



# **OcNOS®**

## **Open Compute Network Operating System for Data Centers Version 6.3.5**

**System Management Guide**

**June 2024**

---

© 2024 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.

3965 Freedom Circle, Suite 200

Santa Clara, CA 95054

+1 408-400-1900

<http://www.ipinfusion.com/>

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

[support@ipinfusion.com](mailto:support@ipinfusion.com)

Trademarks:

IP Infusion and OcNOS 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

<b>Preface</b> .....	<b>xxiii</b>
IP Maestro Support .....	xxiii
Audience .....	xxiii
Conventions .....	xxiii
Chapter Organization .....	xxiii
Related Documentation .....	xxiii
Migration Guide .....	xxiv
Feature Availability .....	xxiv
Support .....	xxiv
Comments .....	xxiv
 <b>Command Line Interface</b> .....	 <b>23</b>
Overview .....	23
Command Line Interface Help .....	23
Command Completion .....	24
Command Abbreviations .....	24
Command Line Errors .....	24
Command Negation .....	25
Syntax Conventions .....	25
Variable Placeholders .....	26
Command Description Format .....	27
Keyboard Operations .....	27
Show Command Modifiers .....	28
String Parameters .....	31
Command Modes .....	31
Transaction-based Command-line Interface .....	33
 <b>System Management Configuration Guide</b> .....	 <b>35</b>
CHAPTER 1   Access Control Lists Configurations .....	37
Overview .....	37
Topology .....	37
IPv4 ACL Configuration .....	37
ICMP ACL Configuration .....	38
Access List Entry Sequence Numbering .....	39
IPv6 ACL Configuration .....	40
MAC ACL Configuration .....	40
Management ACL Overview .....	41
ARP ACL Overview .....	46
ACL OVER LOOPBACK .....	47
ACL OVER VTY .....	49
Timed ACL .....	51
Topology .....	51

CHAPTER 2	Control Plane Policing Configuration . . . . .	55
CHAPTER 3	DHCP Client Configuration . . . . .	61
	Overview . . . . .	61
	DHCP Client Configuration for IPv4 . . . . .	61
CHAPTER 4	DHCP Relay Agent Configuration . . . . .	63
	Overview . . . . .	63
	DHCP Relay for IPv4 . . . . .	63
	DHCP Relay for IPv6 Configuration . . . . .	64
	DHCP Relay option 82 . . . . .	65
	Physical Interface Configuration with non-default vrf . . . . .	67
	Validation . . . . .	68
CHAPTER 5	DHCP Relay Agent Over L3VPN Configuration . . . . .	75
	DHCP Relay Over L3 VPN for IPv4 . . . . .	75
	DHCP Relay Over L3 VPN for IPv6 . . . . .	80
CHAPTER 6	DHCP Snooping . . . . .	87
	Overview . . . . .	87
	Topology . . . . .	88
	Configuration Guidelines . . . . .	88
	Procedures . . . . .	88
	DHCP Snooping Operation . . . . .	89
	DHCP Snooping with Option-82 . . . . .	91
CHAPTER 7	DHCP Snooping IP Source Guard . . . . .	97
	Overview . . . . .	97
	Topology . . . . .	97
	Configuration . . . . .	97
	Configuring Trusted and Un-trusted Ports . . . . .	99
	Configuring IP Source Guard on LAG Port . . . . .	99
CHAPTER 8	DHCP Snooping over MLAG . . . . .	103
	Overview . . . . .	103
	Topology . . . . .	104
	Configuration . . . . .	105
	Validation . . . . .	113
CHAPTER 9	DHCPv6 Prefix Delegation . . . . .	119
	Overview . . . . .	119
	Topology . . . . .	119
	Configuration . . . . .	120
	Validation . . . . .	121
CHAPTER 10	DHCPv6 Relay Prefix Delegation Route Injection Configuration . .	123
	Overview . . . . .	123
	Topology . . . . .	123
CHAPTER 11	DHCP Server Configuration . . . . .	129
	Overview . . . . .	129
	DHCP Server Configuration for IPv4 . . . . .	129

---

DHCP Server Configuration for IPv6 .....	132
CHAPTER 12 DNS Configuration .....	135
Overview .....	135
CHAPTER 13 ErrDisable for Link-Flapping Configuration .....	137
Topology .....	137
Automatic Recovery .....	137
Log Message .....	138
Manual Recovery .....	138
Errdisable at the Interface Level .....	140
CHAPTER 14 Ethernet Interface Loopback Support Configurations .....	141
Overview .....	141
Local Loopback .....	141
Remote Loopback .....	142
Topology .....	142
CHAPTER 15 LAG with RTAG7 Hashing .....	151
Overview .....	151
Topology .....	151
Dynamic LAG with RTAG7 .....	151
Static LAG with RTAG7 .....	154
CHAPTER 16 Link Detection Debounce Timer .....	157
Log Messages .....	158
CHAPTER 17 Max Session and Session Limit Configuration .....	159
Overview .....	159
Configuration of SSH Server Session Limit Lesser than Max-Session .....	160
Configuration of Telnet Session Limit Greater than Max-Session .....	161
Configuration of SSH Session Limit Greater than Max-Session .....	162
CHAPTER 18 NTP Client Configuration .....	163
Overview .....	163
NTP Modes .....	163
NTP Configuration .....	164
Maxpoll and Minpoll Configuration .....	165
NTP Authentication .....	165
CHAPTER 19 Port Breakout Configuration .....	167
Overview .....	167
Terminology .....	167
Pre-Requisite .....	168
Configuring vlan-reservation .....	168
Unconfiguring vlan-reservation .....	168
Validation .....	169
Configuring Port Breakout 40G to 4x10G .....	169
Removing Port Breakout .....	169
Configuring Port Breakout (100G to 4x10G) .....	178
Configuring Port Breakout (100G to 4x25G) .....	179

---

Configuring Port Breakout (100G to 2x50G).....	180
Configuring Port Breakout at Global Configuration Level.....	181
CHAPTER 20 Proxy ARP and Local Proxy ARP .....	185
Overview .....	185
Local Proxy ARP Overview .....	186
CHAPTER 21 RADIUS Client Configuration .....	191
Overview .....	191
RADIUS Server Authentication.....	191
RADIUS Server Accounting .....	201
Sample Radius Clients.conf File.....	202
Sample Radius Users Configuration File .....	203
CHAPTER 22 sFlow Configuration .....	205
Overview .....	205
Configuration.....	206
Validation .....	206
CHAPTER 23 Show Tech Support Configurations.....	207
Overview .....	207
Tech Support Samples .....	207
Validation Commands .....	208
CHAPTER 24 Simple Network Management Protocol.....	209
Overview .....	209
Standard SNMP Configurations .....	210
Validation .....	210
CHAPTER 25 Software Monitoring and Reporting.....	213
Overview .....	213
Configuration.....	213
Validation .....	213
CHAPTER 26 SSH Client Server Configuration.....	215
Overview .....	215
Topology .....	215
Basic Configuration .....	215
SSH Keys.....	216
SSH Encryption Cipher .....	217
SSH Key Based Authentication .....	218
Topology .....	218
Public Key Authentication Method .....	218
Restrictions .....	220
CHAPTER 27 Syslog Configuration .....	223
Logging to a File .....	223
Logging to the Console .....	225
Logging to Remote Server.....	226
Configuration.....	227
Remote machine Syslog Configuration: .....	228

---

Monitoring Logging Server: .....	228
CHAPTER 24 Custom Syslog Port Configuration .....	231
Overview .....	231
Custom Syslog Configuration with IPv4 Address .....	231
Custom Syslog Configuration with IPv6 Address .....	234
Custom Syslog Configuration with HOSTNAME .....	236
CHAPTER 25 Telnet Configuration .....	239
Overview .....	239
Topology .....	239
Enable and Disable the Telnet Server .....	239
Configure the Telnet Server Port .....	239
Telnet Client Session .....	240
CHAPTER 26 TACACS Client Configuration .....	241
Overview .....	241
TACACS Server Authentication .....	241
TACACS Server Accounting .....	251
TACACS Server Authorization .....	253
CHAPTER 27 Traffic Mirroring Configuration .....	255
SPAN Overview .....	255
Port Mirroring Configuration .....	256
Port Mirroring Configuration .....	262
CHAPTER 28 Trigger Failover Configuration .....	267
Overview .....	267
Basic Configuration .....	267
Validation .....	268
Port-Channel Configuration .....	268
Validation .....	269
CHAPTER 29 User Configuration .....	271
Overview .....	271
CHAPTER 30 Using the Management Interface .....	273
Overview .....	273
Management Port .....	273
In-Band Ports .....	274
CHAPTER 31 Fault Management System Configuration .....	277
Implementation .....	278
Enabling and Disabling the Fault Management System .....	278
Alarm Configuration File .....	278
Auto Generating the Alarm Configuration File .....	279
Alarm Descriptions .....	281
CHAPTER 32 Erbium-Doped Fiber Amplifier (EDFA) Configuration .....	283
Overview .....	283
System Description .....	283
Objectives .....	284

---

---

Topology .....	284
CHAPTER 33 NetConf Call Home Configuration .....	287
Configuration .....	287
Validation .....	287
<b>System Management Command Reference .....</b>	<b>291</b>
CHAPTER 1 Access Control List Commands (Standard) .....	293
ip access-list standard .....	294
ip access-list standard filter .....	295
ipv6 access-list standard .....	296
ipv6 access-list standard filter .....	297
CHAPTER 2 Access Control List Commands (XGS) .....	299
access-list logging cache-size .....	301
access-list logging rate-limit .....	302
arp access-group .....	303
arp access-list .....	304
arp access-list filter .....	305
arp access-list remark .....	307
arp access-list resequence .....	308
arp access-list response .....	309
clear access-list .....	311
clear access-list log-cache .....	312
clear arp access-list .....	313
clear ip access-list .....	314
clear ipv6 access-list .....	315
clear mac access-list .....	316
ip access-group .....	317
ip access-list .....	320
ip access-list default .....	321
ip access-list filter .....	322
ip access-list fragments .....	325
ip access-list icmp .....	326
ip access-list remark .....	331
ip access-list resequence .....	332
ip access-list tcp udp .....	333
ipv6 access-group .....	338
ipv6 access-list .....	340
ipv6 access-list default .....	342
ipv6 access-list filter .....	343
ipv6 access-list fragments .....	346
ipv6 access-list icmpv6 .....	347
ipv6 access-list remark .....	351
ipv6 access-list resequence .....	352
ipv6 access-list sctp .....	353
ipv6 access-list tcp udp .....	356



