recovery only in timer mode.
- Trident3 (TD3) platforms do not support 1ms time granularity.
- Tomahawk2 (TH2) platforms are not supported.

Benefits

- Prevents indefinite traffic stalls due to PFC loops.
- Provides flexible recovery options (automatic or manual).
- Improves network reliability in environments that rely on PFC.

Prerequisites

- The device should be enabled with PFC.

© 2026 IP Infusion Inc. Proprietary

Configuring PFC Deadlock Detection and Recovery

Topology

This topology illustrates Deadlock condition using single Switch1:

1. the **xe0** interfaces receives the regular traffic flow from a traffic source which is PFC enabled.
2. the same priority 1 regular unicast traffic is transmitted to the **xe1** interface which is also PFC enabled.
3. the traffic source sends pause frames that have XOFF on priority 1 to the **xe0** interface.
4. the regular traffic received on **xe0** interface is slowed down until no more packets arrive from the regular traffic flow.

Figure 59. PFC Deadlock Detection and Recovery

Configure Using Timer mode

The following configurations, enables PFC deadlock recovery on every priority interfaces. Optionally, the detection multiplier, time granularity and recovery time parameters may be set, otherwise the defaults (respectively 10, 10, 100) will be used.

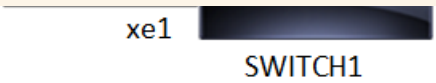
Execute the following steps to configure PFC on both interfaces.

1. Create a bridge 1 as an IEEE VLAN-enabled bridge. Enable DCB and PFC on the bridge.

```
(config)#bridge 1 protocol ieee vlan-bridge
(config)#data-center-bridging enable bridge 1
(config)#priority-flow-control enable bridge 1
```

2. Enable PFC priorities 0 and 1 on both the interfaces **xe0** and **xe1**.

```
(config)#interface xe0
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan all
(config-if)#priority-flow-control mode on
(config-if)#priority-flow-control enable priority 0 1
(config-if)#load-interval 30

(config)interface xe1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan all
(config-if)#priority-flow-control mode on
(config-if)#priority-flow-control enable priority 0 1
(config-if)#load-interval 30
```



3. Configure the priority flow control deadlock recovery mode timer on **xe0** interface.

```
(config)#interface xe0
(config-if)#priority-flow-control deadlock recovery-mode timer
(config-if)#commit
(config-if)#
```

4. Configure the PFC deadlock detection happens with non-default detection-multiplier and time-granularity parameters

```
(config)#interface xe0
(config-if)#priority-flow-control deadlock recovery-mode timer detection-multiplier 10 time-
granularity 10 recovery-time 1000
```

Validation

Check the PFC priority 1 traffic received and send on `xe0` and `xe1` interfaces.

```
OcNOS#show int count rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe0                  0.00           0             1176.62        147078
 xe1                  1176.62        147077        0.00           0
OcNOS#
```

Check the queue-level statistics on each interface to monitor transmitted traffic, drops, and queue.

```
OcNOS#clear interface counters
OcNOS#show interface counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
 * indicates monitor is active
+-----------------+--------------------+------------------+-----------------+-------------------+-
---------------+-------------------+
| Interface | Queue/Class-map | Q-Size | Tx pkts | Tx bytes | Dropped pkts | Dropped bytes |
+-----------------+--------------------+------------------+-----------------+-------------------+-
---------------+-------------------+
xe0 q1 (E) 0 427127 427127000 0 0
```

After 30 seconds, check link throughput, should be like this:

```
OcNOS#show int count rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe0                  0.00           0             1176.62        147077
 xe1                  1176.62        147077        0.00           0
OcNOS#
```

Check the traffic gradually stops after starting the XOFF P1 traffic to simulate the deadlock.

```
OcNOS#show int count rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe0                  0.66           162           540.53         67566
 xe1                  1176.62        147077        0.11           211
```

Check the TX traffic on **`xe0`** is completely stopped after 30 seconds.

```
OcNOS#show int count rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe0                  1.23           300           0.00           0
 xe1                  1176.62        147077        0.20           397
```

Check the traffic flow is restored after 30 seconds even though the XOFF packets exists.

```
OcNOS#show int count rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe0                  1.23           300           1176.68        147086
 xe1                  1176.59        147074        0.00           0
```

Check the PFC deadlock is detected:

```
OcNOS#show priority-flow-control deadlock-status interface xe0

Deadlock Detection and Recovery Configuration
-----------------------------------------------------------------------
interface            recovery     detection     detection     recovery
                     mode         multiplier    granularity   time
=======================================================================
xe0                  Timer        10            10            1500
-----------------------------------------------------------------------------------------------------------
----

Deadlock Detection and Recovery Status
-----------------------------------------------------------------------------------------------------------
----
interface           pri    state          detection    last detection             last recovery
                                          count        timestamp                  timestamp
===========================================================================================================
====
xe0                   0    no deadlock            0    -                          -
xe0                   1       deadlock           35    2025-05-29 19:03:34.611    -
xe0                   2    no deadlock            0    -                          -
xe0                   3    no deadlock            0    -                          -
xe0                   4    no deadlock            0    -                          -
xe0                   5    no deadlock            0    -                          -
xe0                   6    no deadlock            0    -                          -
xe0                   7    no deadlock            0    -                          -

OcNOS#show priority-flow-control deadlock-status

Deadlock Detection and Recovery Configuration
-----------------------------------------------------------------------
interface            recovery     detection     detection     recovery
                     mode         multiplier    granularity   time
=======================================================================
xe0                  Timer        10            10            1500

-----------------------------------------------------------------------------------------------------------
----

Deadlock Detection and Recovery Status
-----------------------------------------------------------------------------------------------------------
----
interface           pri    state          detection    last detection             last recovery
                                          count        timestamp                  timestamp
===========================================================================================================
====
xe0                   1       deadlock           39    2025-05-29 19:03:49.481
```

Check the deadlock detection count:

```
OcNOS#show priority-flow-control deadlock-status interface xe0

Deadlock Detection and Recovery Configuration
-----------------------------------------------------------------------
interface            recovery     detection     detection     recovery
                     mode         multiplier    granularity   time
=======================================================================
xe0                  Timer        1             1             1500

-----------------------------------------------------------------------------------------------------------
----

Deadlock Detection and Recovery Status
-----------------------------------------------------------------------------------------------------------
----
interface           pri    state          detection    last detection             last recovery
                                          count        timestamp                  timestamp
===========================================================================================================
====
```

```
xe0                   0    no deadlock            0    -                           -
xe0                   1    no deadlock          163    2025-05-29 19:55:16.842    2025-05-29
19:55:18.344
xe0                   2    no deadlock            0    -                           -
xe0                   3    no deadlock            0    -                           -
xe0                   4    no deadlock            0    -                           -
xe0                   5    no deadlock            0    -                           -
xe0                   6    no deadlock            0    -                           -
xe0                   7    no deadlock            0    -                           -
```

Change recovery-time to 1000 and check the PFC deadlock.

```
OcNOS#show priority-flow-control deadlock-status interface xe0

Deadlock Detection and Recovery Configuration
------------------------------------------------------------------------
interface            recovery     detection     detection     recovery
                     mode         multiplier    granularity   time
========================================================================
xe0                  Timer        10            10            1000

------------------------------------------------------------------------------------------------------------
----

Deadlock Detection and Recovery Status
------------------------------------------------------------------------------------------------------------
----
interface           pri    state          detection    last detection             last recovery
                                          count        timestamp                  timestamp
============================================================================================================
====
xe0                   0    no deadlock            0    -                          -
xe0                   1       deadlock            9    2025-05-29 20:04:23.251    -
xe0                   2    no deadlock            0    -                          -
xe0                   3    no deadlock            0    -                          -
xe0                   4    no deadlock            0    -                          -
xe0                   5    no deadlock            0    -                          -
xe0                   6    no deadlock            0    -                          -
xe0                   7    no deadlock            0    -                          -
```

PFC State XON mode

Execute the following steps to configure PFC on both interfaces.