---

line vty .....	362
mac access-group .....	363
mac access-list .....	365
mac access-list default .....	366
mac access-list filter .....	367
mac access-list remark .....	369
mac access-list resequence .....	370
show access-lists .....	371
show access-list log-cache .....	372
show arp access-lists .....	373
show ip access-lists .....	374
show ipv6 access-lists .....	375
show mac access-lists .....	376
show running-config aclmgr .....	377
show running-config access-list .....	378
show running-config ipv6 access-list .....	379
 CHAPTER 3 Authentication, Authorization and Accounting .....	 381
aaa authentication login .....	382
aaa accounting default .....	383
aaa authentication login console .....	384
aaa authentication login default .....	385
aaa authorization default .....	386
aaa authentication login console fallback error .....	387
aaa authentication login default fallback error .....	388
aaa group server .....	389
aaa local authentication attempts max-fail .....	390
aaa local authentication unlock-timeout .....	391
debug aaa .....	392
server .....	393
show aaa authentication .....	394
show aaa authentication login .....	395
show aaa authorization .....	396
show aaa groups .....	397
show aaa accounting .....	398
show running-config aaa .....	399
 CHAPTER 4 Basic Commands .....	 401
banner motd .....	403
clock timezone .....	404
clock set .....	405
configure terminal .....	406
configure terminal force .....	407
copy running-config startup-config .....	408
crypto pki generate rsa common-name ipv4 .....	409
debug nsm .....	410
disable .....	412
do .....	413

---

enable	414
enable password	415
end	416
exec-timeout	417
exit	418
help	419
history	420
hostname	421
line console	422
line vty (all line mode)	423
line vty (line mode)	424
logging cli	425
logout	426
max-session	427
ping	428
ping (interactive)	430
quit	432
reload	433
service advanced-vty	434
service password-encryption	435
service terminal-length	436
show clock	437
show cli	438
show cli history	439
show crypto csr	440
show debugging nsm	441
show list	442
show logging cli	443
show nsm client	444
show nsm forwarding-timer	445
show process	446
show running-config	447
show startup-config	448
show timezone	449
show users	452
show version	453
sys-reload	455
sys-shutdown	456
terminal length	457
terminal monitor	458
traceroute	459
write	460
write terminal	461
 CHAPTER 5 Chassis Management Module Commands	 463
cpu-core-usage	464
debug cmm	466

---

locator led	467
show hardware-information	468
show system-information	481
system-load-average	485
CHAPTER 6 Configuration Management	487
copy empty-config startup-config	488
copy running-config	489
copy running-config (interactive)	490
copy startup-config	491
copy startup-config (interactive)	492
copy system file	493
copy system file (interactive)	494
copy ftp startup-config	495
copy scp startup-config	496
copy sftp startup-config	497
copy tftp startup-config	498
copy http startup-config	499
copy ftp startup-config (interactive)	500
copy scp filepath	501
copy scp startup-config (interactive)	502
copy sftp startup-config (interactive)	503
copy tftp startup-config (interactive)	504
copy http startup-config (interactive)	505
copy file startup-config	506
CHAPTER 7 Control Plane Policing Commands	507
clear interface cpu counters	508
cpu-queue	509
show interface cpu counters queue-stats	511
show cpu-queue details	512
CHAPTER 8 Common Management Layer Commands	513
abort transaction	515
cancel-commit	516
cml force-unlock config-datastore	517
cml lock config-datastore	518
cml logging	519
cml netconf translation	520
cml notification	521
cml unlock config-datastore	522
cmlsh multiple-config-session	523
cmlsh notification	525
cmlsh transaction	526
cmlsh transaction limit	527
commit	528
confirm-commit	531
debug cml	532

---

module notification . . . . .	533
show cml config-datastore lock status . . . . .	534
show cml notification status . . . . .	535
show cmlsh multiple-config-session status . . . . .	536
show cmlsh notification status . . . . .	537
show max-transaction limit . . . . .	538
show module-info . . . . .	539
show running-config notification . . . . .	541
show system restore failures . . . . .	542
show transaction current . . . . .	543
show transaction last-aborted . . . . .	544
show (xml json) running-config candidate-config . . . . .	545
<b>CHAPTER 9 DHCP Snooping Commands . . . . .</b>	<b>549</b>
debug ip dhcp snooping . . . . .	550
ip dhcp snooping database . . . . .	551
renew ip dhcp snooping binding database . . . . .	552
show debugging ip dhcp snooping . . . . .	553
show ip dhcp snooping arp-inspection statistics bridge . . . . .	554
show ip dhcp snooping bridge . . . . .	555
show ip dhcp snooping binding bridge . . . . .	557
<b>CHAPTER 10 DHCPv6 Prefix delegation Commands . . . . .</b>	<b>559</b>
ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER . . . . .	560
ipv6 address PREFIX_FROM_SERVER X:X::X:X/M . . . . .	561
ipv6 address autoconfig . . . . .	562
show ipv6 dhcp interface . . . . .	563
<b>CHAPTER 11 Digital Diagnostic Monitoring Commands . . . . .</b>	<b>565</b>
clear ddm transceiver alarm . . . . .	566
clear ddm transceiver alarm all . . . . .	567
ddm monitor . . . . .	568
ddm monitor all . . . . .	569
ddm monitor interval . . . . .	570
debug ddm . . . . .	571
service unsupported-transceiver . . . . .	572
show controller details . . . . .	573
show supported-transceiver . . . . .	574
show interface transceiver details . . . . .	575
<b>CHAPTER 12 Dynamic Host Configuration Protocol Client . . . . .</b>	<b>577</b>
feature dhcp . . . . .	578
ip address dhcp . . . . .	579
ip dhcp client request . . . . .	580
ipv6 address dhcp . . . . .	581
ipv6 dhcp address-prefix-length . . . . .	582
ipv6 dhcp client request . . . . .	583
ipv6 dhcp client . . . . .	585
show ipv6 dhcp vendor-opts . . . . .	587

---

CHAPTER 13	Dynamic Host Configuration Protocol Relay	589
clear ip dhcp relay option statistics		590
clear ip dhcp relay statistics		591
ip dhcp relay (configure mode)		592
ip dhcp relay (interface mode)		593
ip dhcp relay address		594
ip dhcp relay address global		595
ip dhcp relay information option		596
ip dhcp relay information option always-on		597
ip dhcp relay information source-ip		598
ip dhcp relay (L3VPN)		599
ipv6 dhcp relay (configure mode)		600
ipv6 dhcp relay (interface mode)		601
ipv6 dhcp relay address		602
ipv6 dhcp relay address global		603
ipv6 dhcp relay subscriber-id		604
ipv6 dhcp relay (L3VPN)		605
show ip dhcp relay		606
show ip dhcp relay address		608
show ip dhcp relay option statistics		609
show ip dhcp relay statistics		610
show ipv6 dhcp relay		611
show ipv6 dhcp relay address		612
show running-config dhcp		613
CHAPTER 14	IP Source Guard Commands	615
hardware-profile filter ipsg		616
hardware-profile filter ipsg-ipv6		617
ip verify source dhcp-snooping-vlan		618
CHAPTER 14	Domain Name System	619
debug dns client		620
ip domain-list		621
ip domain-lookup		622
ip domain-name		623
ip host		624
ip name-server		625
show hosts		626
show running-config dns		628
CHAPTER 15	Interface Commands	629
admin-group		632
bandwidth		633
bandwidth-measurement static uni-available-bandwidth		634
bandwidth-measurement static uni-residual-bandwidth		635
bandwidth-measurement static uni-utilized-bandwidth		636
clear hardware-discard-counters		637
clear interface counters		638
clear interface cpu counters		639

---

clear interface fec . . . . .	640
clear ip prefix-list . . . . .	641
clear ipv6 neighbors . . . . .	642
clear ipv6 prefix-list . . . . .	643
debounce-time . . . . .	644
delay-measurement dynamic twamp . . . . .	645
delay-measurement a-bit-min-max-delay-threshold . . . . .	647
delay-measurement static . . . . .	648
delay-measurement a-bit-delay-threshold . . . . .	649
description . . . . .	650
duplex . . . . .	651
fec . . . . .	652
flowcontrol . . . . .	653
hardware-profile portmode . . . . .	655
if-arbiter . . . . .	656
interface . . . . .	657
ip address A.B.C.D/M . . . . .	658
ip address dhcp . . . . .	659
ip forwarding . . . . .	660
ip prefix-list . . . . .	661
ip proxy-arp . . . . .	663
ip remote-address . . . . .	664
ip unnumbered . . . . .	665
ip vrf forwarding . . . . .	666
ipv6 address . . . . .	667
ipv6 forwarding . . . . .	668
ipv6 prefix-list . . . . .	669
ipv6 unnumbered . . . . .	671
link-debounce-time . . . . .	672
load interval . . . . .	673
loopback . . . . .	674
loss-measurement uni-link-loss . . . . .	675
monitor speed . . . . .	676
monitor queue-drops . . . . .	677
monitor speed threshold . . . . .	678
mtu . . . . .	679
multicast . . . . .	681
show flowcontrol . . . . .	682
show hardware-discard-counters . . . . .	683
show interface . . . . .	685
show interface capabilities . . . . .	687
show interface counters . . . . .	689
show interface counters drop-stats . . . . .	692
show interface counters error-stats . . . . .	695
show interface counters (indiscard-stats outdiscard-stats) . . . . .	696
show interface counters protocol . . . . .	699
show interface counters queue-drop-stats . . . . .	700