1. Create a bridge 1 as an IEEE VLAN-enabled bridge. Enable DCB on the bridge.
   ```
   (config)#bridge 1 protocol ieee vlan-bridge
   (config)#data-center-bridging enable bridge 1
   ```
2. Enables PFC on the bridge. Configure the advertise flag and start sending DCBX TLVs in LLDP messages.
   ```
   (config)#priority-flow-control enable bridge 1
   (config-if)#priority-flow-control mode on
   ```
3. Enable PFC on priorities 0 and 1.
   ```
   (config-if)#priority-flow-control enable priority 0 1
   ```
4. Enable automatic priority flow control deadlock recovery mode `pfc-state-xon` with custom detection time.
   ```
   (config-if)#priority-flow-control deadlock recovery-mode pfc-state-xon detection-multiplier 10 time-
   granularity 10
   ```

Validation

Change the recovery-mode to `pfc-state-xon` and check PFC deadlocks

```
OcNOS#show int counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
```

```
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe0                  1.23           300           1176.62        147078
 xe1                  1176.62        147077        0.00           0

OcNOS##show priority-flow-control deadlock-status

Deadlock Detection and Recovery Configuration
-----------------------------------------------------------------------
interface            recovery     detection     detection     recovery
                     mode         multiplier    granularity   time
=======================================================================
xe0                  XON          10            10            -

-----------------------------------------------------------------------------------------------------------
----

Deadlock Detection and Recovery Status
-----------------------------------------------------------------------------------------------------------
----
interface           pri    state          detection    last detection             last recovery
                                          count        timestamp                  timestamp
===========================================================================================================
====
xe0                  1       deadlock            1    2025-05-29 20:12:58.089    -
```

Global Mode

When any interface enters deadlock recovery mode, instead of allowing the deadlocked traffic to pass, traffic will be dropped if this command is set globally.

```
(config)#priority-flow-control deadlock recovery-action drop
```

Validation

Change the global action command to drop and check the effect on traffic during the recovery process:

```
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe0                  1.23           300           0.00           0
 xe1                  1176.62        147077        0.00           0
OcNOS#
```

Manual Recovery

Once a deadlock is detected and no manual recovery mode is configured in the interface, it is possible to recover from the deadlock by manually entering and exiting recovery mode on supported boards with the below commands:

1. Start manual deadlock recovery on interface eth1.
   ```
   #priority-flow-control xe0 deadlock manual-recovery start
   ```
2. Stop manual deadlock recovery on interface eth1
   ```
   #priority-flow-control xe1 deadlock manual-recovery stop
   ```

Validation

Start sending XOFF on P1 manual recovery mode and check if traffic starts to flow:

```
OcNOS#priority-flow-control xe0 deadlock-manual-recovery start
OcNOS#show int count rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
```

```
 xe0                  1.21           295           311.12         38890
 xe1                  1176.60        147075        0.15           287
OcNOS#show int count rate mbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+--------------------+--------------+-------------+--------------+-------------+
 xe0                  1.21           295           311.12         38890
 xe1                  1176.60        147075        0.15           287
OcNOS#show int count rate mbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+--------------------+--------------+-------------+--------------+-------------+
 xe0                  1.21           296           595.44         74430
 xe1                  1176.60        147074        0.10           191
```

Stop manual recovery mode and check if traffic stops.

```
OcNOS#priority-flow-control xe0 deadlock-manual-recovery stop
OcNOS#show int count rate mbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+--------------------+--------------+-------------+--------------+-------------+
 xe0                  1.22           297           823.27         102909
 xe1                  1176.61        147076        0.06           115
OcNOS#show int count rate mbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+--------------------+--------------+-------------+--------------+-------------+
 xe0                  1.22           297           823.27         102909
 xe1                  1176.61        147076        0.06           115
OcNOS#show int count rate mbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+--------------------+--------------+-------------+--------------+-------------+
 xe0                  1.21           296           710.29         88786
 xe1                  1176.61        147075        0.08           147
OcNOS#show int count rate mbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+--------------------+--------------+-------------+--------------+-------------+
 xe0                  1.21           296           710.29         88786
 xe1                  1176.61        147075        0.08           147
OcNOS#show int count rate mbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+--------------------+--------------+-------------+--------------+-------------+
 xe0                  1.22           297           537.98         67248
 xe1                  1176.61        147076        0.11           208
OcNOS#
```

Clear PFC Deadlock

Following are the two commands to clear the deadlock.

1. Clearing deadlock status for a specific interface
   ```
   #clear priority-flow-control deadlock-status xe1
   ```
2. Clearing deadlock status for all interfaces
   ```
   #clear priority-flow-control deadlock-status
   ```

Show Running Configuration

```
OcNOS#show running-config
!
! Software version: UFI_S9110-32X-OcNOS-DC-NA-7.0.0.999- 08/21/2025 14:08:11
!
```

```
! Last configuration change at 05:02:36 UTC Sat Aug 16 2025 by root
!
!
service password-encryption
!
logging console 0
logging monitor 7
logging level nsm 7
logging level hsl 7
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
!
qos enable
!
bridge 1 protocol rstp vlan-bridge
tfo Disable
errdisable cause stp-bpdu-guard
data-center-bridging enable bridge 1
snmp-server enable snmp vrf management
snmp-server view all .1 included vrf management
snmp-server community test group network-operator vrf management
snmp-server host 192.168.5.18 traps version 2c test vrf management host-vrf management
feature dns relay
ip dns relay
ipv6 dns relay
!
ip access-list 1
 10 permit ahp any any
!
policy-map type queuing default default-out-policy
 class type queuing default q0
  priority
  lossless
  exit
 class type queuing default q1
  priority
  lossless
  exit
 class type queuing default q2
  priority
  lossless
  exit
 class type queuing default q3
  priority
  lossless
  exit
 class type queuing default q4
  priority
  lossless
  exit
 class type queuing default q5
  priority
  lossless
  exit
 class type queuing default q7
  priority
  lossless
  exit
!
vlan database
 vlan-reservation 4029-4094
 vlan 10 bridge 1
!
ip vrf management
!
interface ce0
!
interface ce6
```

```
!
interface ce7
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 priority-flow-control mode on
 priority-flow-control enable priority 0 1
 load-interval 30
!
interface ce8
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 priority-flow-control mode on
 priority-flow-control enable priority 0 1
 load-interval 30
!
interface ce9
!
interface ce31
!
interface eth0
 ip vrf forwarding management
 ip address dhcp
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface lo.management
 ip vrf forwarding management
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface xe32
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 priority-flow-control mode on
 priority-flow-control enable priority 0 1
 load-interval 30
!
 exit
!
line console 0
 exec-timeout 35791
line vty 0 3
 exec-timeout 35791
!
!
end
```

CLI Commands

The feature introduces the following configuration commands.

clear priority-flow-control deadlock-status

Use this command to clear the PFC deadlock details for a specified interface or for all interfaces.

Command Syntax

```
clear priority-flow-control deadlock-status [ IFNAME ]
```

Parameters

IFNAME
Name of the input or output interface.

Default

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 7.0.0.

Example

```
#clear priority-flow-control deadlock-status interface eth1
```

priority-flow-control deadlock manual-recovery

Use this command to start/stop manually the PFC deadlock recovery on the specified interface.

Command Syntax

```
priority-flow-control <NAME> deadlock manual-recovery ( start | stop )
```

Parameters

IFNAME
Name of the input or output interface.

Default

Nones

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 7.0.0.

Example

```
#priority-flow-control eth1 deadlock manual-recovery start
#priority-flow-control eth1 deadlock manual-recovery stop
```

priority-flow-control deadlock recovery-action drop

Use this command to globally drop deadlocked traffic on Priority-based Flow Control (PFC) deadlock recovery.

© 2026 IP Infusion Inc. Proprietary

Use the `no` form of this command to allow deadlocked traffic when a PFC deadlock recovery occurs.

Command Syntax

```
priority-flow-control deadlock recovery-action drop
no priority-flow-control deadlock recovery-action drop
```

Parameters

None

Default

By default, PFC deadlocked traffic during a recovery is allowed.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 7.0.0.

Example

```
#configure terminal (config)
#priority-flow-control deadlock recovery-action drop
```

priority-flow-control deadlock recovery-mode timer

Use this command to enable Priority-based Flow Control (PFC) deadlock and recovery on all priorities of an interface, using a timer to end the recovery phase.

Use the `no` form of this command to disable PFC deadlock detection and recovery on an interface.

Command Syntax

```
priority-flow-control deadlock recovery-mode timer
[ detection-multiplier <1-1599> time-granularity <1|10|100> ]
[ recovery-time <100-1599> ]

no priority-flow-control deadlock recovery-mode
```

Parameters

detection-multiplier
Specify the detection multiplier duration in micro seconds.

time-granularity
Specify the time granularity duration in micro seconds.

recovery-time
Specify the Recovery time duration in micro seconds.

Default

By default, detection multiplier is 10, time granularity is 10ms and recovery time is 100ms.

PFC deadlock detection is disabled by default.

© 2026 IP Infusion Inc. Proprietary

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 7.0.0.

Example

```
(config)#interface xe1
(config-if)#priority-flow-control deadlock recovery-mode
timer detection-multiplier 100 time-granularity 100
recovery-time 1000

OcNOS(config)#interface xe0
OcNOS(config-if)#no priority-flow-control deadlock recovery-mode
```

priority-flow-control deadlock recovery-mode pfc-state-xon

Use this command to enable Priority-based Flow Control (PFC) deadlock and recovery on all priorities of an interface, using XON packet reception end the recovery phase.m

Use the `no` form of this command to disable PFC deadlock detection and recovery on an interface.

Command Syntax

```
priority-flow-control deadlock recovery-mode pfc-state-xon
[ detection-multiplier <1-1599> time-granularity <1|10|100> ]


no priority-flow-control deadlock recovery-mode
```

Parameters

detection-multiplier
: Specify the detection multiplier duration in micro seconds.

time-granularity
: Specify the time granularity duration in micro seconds.