---

show interface counters queue-stats . . . . .	701
show interface counters rate . . . . .	703
show interface counters speed . . . . .	705
show interface counters summary . . . . .	706
show interface fec . . . . .	708
show ip forwarding . . . . .	710
show ip interface . . . . .	711
show ip prefix-list . . . . .	713
show ip route . . . . .	714
show ip route A.B.C.D/M longer-prefixes . . . . .	716
show ip vrf . . . . .	725
show ipv6 forwarding . . . . .	726
show ipv6 interface brief . . . . .	727
show ipv6 route . . . . .	729
show ipv6 prefix-list . . . . .	731
show hosts . . . . .	732
show running-config interface . . . . .	734
show running-config interface ip . . . . .	736
show running-config interface ipv6 . . . . .	737
show running-config ip . . . . .	738
show running-config ipv6 . . . . .	739
show running-config prefix-list . . . . .	740
shutdown . . . . .	741
speed . . . . .	742
switchport . . . . .	744
switchport allowed ethertype . . . . .	745
switchport protected . . . . .	746
transceiver . . . . .	747
 CHAPTER 16 IP Service Level Agreements Commands . . . . .	 749
clear ip sla statistics . . . . .	750
frequency . . . . .	751
icmp-echo . . . . .	752
ip sla . . . . .	753
ip sla schedule . . . . .	754
show ip sla statistics . . . . .	755
show ip sla summary . . . . .	757
show running-config ip sla . . . . .	758
threshold . . . . .	759
timeout . . . . .	760
 CHAPTER 17 Linux Shell Commands . . . . .	 761
 CHAPTER 18 Network Time Protocol . . . . .	 763
clear ntp statistics . . . . .	764
debug ntp . . . . .	765
feature ntp . . . . .	766
ntp acl . . . . .	767

---

ntp authenticate . . . . .	768
ntp authentication-key . . . . .	769
ntp discard . . . . .	770
ntp enable . . . . .	771
ntp logging . . . . .	772
ntp master . . . . .	773
ntp master stratum . . . . .	774
ntp peer . . . . .	775
ntp request-key . . . . .	777
ntp server . . . . .	778
ntp source-interface . . . . .	780
ntp sync-retry . . . . .	781
ntp trusted-key . . . . .	782
show ntp authentication-keys . . . . .	783
show ntp authentication-status . . . . .	784
show ntp logging-status . . . . .	785
show ntp peer-status . . . . .	786
show ntp peers . . . . .	788
show ntp statistics . . . . .	789
show ntp trusted-keys . . . . .	791
show running-config ntp . . . . .	792
CHAPTER 19 RADIUS . . . . .	793
clear radius-server . . . . .	794
debug radius . . . . .	795
radius-server login host . . . . .	796
radius-server login host acct-port . . . . .	798
radius-server login host auth-port . . . . .	799
radius-server login host key . . . . .	800
radius-server login key . . . . .	802
radius-server login timeout . . . . .	803
show debug radius . . . . .	804
show radius-server . . . . .	805
show running-config radius . . . . .	807
CHAPTER 20 Secure Shell . . . . .	809
clear ssh host-key . . . . .	810
clear ssh hosts . . . . .	811
debug ssh server . . . . .	812
feature ssh . . . . .	813
show debug ssh-server . . . . .	814
show running-config ssh server . . . . .	815
show ssh host-key . . . . .	816
show ssh server . . . . .	818
show username . . . . .	819
ssh . . . . .	820
ssh6 . . . . .	821
ssh server algorithm encryption . . . . .	823



---

ssh keygen host . . . . .	825
ssh login-attempts . . . . .	826
ssh server port . . . . .	827
ssh server session-limit . . . . .	828
username sshkey . . . . .	829
username keypair . . . . .	830
CHAPTER 21 sFlow Commands . . . . .	831
clear sflow statistics . . . . .	832
debug sflow . . . . .	833
feature sflow . . . . .	834
sflow agent-ip . . . . .	835
sflow collector . . . . .	836
sflow poll-interval . . . . .	837
sflow sampling enable . . . . .	838
sflow sampling-rate . . . . .	839
show sflow . . . . .	840
show sflow interface . . . . .	842
show sflow statistics . . . . .	843
CHAPTER 22 Simple Network Management Protocol . . . . .	845
debug snmp-server . . . . .	847
show running-config snmp . . . . .	848
show snmp . . . . .	849
show snmp community . . . . .	850
show snmp context . . . . .	851
show snmp engine-id . . . . .	852
show snmp group . . . . .	853
show snmp host . . . . .	854
show snmp user . . . . .	855
show snmp view . . . . .	856
snmp context . . . . .	857
snmp-server community . . . . .	858
snmp-server community-map . . . . .	859
snmp-server contact . . . . .	860
snmp-server context . . . . .	861
snmp-server disable default . . . . .	862
snmp-server enable snmp . . . . .	863
snmp-server enable traps . . . . .	864
snmp-server engineID . . . . .	866
snmp-server group . . . . .	867
snmp-server host . . . . .	869
snmp-server location . . . . .	871
snmp-server smux-port-disable . . . . .	872
snmp-server tcp-session . . . . .	873
snmp-server user . . . . .	874
snmp-server view . . . . .	876

---

---

CHAPTER 23	Software Monitoring and Reporting	877
clear cores		878
copy core		879
copy techsupport		880
feature software-watchdog		881
show bootup-parameters		882
show cores		883
show running-config watchdog		884
show software-watchdog status		885
show system log		888
show system login		890
show system reboot-history		891
show system resources		892
show system uptime		894
show techsupport		895
show techsupport status		897
software-watchdog		898
software-watchdog keep-alive-time		900
CHAPTER 24	Syslog	901
Syslog Severities		902
Log File Rotation		903
clear logging logfile		905
feature rsyslog		906
log syslog		907
logging console		908
logging level		909
logging logfile		911
logging monitor		912
logging remote facility		913
logging remote server		914
logging timestamp		916
show logging		917
show logging last		919
show logging logfile		920
show logging logfile last-index		921
show logging logfile start-seqn end-seqn		922
show logging logfile start-time end-time		923
show running-config logging		924
CHAPTER 25	System Configure Mode Commands	925
delay-profile interfaces		926
delay-profile interfaces subcommands		927
forwarding custom-profile		929
forwarding profile		931
hardware-profile filter (XGS)		932
hardware-profile filter (Qumran)		934
hardware-profile flowcontrol (Qumran)		935

---

hardware-profile statistics (Qumran) .....	936
load-balance enable .....	937
load-balance rtag7 .....	939
load-balance rtag7 hash .....	942
load-balance rtag7 macro-flow .....	943
show forwarding profile limit .....	944
show hardware-profile filters .....	946
snmp restart .....	948
<b>CHAPTER 26 TACACS+ .....</b>	<b>949</b>
add policy .....	950
clear tacacs-server counters .....	951
debug tacacs+ .....	952
default .....	953
deny .....	954
feature dynamic-rbac .....	955
feature tacacs+ .....	956
permit .....	957
policy .....	958
role .....	959
show debug tacacs+ .....	960
show rbac-policy .....	961
show rbac-role .....	962
show running-config tacacs+ .....	963
show tacacs-server .....	964
tacacs-server login host .....	966
tacacs-server login key .....	968
tacacs-server login timeout .....	969
<b>CHAPTER 27 Telnet .....</b>	<b>971</b>
debug telnet server .....	972
feature telnet .....	973
show debug telnet-server .....	974
show running-config telnet server .....	975
show telnet-server .....	976
telnet .....	977
telnet6 .....	978
telnet server port .....	979
telnet server session-limit .....	980
<b>CHAPTER 28 Time Range Commands .....</b>	<b>981</b>
end-time (absolute) .....	982
end-time after (relative) .....	983
frequency .....	984
frequency days (specific days) .....	985
start-time (absolute) .....	986
start-time after (relative) .....	987
start-time now (current) .....	988

---

---

time-range .....	989
CHAPTER 29 Traffic Mirroring Commands .....	991
monitor session .....	992
monitor session shut .....	993
source port .....	994
source vlan .....	995
destination port .....	996
no shut .....	997
shut .....	998
filter .....	999
description .....	1001
remote destination .....	1002
show monitor .....	1003
show monitor session .....	1005
show filter .....	1008
show monitor running configuration .....	1009
CHAPTER 30 Trigger Failover Commands .....	1011
clear tfo counter .....	1012
fog .....	1013
fog tfo .....	1014
fog type .....	1015
link-type .....	1016
show tfo .....	1017
tfo .....	1019
CHAPTER 31 User Management .....	1021
clear aaa local user lockout username .....	1022
clear line .....	1023
clear user .....	1024
debug user-mgmt .....	1025
show user-account .....	1026
username .....	1027
CHAPTER 32 VLOG Commands .....	1029
show vlog all .....	1030
show vlog clients .....	1031
show vlog terminals .....	1032
show vlog virtual-routers .....	1033
CHAPTER 33 FMS Command Reference .....	1035
fault-management (enable   disable) .....	1036
fault-management close .....	1037
fault-management flush-db .....	1038
fault-management shelve .....	1039
show alarm active .....	1040
show alarm closed .....	1041
show alarm history .....	1042
show alarm shelved .....	1043

---

---

show alarm statistics .....	1044
show alarm transitions.....	1045
show fms status .....	1046
show fms supported-alarm-types.....	1047
show running-config fault-management .....	1048
<b>CHAPTER 34 NetConf Call Home Commands .....</b>	<b>1049</b>
callhome server .....	1050
debug callhome .....	1052
feature netconf callhome.....	1053
management-port.....	1054
netconf callhome .....	1055
reconnect.....	1056
retry-interval .....	1058
retry-max-attempts.....	1060
show (xml) running-config netconf-callhome.....	1062
<b>CHAPTER 35 Internet Protocol Security Commands.....</b>	<b>1063</b>
crypto ipsec transform-set.....	1064
crypto map (Configure Mode).....	1066
mode .....	1067
set peer (Sequence mode).....	1068
set session-key (Sequence mode) .....	1069
set transform-set (Sequence mode) .....	1070
sequence.....	1071
show crypto ipsec transform-set .....	1072
<b>CHAPTER 36 Erbium-doped Fiber Amplifier Commands .....</b>	<b>1073</b>
edfa operating-mode .....	1074
edfa target-gain.....	1075
edfa target-outpwr .....	1076
show edfa operating-mode .....	1077
show interface IFNAME transceiver detail .....	1078
show interface IFNAME transceiver threshold violations .....	1080
show interface IFNAME transceiver .....	1081
show interface transceiver .....	1083
show interface transceiver detail .....	1084
show interface transceiver threshold violations .....	1085
<b>Index .....</b>	<b>1087</b>



# Preface

This guide describes how to configure OcNOS.