Default

By default, detection multiplier is 10, and time granularity is 10ms.

PFC deadlock detection is disabled by default.

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 7.0.0.

Example

#configure terminal (config)

```
#configure terminal (config)
(config)#interface xe1
```

```
(config-if)#priority-flow-control deadlock recovery-mode pfc-state-xon
detection-multiplier 100 time-granularity 100
```

show priority-flow-control deadlock-status

Use this command to display the PFC deadlock details for a specified interface or for all interfaces.

Command Syntax

```
show priority-flow-control deadlock-status [ IFNAME ]
```

Parameters

IFNAME
Name of the input or output interface.

Default

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 7.0.0.

Example

```
#show priority-flow-control deadlock-status

Deadlock Detection and Recovery Configuration
------------------------------------------------------------------------
interface recovery detection detection recovery
mode multiplier granularity time
========================================================================
xe0 Timer 10 10 1500

------------------------------------------------------------------------------------------------------------

Deadlock Detection and Recovery Status
------------------------------------------------------------------------------------------------------------
----
interface pri state detection last detection last recovery
count timestamp timestamp
============================================================================================================
xe0 1 deadlock 39 2025-05-29 19:03:49.481 -
```

Implementation Examples

Use case for PFC monitoring:

In a cloud data center, RoCEv2 traffic (RDMA over Converged Ethernet) runs across the fabric. Lossless transmission is critical, and PFC is used to pause specific priorities when buffers approach congestion. Use PFC monitoring to detect:

- If too many pause frames are being sent (could indicate congestion hotspots).
- If pause frames are stuck (deadlock scenarios).

Use Case for ECN monitoring in Leaf-Spine Fabric:

A hyperscale data center enables ECN marking on switches to signal congestion without dropping packets. End-host TCP stacks respond by reducing transmission rates. For ECN monitoring:

- Enable ECN on switch interfaces.
- Monitor ECN-marked packets per flow.

Glossary

The following table provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
PFC	Priority-based Flow Control. A mechanism to pause specific flows during congestion using pause frames based on defined times for each priority class.
XOFF	A control signal sent from the receiver to the transmitter, indicating that the receiver is congested and cannot accept additional data. It is signaled by a non-zero pause time in the PFC frame.
XON	A control signal sent from the receiver to the transmitter, indicating readiness to accept data (a no-pause condition).
Timer Mode	An automatic recovery mode where the system clears the deadlock after a user-defined time interval (recovery-time). This is the only mode supported by Trident3 (TR3) platforms.
PFC-State-XON Mode	An automatic recovery mode where recovery ends when the interface receives a PFC XON frame, signaling the pause condition is lifted.
Manual Mode	A recovery option that requires explicit user action via CLI commands to start and stop the recovery phase.

© 2026 IP Infusion Inc. Proprietary

PFC Frames and ECN Packets Monitoring

Overview

OcNOS supports Protocols Supported for DCBX to pause frames using defined times for each of the eight priority classes. This prevents congestion and improves transmission performance by letting the transmitter adjust its data flow according to the receiver's processing capacity.

Also supports Explicit Congestion Notification (ECN), which provides end-to-end congestion signaling between ECN-enabled senders and receivers in TCP/IP networks. Instead of dropping packets, ECN marks them to indicate congestion, prompting the sender to temporarily reduce its transmission rate until congestion clears. This reduces both packet loss and delay. ECN is defined in RFC 3168.

Feature Characteristics

This functionality enables:

- ECN marked packet monitoring on an interface
- PFC paused frames monitoring on an interface
- Monitored interfaces generate logs, NETCONF notifications, and SNMP traps whenever monitored packets are detected, including PFC frames and ECN-marked packets.

Limitation:

This functionality is applicable to the chips Tomahawk2 (TH2) platforms , Tomahawk3 (TH3) platforms ,Tomahawk4 (TH4) platforms Tomahawk5 (TH5) platforms, , Trident3 (TD3) platforms and Trident4 (TD4) platforms.

Benefits

Improved Congestion Management – Prevents buffer overflows and packet drops by dynamically controlling traffic flow.

Per-Priority Traffic Control – Ensures that critical traffic classes (e.g., storage or real-time applications) are not impacted by congestion in other classes.

Reduced Packet Loss – Uses packet marking instead of dropping to signal congestion, minimizing retransmissions.

Higher Throughput Efficiency – Link utilization can be optimized via adjusting transmission rates based on real-time network conditions.

Prerequisites

PFC monitoring data requires a working PFC configuration and active PFC traffic. Similarly, ECN monitoring data requires a working ECN configuration and active ECN traffic.

Configuring PFC Frames and ECN Packets Monitoring

The configuration procedure outlines the steps required to enable ECN and PFC Support for Lossless TCP/IP Transport on the L2 networks, ensuring the network can handle high-priority, lossless AI/ML traffic.

The section includes the following configuration and validations:

Configuration - ECN Marking and PFC Pausing (page 856)

- ECN Configuration (Bridging and ECN Marking) (page 857)
- Configuring PFC Frames and ECN Packets Monitoring (page 855)

© 2026 IP Infusion Inc. Proprietary

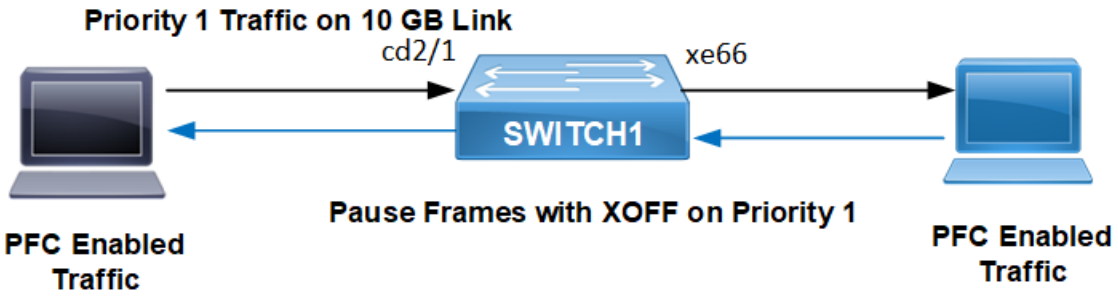
- PFC Configuration (Bridging and PFC Pausing) (page 857)
- Configuring PFC Frames and ECN Packets Monitoring (page 855)

Topology

The topology uses a Switch1 with an ingress interface **cd2/1** (connected to a node which generates traffic) and an egress interface **xe66** (connected to destination node which receives the traffic). Congestion is induced on the egress interface **xe66** using shapers within QoS policy maps.

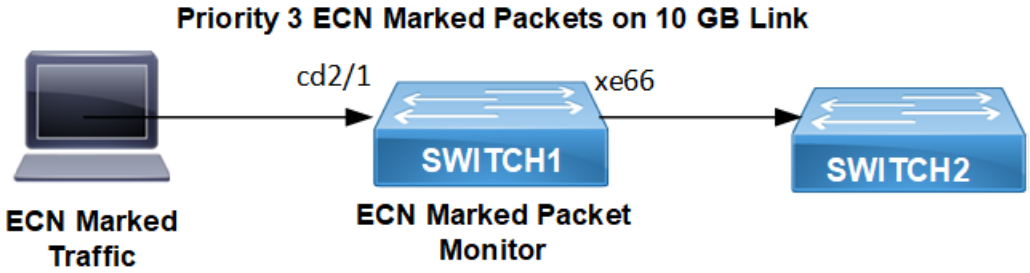
The following topology shows PFC pause frame monitoring on the ingress and egress interfaces of Switch 1.

Figure 60. PFC Enabled Bridge



The following topology shows ECN Marked packets monitoring on the ingress and egress interfaces of Switch 1.

Figure 61. ECN Enabled Bridge



Configuration - ECN Marking and PFC Pausing

The following steps configure monitoring of PFC and ECN packets transmitted and received on an interface when monitoring is enabled.

1. Configure global settings - QoS, VLAN/Bridge, ingress port and egress port on Switch 1.

```
(config)#qos enable

(config)#vlan database
(config-vlan)#vlan-reservation 4001-4094
(config-vlan)#vlan 2 bridge 1 state enable

(config)#bridge 1 protocol rstp vlan-bridge
```

```
(config)#interface cd2/1
(config-if)#description Switch1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan add 2
(config-if)#load-interval 30
(config-if)#mtu 9216
```

ECN Configuration (Bridging and ECN Marking)

2. Configure ECN policy.

```
(config)#policy-map type queuing default ECN
(config-cmap-que)#class type queuing default q0
(config-cmap-que)#priority
(config-cmap-que)#lossless
(config-cmap-que)#exit
(config)#class type queuing default q1
(config-cmap-que)#priority
(config-cmap-que)#lossless
(config-cmap-que)#exit
(config)#class type queuing default q2
(config-cmap-que)#priority
(config-cmap-que)#lossless
(config-cmap-que)#exit
(config)#class type queuing default q3
(config-cmap-que)#shape 1 gbps
(config-cmap-que)#priority
(config-cmap-que)#random-detect green min-threshold 40 max-threshold 50 yellow min-threshold 70 max-
threshold 80 red min-threshold 100 max-threshold 110 packets ecn
(config-cmap-que)#exit
(config)#class type queuing default q4
(config-cmap-que)#priority
(config-cmap-que)#lossless
(config-cmap-que)#exit
(config)#class type queuing default q5
(config-cmap-que)#priority
(config-cmap-que)#lossless
(config-cmap-que)#exit
```

3. Apply policy and monitor. Ensure PFC is not applied when only ECN is required.

```
OcNOS(config)#interface xe66
OcNOS(config-if)#description Egress-interface
OcNOS(config-if)#switchport
OcNOS(config-if)#bridge-group 1
OcNOS(config-if)#switchport mode trunk
OcNOS(config-if)#switchport trunk allowed vlan all
OcNOS(config-if)#load-interval 30
OcNOS(config-if)#mtu 9216
OcNOS(config-if)#service-policy type queuing output ECN
OcNOS(config-if)#monitor ecn
```

PFC Configuration (Bridging and PFC Pausing)

Setup to enable PFC pausing instead of ECN marking on congestion.

4. Configure ingress port `cd2/1` and egress port **`xe66`**.

```
(config)#interface cd2/1
(config-if)#description Switch1
(config-if)# switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan add 2
(config-if)#load-interval 30
```

```
(config-if)#mtu 9216

(config)#interface vlan1.2
(config-if)# mtu 9216

(config)#interface xe66
(config-if)#description Connected-Destination Host
(config-if)#load-interval 30
(config-if)#mtu 9216
(config-if)#service-policy type queuing output ECN
(config-if)#monitor ecn
```

5. Configure PFC policy.

```
(config)#policy-map type queuing default PFC
(config-cmap-que)#class type queuing default q0
(config-cmap-que)#priority
(config-cmap-que)#lossless
(config-cmap-que)#exit
(config)#class type queuing default q1
(config-cmap-que)#priority
(config-cmap-que)#lossless
(config-cmap-que)#exit
(config)#class type queuing default q2
(config-cmap-que)#priority
(config-cmap-que)#lossless
(config-cmap-que)#exit
(config)#class type queuing default q3
(config-cmap-que)#shape 1 gbps
(config-cmap-que)#priority

(config-cmap-que)#exit
(config)#class type queuing default q4
(config-cmap-que)#priority
 (config-cmap-que)#lossless
 (config-cmap-que)#exit
 (config)#class type queuing default q5
 (config-cmap-que)#priority
 (config-cmap-que)#lossless
 (config-cmap-que)#exit
```

6. Enable PFC policy.

```
(config)#interface cd2/1
(config-if)#description Ingress-port
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan all
(config-if)#priority-flow-control mode on
(config-if)#priority-flow-control enable priority 0 1 2 3 4
(config-if)#load-interval 30
(config-if)#mtu 9216
(config-if)#monitor pfc

(config-if)#interface xe66
(config-if)#description Egress-port
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan all
(config-if)#priority-flow-control mode on
(config-if)#priority-flow-control enable priority 0 1 2 3 4
(config-if)#load-interval 30
(config-if)#mtu 9216
(config-if)#service-policy type queuing output PFC
```

© 2026 IP Infusion Inc. Proprietary

Sample Show Running Configuration on Switch 1

For PFC

```
!
service password-encryption
!
logging console 5
logging monitor 5
logging level all 7
!
!
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
!
qos enable
!
hostname DUT1
port cd2 breakout 4X10g
bridge 1 protocol rstp vlan-bridge
tfo Disable
errdisable cause stp-bpdu-guard
data-center-bridging enable bridge 1
priority-flow-control enable bridge 1
feature dns relay
ip dns relay
ipv6 dns relay
!
policy-map type queuing default PFC
 class type queuing default q0
  priority
  lossless
  exit
 class type queuing default q1
  priority
  lossless
  exit
 class type queuing default q2
  priority
  lossless
  exit
 class type queuing default q3
  shape 1 gbps
  priority
  lossless
  exit
 class type queuing default q4
  priority
  lossless
  exit
 class type queuing default q5
  priority
  lossless
  exit
!
vlan database
 vlan-reservation 4001-4094
 vlan 2 bridge 1 state enable
!
ip vrf management
!
interface cd1
!
interface cd2/1
 description Connected-STC
 switchport
```

```
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 priority-flow-control mode on
 priority-flow-control enable priority 0 1 2 3 4
 load-interval 30
 mtu 9216
 monitor pfc
!
interface cd2/2
!
!
interface eth0
 ip vrf forwarding management
 ip address dhcp
!
interface lo
 ip address 127.0.0.1/8
 ip address 1.1.1.1/32 secondary
 ipv6 address ::1/128
!
interface lo.management
 ip vrf forwarding management
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface xe65
!
interface xe66
 description Connected-DUT2
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 priority-flow-control mode on
 priority-flow-control enable priority 0 1 2 3 4
 load-interval 30
 mtu 9216
 service-policy type queuing output PFC
!
 exit
!
!
end
!
```

For ECN

```
!
service password-encryption
!
logging console 5
logging monitor 5
logging level all 7
!
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
!
qos enable
!
hostname DUT1
port cd2 breakout 4X10g
bridge 1 protocol rstp vlan-bridge
tfo Disable
errdisable cause stp-bpdu-guard
data-center-bridging enable bridge 1
priority-flow-control enable bridge 1
feature dns relay
ip dns relay
```

```
ipv6 dns relay
!
policy-map type queuing default ECN
 class type queuing default q0
  priority
  lossless
  exit
 class type queuing default q1
  priority
  lossless
  exit
 class type queuing default q2
  priority
  lossless
  exit
 class type queuing default q3
  shape 1 gbps
  priority
  random-detect green min-threshold 40 max-threshold 50 yellow min-threshold 70 max-threshold 80 red
min-threshold 100 max-threshold 110 packets ecn
  exit
 class type queuing default q4
  priority
  lossless
  exit
 class type queuing default q5
  priority
  lossless
  exit
!
vlan database
 vlan-reservation 4001-4094
 vlan 2 bridge 1 state enable
!
ip vrf management
!
interface cd1
!
interface cd2/1
 description Connected-STC
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 load-interval 30
 mtu 9216
!
interface cd2/2
!
interface eth0
 ip vrf forwarding management
 ip address dhcp
!
interface lo
 ip address 127.0.0.1/8
 ip address 1.1.1.1/32 secondary
 ipv6 address ::1/128
!
interface lo.management
 ip vrf forwarding management
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface xe65
!
interface xe66
 description Connected-DUT2
 switchport
```

```
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 load-interval 30
 mtu 9216
 service-policy type queuing output ECN
 monitor ecn
!
 exit
!
!
end
```

Validation

ECN Validation

Verify the traffic rates on interfaces.

```
Switch1 #sh int counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 cd2/1                4324.80        4223439       0.00           0
 xe66                 0.00           0             1000.08        976642
Switch1 #
Switch1 #sh int counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 cd2/1                4324.81        4223444       0.00           0
 xe66                 0.00           0             1000.08        976641
Switch1 #
Switch1 #
Switch1 #sh int counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 cd2/1                4324.81        4223444       0.00           0
 xe66                 0.00           0             1000.08        976641
Switch1 #
Switch1 #
Switch1 #
Switch1 #sh int counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 cd2/1                4324.81        4223444       0.00           0
 xe66                 0.00           0             1000.08        976641
```

High ingress rate on `cd2/1` (**~4324.81** Mbps), while egress `xe66` is capped at ~1000.08 Mbps due to the shaper. This confirms congestion on `xe66` without PFC pause (ingress rate is high).

Verify packet and byte counters for traffic passing through queues defined in applied policy maps.

```
Switch1 #sh policy-map statistics
Type qos class-map statistics:
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+
|            Class-map              |    Match pkts   |   Match bytes   |   Dropped
pkts  |   Dropped Bytes  |
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+

Type queuing class-map statistics:
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
```

```
|            Class-map           |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped
Bytes  |
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
xe66
 q3                              899353044         115117189632      294034145         37636370560
Switch1 #
Switch1 #sh policy-map statistics
Type qos class-map statistics:
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+
|            Class-map              |    Match pkts   |   Match bytes   |   Dropped
pkts  |   Dropped Bytes  |
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+

Type queuing class-map statistics:
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
|            Class-map           |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped
Bytes  |
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
xe66
 q3                              900905669         115315925632      300527546         38467525888
Switch1 #
Switch1 #
Switch1 #sh policy-map statistics
Type qos class-map statistics:
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+
|            Class-map              |    Match pkts   |   Match bytes   |   Dropped
pkts  |   Dropped Bytes  |
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+

Type queuing class-map statistics:
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
|            Class-map           |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped
Bytes  |
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
xe66
 q3                              901979712         115453403136      303774231         38883101568
Switch1 #
Switch1 #
Switch1 #sh policy-map statistics
Type qos class-map statistics:
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+
|            Class-map              |    Match pkts   |   Match bytes   |   Dropped
pkts  |   Dropped Bytes  |
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+

Type queuing class-map statistics:
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
|            Class-map           |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped
Bytes  |
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
xe66
 q3                              902926872         115574639616      307021247         39298719616
Switch1 #
```

For Interface `xe66`, **`queue q3`** shows a very large number of dropped packets (**`294034145 -> 307021247`**) alongside significant total packets (`902926872`) and total bytes (`115574639616`) successfully transmitted. As

ECN marking via **random-detect** is enabled on this queue, although some actual tail drops might occur if buffers completely fill, as **q3** is not configured as lossless here and PFC is disabled.