## IP Maestro Support

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

## Audience

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

## Conventions

[Table P-1](#) shows the conventions used in this guide.

**Table P-1: Conventions**

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

## Chapter Organization

The chapters in command references are organized as described in [Command Description Format](#).

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

## Related Documentation

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

---

## Migration Guide

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

---

## Feature Availability

The features described in this document that are available depend upon the OcNOS SKU that you purchased. See the *Feature Matrix* for a description of the OcNOS SKUs.

---

## Support

For support-related questions, contact [support@ipinfusion.com](mailto:support@ipinfusion.com).

---

## Comments

If you have comments, or need to report a problem with the content, contact [techpubs@ipinfusion.com](mailto:techpubs@ipinfusion.com).



# 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.

## 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 (see also 'undebug')
  etherchannel           LACP etherchannel
  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 (see also 'undebug')
```

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
```

---

## 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 authent
ication-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 P-2](#) describes the conventions used to represent command syntax in this reference.

**Table P-2: Syntax conventions**

Convention	Description	Example
monospaced font	Command strings entered on a command line	<code>show ip ospf</code>
lowercase	Keywords that you enter exactly as shown in the command syntax.	<code>show ip ospf</code>
UPPERCASE	See <a href="#">Variable Placeholders</a>	<code>IFNAME</code>
( )	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.	<code>(A.B.C.D &lt;0-4294967295&gt;)</code>
( )	Optional parameters, from which you select one or none. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	<code>(A.B.C.D &lt;0-4294967295&gt; )</code>
( )	Optional parameter which you can specify or omit. Do not enter the parentheses or vertical bar as part of the command.	<code>(IFNAME )</code>
{ }	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.	<code>{intra-area &lt;1-255&gt; inter-area &lt;1-255&gt; external &lt;1-255&gt;}</code>

**Table P-2: Syntax conventions (Continued)**

Convention	Description	Example
[ ]	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 P-3 shows the tokens used in command syntax use to represent variables for which you supply a value.

**Table P-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
XX:XX:XX:XX:XX:XX	MAC address
<1-5> <1-65535> <0-2147483647> <0-4294967295>	Numeric range

---

## Command Description Format

Table P-4 explains the sections used to describe each command in this reference.

**Table P-4: Command descriptions**

Section	Description
<b>Command Name</b>	The name of the command, followed by what the command does and when should it be used
<b>Command Syntax</b>	The syntax of the command
<b>Parameters</b>	Parameters and options for the command
<b>Default</b>	The state before the command is executed
<b>Command Mode</b>	The mode in which the command runs; see <a href="#">Command Modes</a>
<b>Example</b>	An example of the command being executed

---

## Keyboard Operations

Table P-5 lists the operations you can perform from the keyboard.

**Table P-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
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

**Table P-5: Keyboard operations (Continued)**

Key combination	Operation
Ctrl+t	Transposes the current character with the previous character
Ctrl+c	Ignores the current line and redisplay 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

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[3-4]

...skipping
```

```

interface xe3
 shutdown
!
interface xe4
 shutdown
!
interface svlan0.1
 no shutdown
!
route-map myroute permit 3
!
route-map mymap1 permit 10
!
route-map rmap1 permit 3
!
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 P-6](#) apply for all string parameters used in OcNOS commands, unless some other restrictions are noted for a particular command.

**Table P-6: String parameter restrictions**

Restriction	Description
Input length	1965 characters or less
Restricted special characters	"?", " ", ">", " ", and "=" The " " is allowed only for <code>description</code> CLI in interface mode.

---

## Command Modes

Commands are grouped into modes arranged in a hierarchy. Each mode has its own set of commands. [Table P-7](#) lists the command modes common to all protocols.

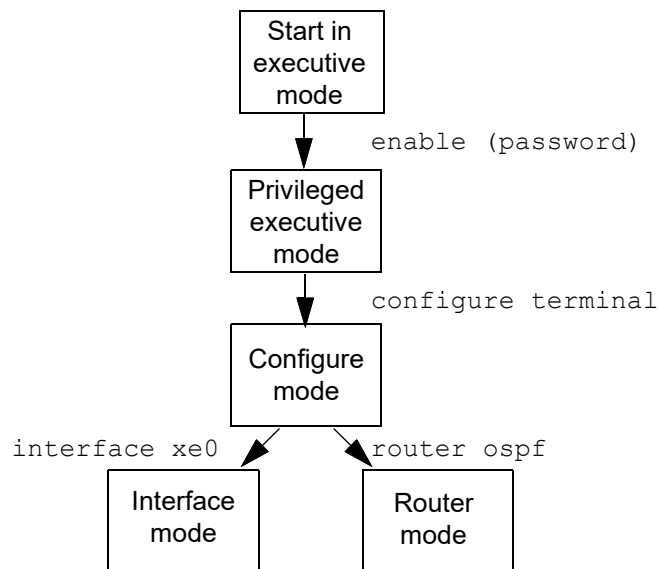
**Table P-7: Common command modes**

Name	Description
Executive mode	Also called <i>view</i> 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 <code>show</code> , <code>exit</code> , <code>quit</code> , <code>help</code> , and <code>enable</code> .
Privileged executive mode	Also called <i>enable</i> mode, in this mode you can run additional basic commands such as <code>debug</code> , <code>write</code> , and <code>show</code> .
Configure mode	Also called <i>configure terminal</i> 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.

---

## Command Mode Tree

The diagram below shows the common command mode hierarchy.



**Figure P-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 `commit` 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 commit. 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.



# System Management Configuration Guide



## CHAPTER 1 Access Control Lists Configurations

This chapter contains a complete example of access control list (ACL) configuration.

### Overview

An Access Control List is a list of Access Control Entries (ACE). Each ACE in ACL specifies the access rights allowed or denied.

Each packet that arrives at the device is compared to each ACE in each ACL in the order they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

**Note:** If there is no match, the packet is dropped (implicit deny). Therefore, an ACL intended to deny a few selected packets should have at least one permit filter of lower priority; otherwise, all traffic is dropped because of the default implicit deny filter.

### Topology

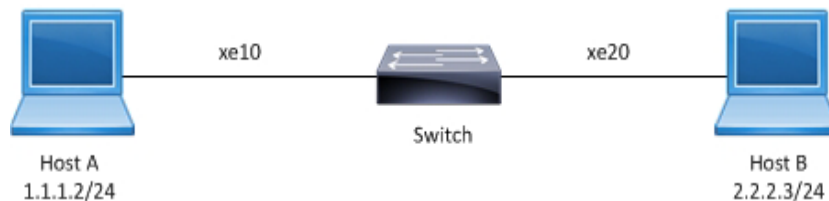


Figure 1-1: ACL sample topology

### IPv4 ACL Configuration

#configure terminal	Enter configure mode.
(config)#ip access-list T1	Create an IP access list named T1.
(config-ip-acl)#deny any host 1.1.1.1 any	Create an access rule to deny IP packets with source address 1.1.1.1.
(config-ip-acl)#permit any host 1.1.1.1 any	Create an access rule to permit IP packets with source address 1.1.1.1.
(config-ip-acl)#exit	Exit access list mode.
(config)#interface xe10	Enter interface mode.
(config-if)#no switchport	Configure the interface as Layer 3.
(config-if)#ip address 1.1.1.3/24	Assign an IP address.
(config-if)#ip access-group T1 in	Apply access group T1 for inbound traffic to the interface.
(config-if)#exit	Exit interface and configure mode.

## Validation

Use the commands below to verify the match count. When inbound IP packets reach interface xe10 with source address 1.1.1.1, then the match count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists T1
  IP access list T1
    10 deny any host 1.1.1.1 any [match=200]
    20 permit any 1.1.1.1/24 any
    default deny-all
```

When inbound IP packets reach interface xe10 with a source address in the range from 1.1.1.1 to 1.1.1.254, then the match count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists T1
  IP access list T1
    10 deny any host 1.1.1.1 any
    20 permit any 1.1.1.1/24 any [match=2000]
    default deny-all
```

**Note:** Use the command `clear ip access-list counters` to clear the statistics of all ACLs or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

## ICMP ACL Configuration

#configure terminal	Enter configure mode.
(config)#ip access-list icmp-acl-01	Create an IP access list named icmp-acl-01.
(config-ip-acl)#deny icmp 1.1.1.1/24 2.2.2.2/24 dscp af11	Create an access rule with sequence number 10 to deny ICMP packets from a specific source towards a specific destination with a DSCP value of af11. Note: The sequence number is optional.
(configip-acl)#20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash	Create an access rule with sequence number 20 to permit ICMP packets from a specific source towards a specific destination with precedence as flash.
(config-ip-acl)#exit	Exit access list mode.
(config)#interface xe10	Enter interface mode.
(config-if)#no switchport	Configure the interface as Layer 3.
(config-if)#ip address 1.1.1.3/24	Assign an IP address.
(config-if)#ip access-group icmp-acl-01 in	Apply access group icmp-acl-01 for inbound traffic to the interface.
(config-if)#exit	Exit interface and configure mode.