Verify the count of packets marked with ECN CE (Congestion Experienced) code point on a per-interface basis.

```
Switch1 #sh int counters ecn
+------------------+----------------------+
|  Interface       |  ECN marked packets  |
+------------------+----------------------+
 xe66                47941117
Switch1 #
Switch1 #sh int counters ecn
+------------------+----------------------+
|  Interface       |  ECN marked packets  |
+------------------+----------------------+
 xe66                48917797
Switch1 #
Switch1 #sh int counters ecn
+------------------+----------------------+
|  Interface       |  ECN marked packets  |
+------------------+----------------------+
 xe66                49894369
Switch1 #
Switch1 #
Switch1 #sh int counters ecn
+------------------+----------------------+
|  Interface       |  ECN marked packets  |
+------------------+----------------------+
 xe66                50871013
Switch1 #

2025 Oct 28 12:24:23.009 : Switch1  : HSL : NOTIF : [IF_ECN_MONITOR_4]: ECN: Interface - xe66, ECN
MARKED PKT: 4883112
2025 Oct 28 12:24:28.009 : Switch1  : HSL : NOTIF : [IF_ECN_MONITOR_4]: ECN: Interface - xe66, ECN
MARKED PKT: 4883148
2025 Oct 28 12:24:33.010 : Switch1  : HSL : NOTIF : [IF_ECN_MONITOR_4]: ECN: Interface - xe66, ECN
MARKED PKT: 4883184
2025 Oct 28 12:24:38.010 : Switch1  : HSL : NOTIF : [IF_ECN_MONITOR_4]: ECN: Interface - xe66, ECN
MARKED PKT: 4883148
2025 Oct 28 12:24:43.010 : Switch1  : HSL : NOTIF : [IF_ECN_MONITOR_4]: ECN: Interface - xe66, ECN
MARKED PKT: 4883076
2025 Oct 28 12:24:48.010 : Switch1  : HSL : NOTIF : [IF_ECN_MONITOR_4]: ECN: Interface - xe66, ECN
MARKED PKT: 4883040
2025 Oct 28 12:24:53.010 : Switch1  : HSL : NOTIF : [IF_ECN_MONITOR_4]: ECN: Interface - xe66, ECN
MARKED PKT: 4883364
2025 Oct 28 12:24:58.011 : Switch1  : HSL : NOTIF : [IF_ECN_MONITOR_4]: ECN: Interface - xe66, ECN
MARKED PKT: 4883292
2025 Oct 28 12:25:03.011 : Switch1  : HSL : NOTIF : [IF_ECN_MONITOR_4]: ECN: Interface - xe66, ECN
MARKED PKT: 4883220
2025 Oct 28 12:25:08.011 : Switch1  : HSL : NOTIF : [IF_ECN_MONITOR_4]: ECN: Interface - xe66, ECN
MARKED PKT: 4883112
```

Interface **xe66** shows a large and increasing number of ECN marked packets (`47941117` **->** `50871013`), directly confirming ECN marking is active due to the egress congestion.

These log messages are generated due to the **monitor ecn** command on **xe66**. The logs periodically report the cumulative count of ECN Marked packet on interface **xe66**, providing real-time visibility into the ECN marking activity. The counts align with the increasing values seen in **sh int counters ecn.**

The configuration given in the Validation (page 862) successfully sets up an L2 path, induces congestion on the egress interface **xe66** via shaping, and applies an ECN policy. Validation confirms that packets exceeding the WRED thresholds in **queue 3** are being marked with ECN (not dropped), as shown by the dedicated ECN counters, interpreted policy map statistics, and system logs.

PFC Validation

Verify the traffic rates on interfaces.

```
Switch1 #sh int counters rate mbps
+------------------+--------------+-------------+--------------+-------------+
|     Interface    |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+------------------+--------------+-------------+--------------+-------------+
 cd2/1               1000.12        976675        13.89          27130
 xe66                0.00           0             1000.12        976679
Switch1 #
Switch1 #
Switch1 #sh int counters rate mbps
+------------------+--------------+-------------+--------------+-------------+
|     Interface    |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+------------------+--------------+-------------+--------------+-------------+
 cd2/1               1000.12        976675        13.89          27130
 xe66                0.00           0             1000.12        976679
Switch1 #
Switch1 #sh int counters rate mbps
+------------------+--------------+-------------+--------------+-------------+
|     Interface    |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+------------------+--------------+-------------+--------------+-------------+
 cd2/1               1000.12        976675        13.89          27130
 xe66                0.00           0             1000.12        976679
Switch1 #
```

The egress interface **xe66** is capped at ~1000.12 Mbps due to the shaper. The ingress interface **cd2/1** also shows a receive rate throttled down to ~1032 Mbps. This indicates that PFC pausing is throttling the source to match the egress shaper rate.

Verify packet and byte counters for traffic passing through queues defined in applied policy maps.

```
Switch1 #sh policy-map statistics
Type qos class-map statistics:
+-----------------------------------+-----------------+----------------+-----------------+---------
---------+
|            Class-map              |    Match pkts   |   Match bytes   |   Dropped
pkts  |   Dropped Bytes  |
+-----------------------------------+-----------------+----------------+-----------------+---------
---------+

Type queuing class-map statistics:
+---------------------------------+-----------------+-----------------+-----------------+-------------
-----+
|            Class-map           |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped
Bytes  |
+---------------------------------+-----------------+-----------------+-----------------+-------------
-----+
xe66
 q3                               222189660         28440276480       0                 0
Switch1 #

Switch1 #sh policy-map statistics
Type qos class-map statistics:
+-----------------------------------+-----------------+----------------+-----------------+---------
---------+
|            Class-map              |    Match pkts   |   Match bytes   |   Dropped
pkts  |   Dropped Bytes  |
+-----------------------------------+-----------------+----------------+-----------------+---------
---------+

Type queuing class-map statistics:
+---------------------------------+-----------------+-----------------+-----------------+-------------
-----+
|            Class-map           |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped
Bytes  |
+---------------------------------+-----------------+-----------------+-----------------+-------------
-----+
xe66
 q3                               222980616         28541518848       0                 0
Switch1 #
```

```
Switch1 #sh policy-map statistics
Type qos class-map statistics:
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+
|            Class-map              |    Match pkts   |   Match bytes   |   Dropped
pkts  |   Dropped Bytes  |
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+

Type queuing class-map statistics:
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
|            Class-map           |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped
Bytes  |
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
xe66
 q3                              223732822         28637801216       0                 0
Switch1 #
Switch1 #
Switch1 #sh policy-map statistics
Type qos class-map statistics:
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+
|            Class-map              |    Match pkts   |   Match bytes   |   Dropped
pkts  |   Dropped Bytes  |
+-----------------------------------+-----------------+-----------------+-----------------+---------
---------+

Type queuing class-map statistics:
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
|            Class-map           |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped
Bytes  |
+--------------------------------+-----------------+-----------------+-----------------+-------------
-----+
xe66
 q3                              224865972         28782844416       0                 0
```

Interface **xe66**, **queue q3** shows a large number of Total pkts **(224865972)** and Total bytes (28782844416) successfully transmitted, but critically shows Dropped pkts: 0. This confirms that PFC is working as intended in this L2 scenario, preventing drops despite the 1 Gbps shaper inducing congestion on a lossless queue.

Verify the counters for PFC pause frames sent and received per priority per interface.

```
Verify the counters for PFC pause frames sent and received per priority per interface.
Switch1 #sh priority-flow-control statistics all
interface         pri   pause sent     pause received
=====================================================
xe66              0     0              0
xe66              1     0              0
xe66              2     0              0
xe66              3     0              0
xe66              4     0              0
xe66              5     0              0
xe66              6     0              0
xe66              7     0              0
cd2/1             0     0              0
cd2/1             1     0              0
cd2/1             2     0              0
cd2/1             3     6323876        0
cd2/1             4     0              0
cd2/1             5     0              0
cd2/1             6     0              0
cd2/1             7     0              0
Switch1 #
sh priority-flow-control statistics all
```

```
interface         pri   pause sent     pause received
=======================================================
xe66              0     0              0
xe66              1     0              0
xe66              2     0              0
xe66              3     0              0
xe66              4     0              0
xe66              5     0              0
xe66              6     0              0
xe66              7     0              0
cd2/1             0     0              0
cd2/1             1     0              0
cd2/1             2     0              0
cd2/1             3     6432396        0
cd2/1             4     0              0
cd2/1             5     0              0
cd2/1             6     0              0
cd2/1             7     0              0
Switch1 #

Switch1 #sh priority-flow-control statistics all
interface         pri   pause sent     pause received
=======================================================
xe66              0     0              0
xe66              1     0              0
xe66              2     0              0
xe66              3     0              0
xe66              4     0              0
xe66              5     0              0
xe66              6     0              0
xe66              7     0              0
cd2/1             0     0              0
cd2/1             1     0              0
cd2/1             2     0              0
cd2/1             3     6459528        0
cd2/1             4     0              0
cd2/1             5     0              0
cd2/1             6     0              0
cd2/1             7     0              0
Switch1 #
Switch1 #sh priority-flow-control statistics all
interface         pri   pause sent     pause received
=======================================================
xe66              0     0              0
xe66              1     0              0
xe66              2     0              0
xe66              3     0              0
xe66              4     0              0
xe66              5     0              0
xe66              6     0              0
xe66              7     0              0
cd2/1             0     0              0
cd2/1             1     0              0
cd2/1             2     0              0
cd2/1             3     6486658        0
cd2/1             4     0              0
cd2/1             5     0              0
cd2/1             6     0              0
cd2/1             7     0              0
Switch1 #
```

Interface **cd2/1** shows a large and rapidly increasing count of **pause sent** frames specifically for **priority 3** (**6323876 ->** 6486658). No pause frames are received (pause received is 0). This confirms that Switch1 is sending PFC pause frames out of the ingress interface **cd2/1** for priority 3. This happens because the downstream path (egress interface **xe66**) is congested for queue 3 (due to the shaper), and PFC is enabled for this priority.

Verify the administrative and operational status of PFC per interface.

```
Switch1 #sh priority-flow-control details all


Switch1 #2025 Oct 28 11:48:37.913 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface -
cd2/1, PG[3]: Pause-Tx: 140027
2025 Oct 28 11:48:42.913 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 140026
~2025 Oct 28 11:48:47.913 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 140028
2025 Oct 28 11:48:52.913 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 140023
2025 Oct 28 11:48:57.914 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 140023
2025 Oct 28 11:49:02.914 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 140025
2025 Oct 28 11:49:07.914 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 140026
2025 Oct 28 11:49:12.914 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 140023
2025 Oct 28 11:49:17.914 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 140037
2025 Oct 28 11:49:22.915 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 140014
2025 Oct 28 11:49:27.915 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 140031
2025 Oct 28 11:49:32.915 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 140019
2025 Oct 28 12:16:32.991 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 135652
2025 Oct 28 12:16:37.991 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 135647
2025 Oct 28 12:16:42.991 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 135652
2025 Oct 28 12:16:47.991 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 135647
2025 Oct 28 12:16:52.992 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 135648
2025 Oct 28 12:16:57.992 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 135650
2025 Oct 28 12:17:02.992 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 135648
2025 Oct 28 12:17:07.992 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 135652
2025 Oct 28 12:17:12.992 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 135646
2025 Oct 28 12:17:17.993 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 135648
2025 Oct 28 12:17:22.993 : Switch1  : HSL : NOTIF : [IF_PFC_MONITOR_4]: PFC: Interface - cd2/1, PG
[3]: Pause-Tx: 135662
!
```

Logs periodically report the number of Pause-Tx (transmitted pause frames) for Priority Group 3 (PG[3]) on interface **cd2/1**, confirming the PFC activity shown in the statistics command. Conversely, if pause frames are received rather than transmitted, equivalent Pause-Rx logs will be displayed.

The configuration given in the Validation (page 862) establishes an L2 path with shaping on egress (**xe66**) and PFC enabled on both ingress (**cd2/1**) and egress for relevant priorities. Validation confirms that congestion on the egress interface triggers PFC pause frames to be sent from the ingress interface (**cd2/1**), successfully throttling the traffic source. The policy map statistics verify that no packets are dropped for the shaped lossless queue (**q3**) due to PFC being active.

CLI Commands

The feature introduces the following configuration commands.

monitor ecn

monitor pfc

Glossary

The following table provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
PFC	Priority-based Flow Control. A mechanism supported by OcNOS to pause frames using defined times for each of the eight priority classes to prevent congestion.
ECN	Explicit Congestion Notification. A mechanism defined in RFC 3168 that provides end-to-end congestion signaling between ECN-enabled senders and receivers in TCP/IP networks. Instead of dropping packets, ECN marks them to indicate congestion.

© 2026 IP Infusion Inc. Proprietary

Data Centre Bridging Capability Exchange Configuration

Overview

The Data Center Bridging (page 824) (DCBx) protocol extends the Link Layer Discovery Protocol (LLDP). It facilitates the exchange of Data Center Bridging Configuration parameters between directly connected devices, such as switches and network interface cards (NICs). DCBx enables automatic negotiation and configuration of DCB features to ensure consistent quality of service (QoS) and traffic prioritization across a network.

DCBx plays a crucial role in modern data centers by enabling seamless configuration and interoperability between DCB-capable devices, ensuring efficient network performance.

Limitation:

If Link Layer Discovery Protocol (LLDP) is disabled on an interface, DCBX cannot operate on that interface. Attempting to enable DCBX on an interface where LLDP is disabled will result in a configuration commit failure.

Benefits

- Discovers the DCB capabilities of neighboring devices.
- Detects incorrect configurations or mismatches in DCB settings between peers.
- Configures DCB parameters on connected devices for interoperability.

DCBX Configuration for PFC via LLDP

Configuring PFC parameter exchange typically involves enabling PFC mode, LLDP, activating DCBX, turning on PFC, and allowing the negotiation of control for each traffic priority (priorities 0–7).

Topology

The topology involves two switches SW1 and SW2 directly connected and enabled with DCBx and PFC.

Figure 62. PFC Configuration

Configuration

The following procedure configures PFC parameters and sent them in LLDP messages.

1. Create bridge and enable DCB and PFC on SW1 and SW2.

```
bridge 1 protocol ieee vlan-bridge
data-center-bridging enable bridge
priority-flow-control enable bridge1
```

2. Set interface cd1/1 on SW1 and SW2 to layer 2 and bind it to bridge group.

```
interface cd1/1
 switchport
 bridge-group 1
```

3. Enable LLDP and DCBx on SW1 and SW2. Set LLDP for transmit and receive mode on the interface. Set the TLVs enabled for transmission on the interface to send an IEEE 802.1 organizationally specific TLV set in the packet.

```
!
lldp-agent
 set lldp enable txrx
 lldp tlv ieee-8021-org-specific data-center-bridging select
 dcbx enable
!
```

4. Configure PFC on SW1 and SW2. Set the maximum number of priorities allowed for priority flow control on the interface. Enable PFC on priorities 0,1, and 2

```
!
priority-flow-control mode auto
priority-flow-control cap 3
priority-flow-control link-delay-allowance 65345
priority-flow-control enable priority 0 1 2
!
```

on SW2.

```
!
priority-flow-control mode auto
priority-flow-control cap 6
priority-flow-control link-delay-allowance 5678
priority-flow-control enable priority 5 6 7
!
```

Validation

Verify DCBx and PFC status on SW1.

```
SW1#show priority-flow-control details interface cd1/1

bridge : 1
priority flow control : on
interface : cd1/1

Admin Configuration
--------------------
mode  advertise willing   cap   link delay  priorities
                                allowance
================================================================================
auto  on        on        3     65345       0 1 2

--------------------------------------------------------------------------------

Operational Configuration
-------------------------
state cap   link delay  priorities
            allowance
================================================================================
on    6     65345       5 6 7
```

Verify DCBx and PFC status on SW2.

```
SW2#show priority-flow-control details interface cd1/1

bridge : 1
```

```
priority flow control : on
interface : cd1/1

Admin Configuration
--------------------
mode  advertise willing   cap   link delay  priorities
                                allowance
================================================================================
auto  on        on        6     5678        5 6 7

--------------------------------------------------------------------------------

Operational Configuration
-------------------------
state cap   link delay  priorities
            allowance
================================================================================
on    6     5678        5 6 7
```

Verify Interface on SW1.

```
SW1#show int cd1/1
Interface cd1/1
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: 5c17.83f0.8523
  Physical:5c17.83f0.8523  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC operational status is off
  Port Mode is access
  Protected Mode is Promiscuous
  Interface index: 5067
  Metric 1 mtu 1500 duplex-full  link-speed 10g
  Debounce timer: disable
  <UP,BROADCAST,RUNNING,ALLMULTI,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2025 Feb 25 16:54:32 (00:13:05 ago)
  Load Interval: 300 seconds.
  Statistics last cleared: 2025 Feb 25 16:54:32 (00:13:05 ago)
  ND router advertisements are sent approximately every 0 seconds
  ND next router advertisement due in 0 seconds.
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
  5 minute input rate 16 bits/sec, 0 packets/sec
  5 minute output rate 292 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 29 broadcast packets 0
    input packets 29 bytes 1856
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 423 broadcast packets 0
    output packets 423 bytes 29717
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```

Verify Interface on SW2