## Validation

Use the commands below to verify the match count. When inbound IP packets reach interface xe10 with source address 1.1.1.X, destination address 2.2.2.X, DSCP value af11, and are fragmented, then the count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists icmp-acl-01
  IP access-list icmp-acl-01
    deny icmp 1.1.1.1/24 2.2.2.2/24 precedence flash [match=200]
```



```
20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
default deny-all
```

When inbound IP packets reach interface xe10 with source address as 1.1.1.X, destination address 2.2.2.X, and precedence value flash, then the count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists icmp-acl-01
IP access-list icmp-acl-01
  deny icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
  20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash [match=200]
  default deny-all
```

**Note:** Use the command `clear ip access-list counters` to clear statistics of all ACLs configured or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

## Access List Entry Sequence Numbering

You can change the sequence numbers of rules in an access list.

**Note:** Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

#configure terminal	Enter configure mode.
(config)#ip access-list icmp-acl-01	Enter access list mode for ACL icmp-acl-01.
(config-ip-acl)#resequence 100 200	Re-sequence the access list, starting with sequence number 100 and incrementing by 200.
(config-ip-acl)#1000 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11	Re-sequencing specific access rule 100 with sequence number 1000
(config-ip-acl)#exit	Exit access list mode.

## Validation

Before re-sequencing:

```
#show access-lists icmp-acl-01
IP access list icmp-acl-01
  deny icmp 1.1.1.1/24 2.2.2.2/24 precedence flash log
  20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
  default deny-all
```

After re-sequencing the access list, starting with sequence number 100 and incrementing by 200

```
#show access-lists icmp-acl-01
IP access list icmp-acl-01
  100 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
  300 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
  default deny-all
```

After re-sequencing specific access rule 100 with sequence number 1000

```
#show access-lists icmp-acl-01
IP access list icmp-acl-01
  300 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
  1000 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
  default deny-all
```

## IPv6 ACL Configuration

#configure terminal	Enter configure mode.
(config)#ipv6 access-list ipv6-acl-01	Create an IPv6 access list named as icmp-acl-01.
(config-ipv6-acl)#11 deny ipipv6 any any flow-label 100	Create access rule sequence number 11 to deny IPv4 encapsulated packets in IPv6 with any source address to any destination address with flow label 100.
(config-ipv6-acl)#default permit-all	Update the default rule to permit all.
(config-ipv6-acl)#exit	Exit access list mode
(config)#interface xe10	Enter interface mode.
(config-if)#no switchport	Configure the interface as Layer 3.
(config-if)#ipv6 address 1::1:3/64	Assign an IPv6 address.
(config-if)#ipv6 access-group ipv6-acl-01 in	Apply access group ipv6-acl-01 for inbound traffic to the interface.
(config-if)#exit	Exit interface and configure mode.

## Validation

Use the commands below to verify the match count. When inbound IPv6 packets reach interface xe10 with IPv4 packets encapsulated with flow label 100, then count for access rule 11 increases equal to the number of packets sent.

```
#show ipv6 access-lists ipv6-acl-01
IPv6 access-list ipv6-acl-01
  11 deny ipipv6 any any flow-label 100 [match=1000]
  default permit all
```

For all other IPv6 packets, access rule 100 is invoked and the match counts increase equal to the number of packets sent.

```
#show ipv6 access-lists ipv6-acl-01
IPv6 access-list ipv6-acl-01
  11 deny ipipv6 any any flow-label 100
  default permit-all [match=2000]
```

**Note:** Use the command `clear ipv6 access-list counters` to clear statistics of all IPv6 ACLs configured or `clear ipv6 access-list <ipv6 access-list name> counters` to clear statistics of the particular IPv6 ACL.

## MAC ACL Configuration

#configure terminal	Enter configure mode.
(config)#mac access-list mac-acl-01	Create a MAC access list named mac-acl-01.
(config-mac-acl)#22 permit host 0000.0011.1212 host 0000.1100.2222 vlan 2	Create an access rule with sequence number 22 to permit packets from a host with a specific MAC towards a host with a specific MAC with VLAN 2.
(config-mac-acl)#exit	Exit access list mode.

(config)#bridge 1 protocol rstp vlan-bridge	Create a VLAN-aware RSTP bridge.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface xe10	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2.
(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)#mac access-group mac-acl-01 in	Applies the MAC access list mac-acl-01 to ingress traffic.
(config-if)#exit	Exit interface and configure mode.

## Validation

Use the commands below to verify the match count. When inbound packets reach interface xe10 with the specific source and destination MAC with the VLAN as 2, then the count for access rule 22 increases equal to the number of packets sent.

```
#show mac access-lists
    MAC access list mac-acl-01
      22 permit mac host 0000.0011.1212 host 0000.1100.2222 vlan 2 [match=3000]
      default deny-all
```

For all other packets, default rule is invoked and the match counts increases equal to the number of packets sent.

```
#show mac access-lists mac-acl-01
    MAC access list mac-acl-01
      22 permit mac host 0000.0011.1212 host 0000.1100.2222 vlan 2
      default deny-all [match=2000]
```

**Note:** As per the present design, ARP/ND packets will be filtered based on the source MAC address only (host mac address).

**Note:** Use the command `clear mac access-list counters` to clear statistics of all MAC ACLs or `clear mac access-list <mac access-list name> counters` to clear statistics of a particular MAC ACL.

## Management ACL Overview

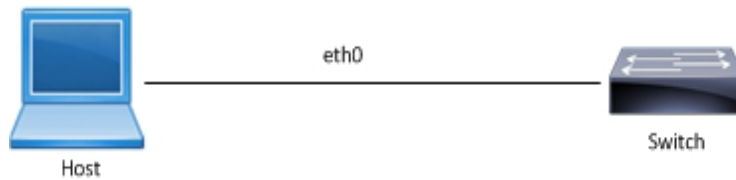
Management Port ACL can be used to provide basic level of security for accessing the management network. ACLs can also be used to decide which types of management traffic to be forwarded or blocked at the management port.

When configuring access list on a router or a switch, each access list needs to be identified by a unique name or a number. Each access list entry can have permit or deny actions. Each entry will be associated with a sequence number in the range of <1-268435453>. Lower the sequence number, higher the priority.

User should be able to configure the system to allow certain IP address for a protocol and don't allow any other IP address matching for that protocol.

**Note:** If there is no match, the packet is dropped (implicit deny). Therefore, an ACL intended to deny a few selected packets should have at least one permit filter of lower priority; otherwise, all traffic is dropped because of the default implicit deny filter.

## Topology



**Figure 1-2: Management ACL Sample Topology**

## Management ACL Configuration

#configure terminal	Enter configure mode.
(config)#ip access-list mgmt	Create an IP access list named mgmt
(config-ip-acl)#permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh	Create an access rule to permit TCP connection with source address 10.12.45.57 with destination address 10.12.29.49 on destination port equal to SSH.
(config-ip-acl)#permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet	Create an access rule to permit TCP connection with source address 10.12.45.58 with Destination address 10.12.29.49 on destination port equal to Telnet.
(config-ip-acl)#permit udp any host 10.12.29.49 eq snmp	Create an access rule to permit UDP packet with any source address with Destination address 10.12.29.49 on destination port equal to SNMP.
(config-ip-acl)#permit udp any host 10.12.29.49 eq ntp	Create an access rule to permit UDP packet with any source address with Destination address 10.12.29.49 on destination port equal to NTP.
(config-ip-acl)#permit udp host 10.12.29.49 any eq snmptrap	Create an access rule to permit UDP packet with source address 10.12.29.49 with any Destination address on destination port equal to SNMPTrap.
(config-ip-acl)#permit tcp host 10.12.29.49 eq ssh host 10.12.45.57	Create an access rule to permit TCP connection with source address 10.12.29.49 on source port equal to ssh with Destination address 10.12.45.57.
(config-ip-acl)#deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh	Create an access rule to deny TCP connection with source address 10.12.45.58 with Destination address 10.12.29.49 on destination port equal to SSH.
(config-ip-acl)# deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet	Create an access rule to deny TCP connection with source address 10.12.45.57 with Destination address 10.12.29.49 on destination port equal to Telnet.
(config-ip-acl)#exit	Exit access list mode.
(config)#interface eth0	Enter interface mode of Management Interface.
(config-if)#no switchport	Configure the interface as Layer 3.
(config-if)#ip address 10.12.29.49/24	Assign an IP address.
(config-if)#ip access-group mgmt in	Apply access group mgmt for inbound traffic to the interface.
(config-if)#exit	Exit interface and configure mode.

## Validation

Use the commands below to verify the match count. When a TCP connection for Destination Port SSH reach interface eth0 with source address 10.12.45.57, then the match count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
  IP access list mgmt
    10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh [match=9]
    20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
    30 permit udp any host 10.12.29.49 eq snmp
    40 permit udp any host 10.12.29.49 eq ntp
    50 permit udp host 10.12.29.49 any eq snmptrap
    60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
    70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
    80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
    default deny-all
```

When a TCP connection for Destination Port Telnet reach interface eth0 with source address 10.12.45.58, then the match count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
  IP access list mgmt
    10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
    20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet [match=10]
    30 permit udp any host 10.12.29.49 eq snmp
    40 permit udp any host 10.12.29.49 eq ntp
    50 permit udp host 10.12.29.49 any eq snmptrap
    60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
    70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
    80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
    default deny-all
```

When a UDP packet for Destination Port SNMP reach interface eth0 with any source address, then the match count for access rule 30 increases equal to the number of packets sent. Prior to this SNMP should be configured on Device (10.12.29.49).