```
SW2#show int cd1/1
Interface cd1/1
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: 5c17.83ff.305f
  Physical:5c17.83ff.305f  Logical:(not set)
```

```
Forward Error Correction (FEC) configured is Auto (default)
FEC operational status is off
Port Mode is access
Protected Mode is Promiscuous
Interface index: 5035
Metric 1 mtu 1500 duplex-full  link-speed 10g
Debounce timer: disable
<UP,BROADCAST,RUNNING,ALLMULTI,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2025 Feb 25 16:59:54 (00:13:49 ago)
Load Interval: 300 seconds.
Statistics last cleared: 2025 Feb 25 16:59:54 (00:13:49 ago)
ND router advertisements are sent approximately every 0 seconds
ND next router advertisement due in 0 seconds.
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
5 minute input rate 294 bits/sec, 0 packets/sec
5 minute output rate 17 bits/sec, 0 packets/sec
RX
  unicast packets 0 multicast packets 446 broadcast packets 0
  input packets 446 bytes 31279
  jumbo packets 0
  undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
  input error 0
  input with dribble 0 input discard 0
  Rx pause 0
TX
  unicast packets 0 multicast packets 31 broadcast packets 0
  output packets 31 bytes 1984
  jumbo packets 0
  output errors 0 collision 0 deferred 0 late collision 0
  output discard 0
  Tx pause 0
```

DATA CENTER BRIDGING COMMAND REFERENCE

Data Center Bridge Commands 875
data-center-bridging 876
show data-center-bridging 877
Priority-based Flow Control Commands 879
clear priority-flow-control deadlock-status 880
monitor ecn 881
monitor pfc 882
priority-flow-control accept-peer-config 883
priority-flow-control advertise-local-config 884
priority-flow-control cap 885
priority-flow-control deadlock manual-recovery 886
priority-flow-control enable 887
priority-flow-control enable priority 888
priority-flow-control link-delay-allowance 889
priority-flow-control mode 890
priority-flow-control deadlock recovery-action drop 891
priority-flow-control deadlock recovery-mode timer 892
priority-flow-control deadlock recovery-mode pfc-state-xon 893
show priority-flow-control details 894
show priority-flow-control statistics 896
show priority-flow-control deadlock-status 897

© 2026 IP Infusion Inc. Proprietary

Data Center Bridge Commands

This section lists and describes the commands that can be used in a Data Center Bridging (DCB) environment.

data-center-bridging 876
show data-center-bridging 877

data-center-bridging

Use this command to enable the Data Center Bridging.

Use the **no** form of this command to disable the Data Center Bridging

Command Syntax

```
data-center-bridging enable
data-center-bridging disable
```

Parameters

None

Default

Disable

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.1 This command is applicable for earlier releases prior to OcNOS version 6.6.1 for backward compatibility.

Example

```
OcNOS(config)#data-center-bridging enable bridge 1
OcNOS(config)#commit
OcNOS(config)#
OcNOS(config)#data-center-bridging disable bridge 1
OcNOS(config)#commit
OcNOS(config)#
```

© 2026 IP Infusion Inc. Proprietary

show data-center-bridging

Use this command to display information about show data-center-bridging.

Command Syntax

```
show data-center-bridging admin-details
show data-center-bridging operational-details
show data-center-bridging remote-details
```

Parameters

admin-details
administrative details

operational-details
operational details

remote-details
remote details

Default

None

Command Mode

Execution mode Privileged execution mode

Applicability

This command is introduced in OcNOS version 6.5.1.

Example

The following example shows the creation of a TWAMP Session and the change into `twamp-session` mode prompt.

```
#show data-center-bridging admin-details interface xe4/3
PFC administrative details
interface : xe4/3
State advertise willing   cap   syncd     priorities

================================================================================
On    On        On        4     On        3 4


#show data-center-bridging operational-details interface xe4/3
PFC Operational details
interface : xe4/3
state cap    syncd priorities
================================================================================
On    4      On    0 1 2


#show data-center-bridging remote-details interface xe4/3
PFC Remote details
```

```
interface : xe4/3
State Willing   Cap       Priorities
================================================================================
On    On        4         0 1 2
```

Priority-based Flow Control Commands

This section lists and describes the commands that can be used to configure Priority-based Flow Control (PFC) in a Data Center Bridging (DCB) environment.It includes the following commands:

clear priority-flow-control deadlock-status 880
monitor ecn 881
monitor pfc 882
priority-flow-control accept-peer-config 883
priority-flow-control advertise-local-config 884
priority-flow-control cap 885
priority-flow-control deadlock manual-recovery 886
priority-flow-control enable 887
priority-flow-control enable priority 888
priority-flow-control link-delay-allowance 889
priority-flow-control mode 890
priority-flow-control deadlock recovery-action drop 891
priority-flow-control deadlock recovery-mode timer 892
priority-flow-control deadlock recovery-mode pfc-state-xon 893
show priority-flow-control details 894
show priority-flow-control statistics 896
show priority-flow-control deadlock-status 897

© 2026 IP Infusion Inc. Proprietary

clear priority-flow-control deadlock-status

Use this command to clear the PFC deadlock details for a specified interface or for all interfaces.

Command Syntax

```
clear priority-flow-control deadlock-status [ IFNAME ]
```

Parameters

IFNAME
Name of the input or output interface.

Default

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 7.0.0.

Example

```
#clear priority-flow-control deadlock-status interface eth1
```

© 2026 IP Infusion Inc. Proprietary

monitor ecn

Use this command to enable Explicit-Congestion-Notification (ECN) marked packets monitoring on a physical interface.

Use the `no` form of this command to disable ECN monitoring on the interface

Command Syntax

```
monitor ecn
no monitor ecn
```

Parameters

None

Default

None

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 7.0.0.

Example

```
(config)#interface xe1
(config-if)#monitor ecn
```

© 2026 IP Infusion Inc. Proprietary

monitor pfc

Use this command to enable Priority-based Flow Control (PFC) pause frames monitoring on a physical interface.

Use the `no` form of this command to disable PFC monitoring on the interface.

Command Syntax

```
monitor pfc
no monitor pfc
```

Parameters

None

Default

None

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 7.0.0.

Example

```
(config)#interface xe1
(config-if)#monitor pfc
```

© 2026 IP Infusion Inc. Proprietary

priority-flow-control accept-peer-config

Use this command to enable willing mode for PFC on the interface. If willing is enabled, then by default advertise mode is also enabled. Use the no form of this command to disable willing mode.

Command Syntax

```
priority-flow-control accept-peer-config
no priority-flow-control accept-peer-config
```

Parameters

None

Default

By default, willing mode for PFC on the interface is disabled. If willing is enabled, then by default advertise mode is also enabled.

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#priority-flow-control accept-peer-config
```

© 2026 IP Infusion Inc. Proprietary

priority-flow-control advertise-local-config

Use this command to enable advertising mode for PFC on the interface.

Use the no form of this command to disable advertising mode.

Command Syntax

```
priority-flow-control advertise-local-config
no priority-flow-control advertise-local-config
```

Parameters

None

Default

By default, advertising mode for PFC on the interface is disabled. If willing is enabled, then by default advertise mode is also enabled.

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#priority-flow-control advertise-local-config
```

© 2026 IP Infusion Inc. Proprietary

priority-flow-control cap

Use this command to configure a priority-flow-control cap for the number of priorities allowed on an interface.

Use the no parameter along with this command to return the value to its default level.

Command Syntax

```
priority-flow-control cap <0-8>
no priority-flow-control cap
```

Parameters

<0-8>

Select a cap value. Zero indicates that there is no limitations.

Default

By default, priority-flow-control cap value is 8.

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe2
(config-if)#priority-flow-control cap 7
```

© 2026 IP Infusion Inc. Proprietary

priority-flow-control deadlock manual-recovery

Use this command to start/stop manually the PFC deadlock recovery on the specified interface.

Command Syntax

```
priority-flow-control <NAME> deadlock manual-recovery ( start | stop )
```

Parameters

IFNAME
Name of the input or output interface.

Default

Nones

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 7.0.0.

Example

```
#priority-flow-control eth1 deadlock manual-recovery start
#priority-flow-control eth1 deadlock manual-recovery stop
```

© 2026 IP Infusion Inc. Proprietary

priority-flow-control enable

Use this command to enable Priority-based Flow Control (PFC) on a switch (bridge).

Use the `no` form of this command to disable PFC.

Command Syntax

```
priority-flow-control enable bridge <1-32>
no priority-flow-control bridge <1-32>
```

Parameters

<1-32>
Bridge ID.

Default

By default, PFC is disabled.

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 1.3. This command is applicable for L3 interface from OcNOS version 6.6.1.