Example:

```
snmp-server community SNMPTEST group network-admin vrf management
snmp-server host 10.12.6.86 traps version 2c SNMPTEST udp-port 162 vrf
management
snmp-server enable snmp vrf management
```

```
#show ip access-lists mgmt
  IP access list mgmt
    10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
    20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
    30 permit udp any host 10.12.29.49 eq snmp [match=50]
    40 permit udp any host 10.12.29.49 eq ntp
    50 permit udp host 10.12.29.49 any eq snmptrap
    60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
    70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
    80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
    default deny-all
```

When a UDP packet for Destination Port NTP reach interface eth0 with any source address, then the match count for access rule 40 increases equal to the number of packets sent. Prior to this NTP should be configured on Device (10.12.29.49).

Example:

```
ntp enable vrf management
ntp authenticate vrf management
ntp authentication-key 123 md5 swwx 7 vrf management
ntp trusted-key 123 vrf management
ntp server 10.12.45.36 vrf management
ntp server 10.12.16.16 prefer vrf management
ntp server 10.12.16.16 key 123 vrf management
```

```
#show ip access-lists mgmt
IP access list mgmt
 10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
 20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
 30 permit udp any host 10.12.29.49 eq snmp
 40 permit udp any host 10.12.29.49 eq ntp [match=1]
 50 permit udp host 10.12.29.49 any eq snmptrap
 60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
 70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
 80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
default deny-all
```

When a TCP connection request for Destination Port SSH reach interface eth0 with source address 10.12.45.58, this should deny the connection and the match count for access rule 70 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
IP access list mgmt
 10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
 20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
 30 permit udp any host 10.12.29.49 eq snmp
 40 permit udp any host 10.12.29.49 eq ntp
 50 permit udp host 10.12.29.49 any eq snmptrap
 60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
 70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh [match=1]
 80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
default deny-all
```

When a TCP connection request for Destination Port Telnet reach interface eth0 with source address 10.12.45.57, this should deny the connection and the match count for access rule 80 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
IP access list mgmt
 10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
 20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
 30 permit udp any host 10.12.29.49 eq snmp
 40 permit udp any host 10.12.29.49 eq ntp
 50 permit udp host 10.12.29.49 any eq snmptrap
 60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
 70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
 80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet [match=1]
default deny-all
```

To enable SNMPTRAPS, apply the ACL outbound to the Management interface.

#configure terminal	Exit access list mode.
(config)#interface eth0	Enter interface mode of Management Interface.
(config-if)#ip access-group mgmt out	Apply access group mgmt for outbound traffic to the interface.
(config-if)#exit	Exit interface and configure mode.

When a UDP packet for Destination Port SNMPTrap sends out of interface eth0 with any Destination address, then the match count for access rule 50 increases equal to the number of packets received. Prior to this SNMPTrap should be configured on Device (10.12.29.49) to listen to port 162.

Example:

```
snmp-server community SNMPTEST group network-admin vrf management
snmp-server host 10.12.6.86 traps version 2c SNMPTEST udp-port 162 vrf
management
snmp-server enable snmp vrf management
```

```
#show ip access-lists mgmt
```

```
IP access list mgmt
 10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
 20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
 30 permit udp any host 10.12.29.49 eq snmp
 40 permit udp any host 10.12.29.49 eq ntp
 50 permit udp host 10.12.29.49 any eq snmptrap [match=5]
 60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
 70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
 80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
default deny-all
```

When an ACL is applied on interface eth0 outbound and inbound together, then we must configure an ACL to establish a TCP connection between source 10.12.29.49 with source Port SSH to destination address 10.12.45.57. When a TCP connection is established on port SSH, then the match count for access rule 10 and 60 increases equal to the number of packets sent and received.

```
#show ip access-lists mgmt
```

```
IP access list mgmt
 10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh [match=9]
 20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
 30 permit udp any host 10.12.29.49 eq snmp
 40 permit udp any host 10.12.29.49 eq ntp
 50 permit udp host 10.12.29.49 any eq snmptrap
 60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57 [match=9]
 70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
 80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
default deny-all
```

**Note:** Use the command `clear ip access-list counters` to clear the statistics of all ACLs or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

```
#show access-lists
```

```
IP access list mgmt
 10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
 20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
 30 permit udp any host 10.12.29.49 eq snmp
 40 permit udp any host 10.12.29.49 eq ntp
 50 permit udp host 10.12.29.49 any eq snmptrap
 60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
 70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
 80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
```

```
#show access-lists summary
```

```
IPV4 ACL mgmt
  statistics enabled
  Total ACEs Configured: 8
  Configured on interfaces:
```

```
eth0 - ingress (Router ACL)
Active on interfaces:
eth0 - ingress (Router ACL)

#show access-lists expanded
IP access list mgmt
10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
30 permit udp any host 10.12.29.49 eq snmp
40 permit udp any host 10.12.29.49 eq ntp
50 permit udp host 10.12.29.49 any eq snmptrap
60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
default deny-all [match=4]
```

## ARP ACL Overview

ARP ACL can be used to permit or deny the ARP packets, based on the ARP request or response option configured.

### Topology

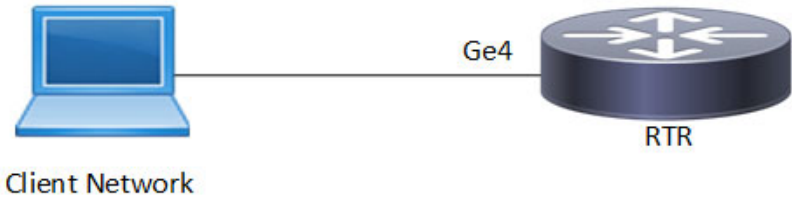


Figure 1-3: ARP ACL Sample Topology

## ARP ACL Configuration

#configure terminal	Enter configure mode.
(config)#interface ge4	Enter interface mode.
(config-if)#ip address 11.11.11.11/24	Assign IPv4 address.
(config-if)#exit	Exit access list mode.
(config)# mac access-list mac1	Enter mac access list mode.
(config-mac-acl)#permit 0000.3ae0.456d 0000.0000.0000 any arp request	Create an access rule to permit specific ARP request.
(config-mac-acl)#permit 0000.3ae0.456d 0000.0000.0000 any arp response	Create an access rule to permit specific ARP response.
(config-mac-acl)#permit any any ipv4	Create an access rule to permit any IPv4 packet.
(config-mac-acl)#exit	Exit access list mode.
(config)#interface ge4	Enter interface mode.



(config-if)#mac access-group mac1 in	Apply access group mac1 for inbound traffic to the interface.
(config-if)#exit	Exit interface and configure mode.

## Validation

Use the commands below to assign IP address on IXIA and ping from IXIA.

```
#show mac access-lists
    MAC access list mac1
      10 permit host 0000.3AE0.456D any arp request [match=1]
      20 permit host 0000.3AE0.456D any arp response [match=1]
      30 permit any any ipv4 [match=1]
      default deny-all
```

## ACL OVER LOOPBACK

The loopback interface ACL is the feature to be used to provide this basic level security for the management applications accessible through In-band interfaces.

Note: Refer to the command reference section for limitations, default behavior, and unsupported features.

## Topology

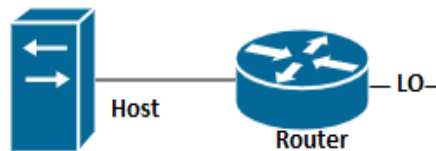


Figure 1-4: ACL Loopback Topology

## Loopback ACL Configuration

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 3.3.3.3/32 secondary	Assign the IPv4 secondary address.
(config-if)#ip address 4.4.4.4/32 secondary	Assign the IPv4 secondary address.
(config-if)#ip address 5.5.5.5/32 secondary	Assign the IPv4 secondary address.
(config-if)#ip address 6.6.6.6/32 secondary	Assign the IPv4 secondary address.
(config-if)#ip address 7.7.7.7/32 secondary	Assign the IPv4 secondary address.
(config-if)# exit	Exit interface mode.

## Access Control Lists Configurations

(config)#ip access-list loopback	Create loopback access list
(config-ip-acl)# 10 permit tcp any host 3.3.3.3 eq telnet	Permit telnet session from any source with specific destination.
(config-ip-acl)# 20 deny tcp any host 4.4.4.4 eq telnet	Deny telnet session from any source with specific destination.
(config-ip-acl)# 30 permit tcp any host 5.5.5.5 eq ssh	Permit ssh session from any source with specific destination.
(config-ip-acl)# 40 deny tcp any host 6.6.6.6 eq ssh	Deny ssh session from any source with specific destination.
(config-ip-acl)# 50 deny udp any host 6.6.6.6 eq snmp	Deny udp from any source with specific destination.
(config-ip-acl)# 60 deny udp any host 7.7.7.7 eq ntp	Deny udp from any source with specific destination.
(config-ip-acl)#exit	Exit interface acl mode
(config)#interface lo	Enter interface lo mode
(config-if)#ip access-group loopback in	Associate loopback acl over lo interface
(config-if)#exit	Exit interface mode
(config)#exit	Exit config mode

## Validation

Use the commands below to validate ACL loopback.

```
OcNOS#show access-lists
IP access list loopback
    10 permit tcp any host 3.3.3.3 eq telnet [match=12]
    20 deny tcp any host 4.4.4.4 eq telnet [match=12]
    30 permit tcp any host 5.5.5.5 eq ssh
    40 deny tcp any host 6.6.6.6 eq ssh
    50 deny udp any host 6.6.6.6 eq snmp [match=6]
    60 deny udp any host 7.7.7.7 eq ntp
```

```
OcNOS#show ip access-lists summary
IPV4 ACL loopback
    statistics enabled
    Total ACEs Configured: 6
    Configured on interfaces:
        lo - ingress (Router ACL)
    Active on interfaces:
        lo - ingress (Router ACL)
    Configured on line vty:
```

```
OcNOS#show running-config aclmgr
ip access-list loopback
    10 permit tcp any host 3.3.3.3 eq telnet
    20 deny tcp any host 4.4.4.4 eq telnet
    30 permit tcp any host 5.5.5.5 eq ssh
    40 deny tcp any host 6.6.6.6 eq ssh
    50 deny udp any host 6.6.6.6 eq snmp
    60 deny udp any host 7.7.7.7 eq ntp
!
interface lo
    ip access-group loopback in
!
```

---

## ACL OVER VTY

When a Telnet/SSH/NetConf connection is established in the OcNOS, it associates the connection with a virtual terminal (VTY) line. The ACL over VTY feature provides security for management features associated with VTY.

Users can create Standard and Extended ACL rules and attach them to a virtual teletype (VTY) command line interface. These ACL rules are applied on both Management and Default virtual routing forwarding (VRFs).

OcNOS supports both IPv4 and IPv6 access lists for VTY lines, providing flexibility for network configurations.

Applying a standard ACL rule on a VTY line permits or denies only management access protocols such as SSH, Telnet, and SSH-Netconf protocols (port numbers 22,23,830)).

Extended ACL rules are applied as configured by the user, and it is not limited to management protocols only, unlike Standard ACLs.

When a user configures a rule with 'deny any any any' and attaches it to the VTY, it effectively blocks only the Telnet, SSH, and NetConf protocols on the control plane

For example, when a user configures a rule as below and attach them to VTY, If the deny ACL rule includes 'any' value in protocol, only Telnet/SSH/SSH-NetConf protocols are denied.

```
ip access-list ssh-access
10 permit tcp 10.12.43.0/24 any eq ssh
20 deny any any any
```

**Note:** To deny any protocols other than Telnet/SSH/SSH-Netconf, create a deny rule with the specific protocol access on VTY. For example: To deny OSPF protocol from all the source and destination address, apply the rule, 10 deny ospf any any.

In general, the VTY ACLs are more specific to management protocols. Hence, the Extended ACL “any” rule translation is enhanced to allow management protocols as follows:

- If the **deny** ACL rule includes any value in protocol, only Telnet/SSH/SSH-Netconf protocols are denied.
- The **permit** ACL rule is unchanged.

**Note:** Refer to the command reference section for limitations, default behavior, and unsupported features.

**Note:** This feature allows the customer to define a Extended ACL deny rule only to the management protocol without impacting other control protocols.

**Note:** Configure a separate Extended ACL deny rule to deny protocols other than Telnet, SSH, and NetConf.

---

## Topology

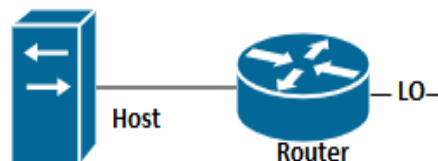


Figure 1-5: ACL VTY Topology

---

## VTY ACL Configuration

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 3.3.3.3/32 secondary	Assign the IPv4 secondary address.
(config-if)# exit	Exit interface mode.
(config)#ip access-list vty	Create loopback access list
(config-ip-acl)# 10 permit tcp any host 3.3.3.3 eq telnet	Permit telnet session from any source with specific destination.
(config-ip-acl)#exit	Exit interface acl mode
(config)#line vty	Enter interface vty mode
(config-all-line)#ip access-group vty in	Associate acl over
(config-if)#exit	Exit interface mode
(config)#exit	Exit config mode

## Validation

```
OcNOS#sh access-lists
IP access list vty
    10 permit tcp any host 3.3.3.3 eq telnet
```

```
OcNOS#sh ip access-lists summary
IPV4 ACL vty
    statistics enabled
    Total ACEs Configured: 1
    Configured on interfaces:
    Active on interfaces:
    Configured on line vty:
    all vty lines - ingress
```

```
OcNOS#sh running-config access-list
ip access-list vty
10 permit tcp any host 3.3.3.3 eq telnet
!
line vty
ip access-group vty in
```

## Timed ACL

The time range feature was introduced to be able to add a timing boundary for specified activities. The activity would start, end and repeat at the specific times set by the user. This time-range feature will enable creating "Timed ACLs". This will help service providers customize the internet data to customers based on time to increase the video traffic during weekends and reduce data traffic, restrict the internet traffic in school/college non-working hours etc.

## Topology

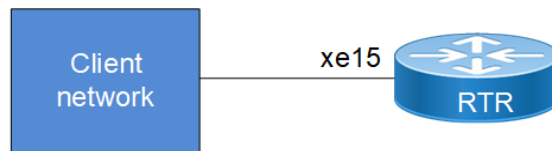


Figure 1-6: Timed acl sample topology

## Configuration with ipv4 Address

#configure terminal	Enter configure mode.
(config)# time-range TIMER1	Configure a timer
(config-tr)#start-time 10:00 03 nov 2021	Configure start time
(config-tr)#end-time 18:00 03 nov 2021	Configure end time
(config-tr)#exit	Exit timer
(config)# ip access-list ACL1	Create ip access list
(config-ip-acl)# deny icmp host 10.1.1.1 host 10.1.2.2	Create an acl rule to deny icmp
(config-ip-acl)#exit	Exit Acl mode
(config)#hardware-profile filter egress-ipv4 enable	Hardware profile enable for the acl
(config)#int xe15	Enter into the interface mode
(config-if)#ip access-group ACL1 out time-range TIMER1	Apply the acl along with the timer.
(config-if)#commit	To save the changes
(config-if)#exit	Exit

## Configuration with ipv6 Address

(config)# ipv6 access-list ACL1v6	Create ipv6 access list
(config-ipv6-acl)# deny any any any	Create an acl rule to deny
(config-ipv6-acl)#exit	Exit Acl mode
(config)# hardware-profile filter ingress-ipv6 enable	Hardware profile enable for the acl

(config)#int xe12	Enter into the interface mode
(config-if)# ipv6 access-group ACL1v6 in time-range TIMER1	Apply the acl along with the timer.
(config-if)#commit	To save the changes
(config-if)#exit	Exit

## Configuration with mac

(config)# mac access-list ACL1mac	Create ip access list
(config-mac-acl)# deny 0000.0000.0000 1111.2222.3333 0000.0000.0000 4444.5555.6666	Create an acl rule to deny icmp
(config-mac-acl)#exit	Exit Acl mode
(config)# hardware-profile filter ingress-12 enable	Hardware profile enable for the acl
(config)#int xe13	Enter into the interface mode
(config-if)# mac access-group ACL1mac in time-range TIMER1	Apply the acl along with the timer.
(config-if)#commit	To save the changes
(config-if)#exit	Exit

## Validation

```
#sh running-config in xe15
!
interface xe15
 ip access-group ACL1 out time-range TIMER1
!
OcNOS#sh running-config in xe12
!
interface xe12
 ipv6 access-group ACL1v6 in time-range TIMER1
!
OcNOS#sh running-config in xe13
!
interface xe13
 mac access-group ACL1mac in time-range TIMER1

#sh time-range
=====
TR handler interval: 10 seconds
=====
TR entries: 1
Entry: 0
  name: TIMER1
  state: Pending
```

frequency: none  
start time: Wed Nov 3 10:00:00 2021  
end time: Wed Nov 3 18:00:00 2021  
=====

RUNNING TR entries: 0  
=====

COMPLETED TR entries: 0





## CHAPTER 2 Control Plane Policing Configuration

This chapter contains basic information about cpu-queue properties and complete sample configuration for cpu-queue properties.

DUT have many CPU queues for management/classification of control traffic and provides rate limiters for control plane protection. Different types of CPU port bound packets are queued in different cpu-queues each with different properties like rate, queue-limit, monitoring status and drop status.

Control plane policing (CoPP) manages the traffic flow destined to the host router CPU for control plane processing.

CoPP limits the traffic forwarded to the host CPU and avoids impact on system performance.

1. CoPP has organized handling of control packets by providing per-protocol hardware CPU queues. So, control packets are queued in different CPU queues based on protocol.
2. Per-protocol CPU queue rate limits and buffer allocations are programmed during router initialization, thus every CPU queue is rate-limited to a default stable and balanced behavior across protocols.
3. When control packets received at higher rate than the programmed rate, the excess traffic is dropped at queue level in the packet processor hardware itself.
4. All CPU queues are pre-programmed with default rate limits and buffer allocations to ensure a default stable and balanced behavior across protocols.