Example

```
#configure terminal
(config)#priority-flow-control enable bridge 32

#configure terminal
(config)#no priority-flow-control bridge 32
```

© 2026 IP Infusion Inc. Proprietary

priority-flow-control enable priority

Use this command to enable the PFC at the interface level for a specific priority.

Use the no parameter along with this command to disable PFC for a priority.

Command Syntax

```
priority-flow-control enable priority <0-7> (<0-7>(<0-7>(<0-7> (<0-7>(<0-7>(<0-7>(<0-7>|)|)|)|)|)|)|)
no priority-flow-control enable priority <0-7> (<0-7>(<0-7>(<0-7>(<0-7>(<0-7>(<0-7>(<0-
7>|)|)|)|)|)|)|)
```

Parameters

<0-7>

Traffic-priority value. You can specify up to seven priorities.

Default

None

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 1.3.

Example

```
(config)#interface xe1
(config-if)#priority-flow-control enable priority 1 2 3 4 5 6 7

(config)#interface xe1
(config-if)#no priority-flow-control enable priority 2 3 4
```

© 2026 IP Infusion Inc. Proprietary

priority-flow-control link-delay-allowance

Use this command to set PFC link delay allowance on an interface. This command provides allowance for round-trip propagation delay of the link in bits; moreover, it is one of the factors that determines when to trigger PAUSE.

Use the no parameter along with this command to unset PFC link delay allowance on an interface.

Command Syntax

```
priority-flow-control link-delay-allowance <0-4294967296>
no priority-flow-control link-delay-allowance
```

Parameters

<0-4294967296>

Link characteristics that affect the link delay (for example, link length).

Note: The range value is determined by the board type: for Tomahawk 3, it is 8,388,608; for Trident 3, it is 4,194,304; and for all other boards, the default value is 524,288.

Default

Default value is zero.

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#priority-flow-control link-delay-allowance 5

(config)#interface xe1
(config-if)#no priority-flow-control link-delay-allowance
```

© 2026 IP Infusion Inc. Proprietary

priority-flow-control mode

Use this command to enable Priority-based Flow Control (PFC) on an interface.

Ues the no form of this command to disable PFC on an interface.

Command Syntax

```
priority-flow-control mode (on | auto)
no priority-flow-control
```

Parameters

auto
Negotiate PFC capabilities.

on
Force-enable PFC, overriding negotiation.

Default

By default, PFC is disabled.

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 1.3. his command is applicable for L3 interface from OcNOS version 6.6.1.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#priority-flow-control mode auto
```

© 2026 IP Infusion Inc. Proprietary

priority-flow-control deadlock recovery-action drop

Use this command to globally drop deadlocked traffic on Priority-based Flow Control (PFC) deadlock recovery.

Use the `no` form of this command to allow deadlocked traffic when a PFC deadlock recovery occurs.

Command Syntax

```
priority-flow-control deadlock recovery-action drop
no priority-flow-control deadlock recovery-action drop
```

Parameters

None

Default

By default, PFC deadlocked traffic during a recovery is allowed.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 7.0.0.

Example

```
#configure terminal (config)
#priority-flow-control deadlock recovery-action drop
```

© 2026 IP Infusion Inc. Proprietary

priority-flow-control deadlock recovery-mode timer

Use this command to enable Priority-based Flow Control (PFC) deadlock and recovery on all priorities of an interface, using a timer to end the recovery phase.

Use the `no` form of this command to disable PFC deadlock detection and recovery on an interface.

Command Syntax

```
priority-flow-control deadlock recovery-mode timer
[ detection-multiplier <1-1599> time-granularity <1|10|100> ]
[ recovery-time <100-1599> ]

no priority-flow-control deadlock recovery-mode
```

Parameters

detection-multiplier
Specify the detection multiplier duration in micro seconds.

time-granularity
Specify the time granularity duration in micro seconds.

recovery-time
Specify the Recovery time duration in micro seconds.

Default

By default, detection multiplier is 10, time granularity is 10ms and recovery time is 100ms.

PFC deadlock detection is disabled by default.

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 7.0.0.

Example

```
(config)#interface xe1
(config-if)#priority-flow-control deadlock recovery-mode
timer detection-multiplier 100 time-granularity 100
recovery-time 1000

OcNOS(config)#interface xe0
OcNOS(config-if)#no priority-flow-control deadlock recovery-mode
```

© 2026 IP Infusion Inc. Proprietary

priority-flow-control deadlock recovery-mode pfc-state-xon

Use this command to enable Priority-based Flow Control (PFC) deadlock and recovery on all priorities of an interface, using XON packet reception end the recovery phase.m

Use the `no` form of this command to disable PFC deadlock detection and recovery on an interface.

Command Syntax

```
priority-flow-control deadlock recovery-mode pfc-state-xon
[ detection-multiplier <1-1599> time-granularity <1|10|100> ]


no priority-flow-control deadlock recovery-mode
```

Parameters

detection-multiplier
Specify the detection multiplier duration in micro seconds.

time-granularity
Specify the time granularity duration in micro seconds.

Default

By default, detection multiplier is 10, and time granularity is 10ms.

PFC deadlock detection is disabled by default.

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 7.0.0.

Example

#configure terminal (config)

```
#configure terminal (config)
(config)#interface xe1

(config-if)#priority-flow-control deadlock recovery-mode pfc-state-xon
detection-multiplier 100 time-granularity 100
```

show priority-flow-control details

Use this command to display the PFC details for a specified interface.

Command Syntax

```
show priority-flow-control details ((all|interface IFNAME)|(bridge <1-32>))
```

Parameters

IFNAME
Name of the input or output interface.

<1-32>
Specify a bridge ID.

all
Display PFC enabled L2 and L3 interfaces

Default

By default, PFC is disabled.

Command Mode

Execution mode

Applicability

This command is introduced in OcNOS version 1.3. Updated to add “all” attribute which displays PFC enabled L2 and L3 interfaces in the show output from OcNOS version 6.6.1.

Example

```
#show priority-flow-control details interface xe1
bridge : 2
priority flow control : on
interface : xe1

Admin Configuration
mode  advertise willing   cap   link        priorities
                                delay
                                allowance
================================================================================
on    on        off       5     128         2 3 4 5

Operational Configuration
state cap   link        priorities
            delay
            allowance
================================================================================
on    5     128         2 3 4 5
```

Entry	Description
bridge	The bridge number to which this interface is associated (1-32).
priority flow control	Show whether priority flow control is either on or off.
interface	The interface name.
Admin Configuration	The configuration as entered on this device.e.
mode	The priority flow control operating mode – on, off, or auto.
advertise	Status of advertisement of the configuration to the peer devic
willing	The willingness of the local interface to learn the PFC configuration from the peer.
cap	Values are either on or off.
link delay allowance	Cap is a limit set that specifies the maximum number of PFC priorities. The allowance made for round-trip propagation delay of the link in bits.
Priorities	Shows the PFCs that have been to be used on the priorities.
Operational Configuration s	The actual configuration that exists between this device and its PFC peer.
state	Shows whether PFC is functioning. Values are on, off, or auto.
cap	Cap is the limit that specifies the maximum number of PFC priorities.
link delay allowance	The allowance being used for round-trip propagation delay of the link in bits.
priorities	The PFCs actually being used by this device and its peer.

© 2026 IP Infusion Inc. Proprietary

show priority-flow-control statistics

Use this command to display statistics about the number of PFC Pause frames sent and received for a specified interface or bridge. If you do not specify a bridge or interface, this commands shows statistics for the bridge.

Command Syntax

```
show priority-flow-control statistics ((all|interface IFNAME)| (bridge <1-32>))
```

Parameters

<1-32>
Specify bridge ID.

IFNAME
Name of the input or output interface

all
Display PFC enabled L2 and L3 interfaces

Default

None

Command Mode

Execution mode

Applicability

This command is introduced in OcNOS version 1.3. Updated to add “all” attribute which displays PFC enabled L2 and L3 interfaces in the show output from OcNOS version 6.6.1.

Example

```
#show priority-flow-control statistics interface xe1
bridge : 2
interface : xe1
pause sent     pause received
==============================
5968061499624837205583457486l
```

show priority-flow-control deadlock-status

Use this command to display the PFC deadlock details for a specified interface or for all interfaces.

Command Syntax

```
show priority-flow-control deadlock-status [ IFNAME ]
```

Parameters

IFNAME
Name of the input or output interface.

Default

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 7.0.0.

Example

```
#show priority-flow-control deadlock-status

Deadlock Detection and Recovery Configuration
-------------------------------------------------------------------------
interface recovery detection detection recovery
mode multiplier granularity time
=========================================================================
xe0 Timer 10 10 1500

-------------------------------------------------------------------------------------------------------

Deadlock Detection and Recovery Status
-------------------------------------------------------------------------------------------------------
----
interface pri state detection last detection last recovery
count timestamp timestamp
=======================================================================================================
xe0 1 deadlock 39 2025-05-29 19:03:49.481 -
```