### Topology



Figure 2-7: Simple configuration of CPU Queuing

Table 2-1: Default CPU queues

Protocol Queues	Default rate in PPS	Maximum configurable rate in PPS
best-effort	2113	2113
ipmc-miss	2113	2113
L3-miss	211	211
Sflow	32000	100000
Bgp	1500	1500
Vrrp	500	500
ldp-rsvp	500	500
Rip	500	500

**Table 2-1: Default CPU queues**

Ospf	2000	2000
Dhcp	100	2048
Nd	6000	6000
Mpls	500	500
pim	4000	4000
arp	6000	6000
igmp	4000	4000
Bpdu	10000	10000
Ccm	500	500
Bfd	2000	2000
Ptp	1000	1000
isis	500	1000
trill-isis	1000	1000
Acl	200	200
vxlan	500	500
daivm	100	500

## #show cpu-queue details

\* - Can not configure the parameter

Cpu queue		Rate In PPS		Monitor Status	
Lossy Status					
Name	Configured	Default	Max Rate Allowed	Configured	Default
=====	=====	=====	=====	=====	=====
best-effort	-	2113	2113	-	* lossy
ipmc-miss	-	2113	2113	-	* lossy
l3-miss	-	211	211	-	* lossy
sflow	-	32000	100000	-	* lossy
bgp	-	1500	1500	-	lossless
vrrp	-	500	500	-	lossless
ldp-rsvp	-	500	500	-	lossless
rip	-	500	500	-	lossless
ospf	-	2000	2000	-	lossless
dhcp	-	100	2048	-	lossy
nd	-	6000	6000	-	lossless
mpls	-	500	500	-	lossy
pim	-	4000	4000	-	* lossy
arp	-	6000	6000	-	lossless
igmp	-	4000	4000	-	* lossy
bpdu	-	10000	10000	-	lossless
ccm	-	500	500	-	lossy
bfd	-	2000	2000	-	lossy
ptp	-	1000	1000	-	lossy
isis	-	500	1000	-	lossless
trill-isis	-	1000	1000	-	lossless
acl	-	200	1000	-	* lossy
vxlan	-	500	500	-	lossy
daivm	-	100	500	-	lossy

**Note:** Enable feature before validating cpu-queue for that protocol.

Monitor option will start generating operational log for number of drop packets and percent.

```
OcNOS(config)#2021 Nov 16 11:40:24.188 : OcNOS : HSL : CRITI : [CPU_QUEUE_IS_FULL_2]:
967368133 packets dropped at queue bpdu due to queue full. Average CPU queue rate is 99%
(499 pkts/sec).
```

## Configuring CPU Queuing Lossless

Do the following to configure CPU queuing on an interface.

configure terminal	Enter config mode
(config)#cpu queue bpdu rate 600 lossless no monitor	Configure bpdu cpu-queue with rate of 600 pps and lossless and no-monitor option
(config)#exit	Exit config mode

## Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config | in cpu
```

```
cpu-queue bpdu rate 600 lossless no-monitor
```

```
#show cpu-queue details
```

```
* - Can not configure the parameter
```

Cpu queue Lossy Status		Rate In PPS			Monitor Status		
Name	Configured	Default	Max Rate Allowed	Configured	Default	Configured	Default
best-effort	-	2113	2113	-	* no-monitor	-	* lossy
ipmc-miss	-	2113	2113	-	* no-monitor	-	* lossy
l3-miss	-	211	211	-	* no-monitor	-	* lossy
sflow	-	32000	100000	-	monitor	-	* lossy
bgp	-	1500	1500	-	monitor	-	lossless
vrrp	-	500	500	-	monitor	-	lossless
ldp-rsvp	-	500	500	-	monitor	-	lossless
rip	-	500	500	-	monitor	-	lossless
ospf	-	2000	2000	-	monitor	-	lossless
dhcp	-	100	2048	-	no-monitor	-	lossy
nd	-	6000	6000	-	monitor	-	lossless
mpls	-	500	500	-	no-monitor	-	lossy
pim	-	4000	4000	-	* no-monitor	-	lossy
arp	-	6000	6000	-	monitor	-	lossless
igmp	-	4000	4000	-	* no-monitor	-	* lossy
bpdu	500	10000	10000	no-monitor	monitorloss	less	lossless
ccm	-	500	500	-	no-monitor	-	lossy
bfd	-	2000	2000	-	no-monitor	-	lossy
ptp	-	1000	1000	-	no-monitor	-	lossy
isis	-	500	1000	-	monitor	-	lossless
trill-isis	-	1000	1000	-	monitor	-	lossless
acl	-	200	1000	-	* no-monitor	-	* lossy
vxlan	-	500	500	-	monitor	-	lossy
daivm	-	100	500	-	no-monitor	-	lossy

```
#show int cpu counters rate kbps
```

```
Load interval: 30 second
```

```
+-----+-----+-----+-----+-----+
| CPU Queue(%) | Rx kbps | Rx pps | Tx kbps | Tx pps |
```

```
+-----+-----+-----+-----+
bpdu      ( 99%) -          -          38.41      599
```

```
#show interface cpu 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
cpu	bpdu	(E) 320736	21703	1388992	5363326	343240064

## Configuring CPU Queuing Lossy

Do the following to configure CPU queuing on an interface.

configure terminal	Enter config mode
(config)#cpu queue bpdu rate 500 lossy no monitor	Configure bpdu cpu-queue with rate of 500 pps and lossy and no-monitor option
(config)#exit	Exit config mode

## Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config | in cpu
cpu-queue bpdu rate 500 lossy no-monitor
```

```
#show cpu-queue details
```

```
* - Can not configure the parameter
```

Cpu queue		Rate In PPS		Monitor Status		Lossy Status	
Name	Configured	Default	Max Rate Allowed	Configured	Default	Configured	Default
best-effort	-	2113	2113	-	* no-monitor	-	* lossy
ipmc-miss	-	2113	2113	-	* no-monitor	-	* lossy
l3-miss	-	211	211	-	* no-monitor	-	* lossy
sflow	-	32000	100000	-	monitor	-	* lossy
bgp	-	1500	1500	-	monitor	-	lossless
vrrp	-	500	500	-	monitor	-	lossless
ldp-rsvp	-	500	500	-	monitor	-	lossless
rip	-	500	500	-	monitor	-	lossless
ospf	-	2000	2000	-	monitor	-	lossless
dhcp	-	100	2048	-	no-monitor	-	lossy
nd	-	6000	6000	-	monitor	-	lossless
mpls	-	500	500	-	no-monitor	-	lossy
pim	-	4000	4000	-	* no-monitor	-	* lossy
arp	-	6000	6000	-	monitor	-	lossless
igmp	-	4000	4000	-	* no-monitor	-	* lossy
bpdu	500	10000	10000	no-monitor	monitor	lossy	lossless
ccm	-	500	500	-	no-monitor	-	lossy
bfd	-	2000	2000	-	no-monitor	-	lossy
ptp	-	1000	1000	-	no-monitor	-	lossy
isis	-	500	1000	-	monitor	-	lossless
trill-isis	-	1000	1000	-	monitor	-	lossless
acl	-	200	1000	-	* no-monitor	-	* lossy
vxlan	-	500	500	-	monitor	-	lossy
daivm	-	100	500	-	no-monitor	-	lossy

```
OcNOS#show interface cpu 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
cpu	nd	(E) 0	17	1998	0	0
cpu	bpdu	(E) 86320	153802	9843328	39667426	2538702464

OcNOS#show int cpu counters rate kbps  
Load interval: 30 second

CPU Queue(%)	Rx kbps	Rx pps	Tx kbps	Tx pps
bpdu ( 99%) -	-	31.97	499	



# CHAPTER 3 DHCP Client Configuration

## Overview

Dynamic Host Configuration Protocol (DHCP) protocol is used for assigning dynamic IP addresses to systems on a network. Dynamic addressing allows a system to have an IP address each time it connects to the network. DHCP makes network administration easier by removing the need to manually assign a unique IP address every time a new system is added to the network. It is especially useful to manage mobile users. Once a system is configured to use DHCP, it can be automatically configured on any network that has a DHCP server.

DHCP uses a client-server model, in which the DHCP server centrally manages the IP addresses used in the network. DHCP clients obtain an IP address on lease from the DHCP server.

## DHCP Client Configuration for IPv4

Before configuring the DHCP in client, make sure that DHCP server is ready and also dhcpd is running on the server machine.

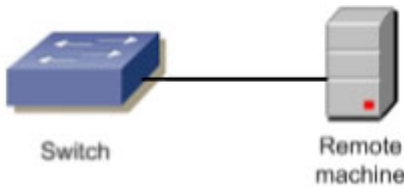


Figure 3-8: DHCP sample topology

#configure terminal	Enter configure mode.
(config)#feature dhcp	Enable the feature dhcp. This will be enabled by default.
(config)#interface xe1	Enter interface mode.
(config-if)#ip address dhcp	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
(config if)#exit	Exit interface mode.
(config)#interface eth0	Enter management interface mode.
(config-if)#ip address dhcp	The client requests for the IP address to the server, once it receives the Acknowledgement from the server, it assigns the IP address to the management interface.
(config if)#exit	Exit interface mode.

## Validation Commands

```
#show running-config dhcp
  interface xe2
    ip address dhcp
  !
  ip dhcp relay information option
```

#sh ip interface brief

Interface	IP-Address	Admin-Status	Link-Status
GMPLS Type			
eth0	10.12.44.20	up	up
-			
lo	127.0.0.1	up	up
-			
lo.4	127.0.0.1	up	up
-			
vlan1.1	unassigned	up	down
-			
xe1/1	2.2.2.3	up	up
-			
xe1/2	unassigned	down	down
-			
xe1/3	unassigned	down	down
-			
xe1/4	unassigned	up	down
-			
xe2	*40.40.40.40	up	down
-			
xe3/1	20.20.30.1	up	up
-			



## CHAPTER 4 DHCP Relay Agent Configuration

### Overview

The DHCP Relay feature was designed to forward DHCP broadcast requests as unicast packets to a configured DHCP server or servers for redundancy in different network segments.

### DHCP Relay for IPv4

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.

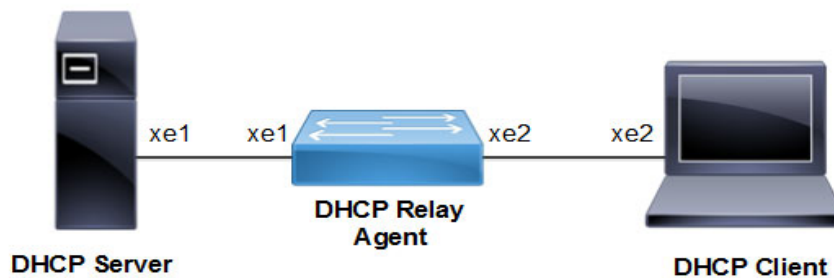


Figure 4-9: DHCP Relay Configuration

### DHCP Agent

#configure terminal	Enter configure mode.
(config)#feature dhcp	Enable the feature dhcp. This is enabled by default.
(config)#ip dhcp relay	By default this will be enabled. It starts the ip dhcp relay service.
(config)# ip dhcp relay address 10.10.10.2	The relay address configured should be server interface address connected to DUT machine.
(config)#interface xe1	Enter interface mode.
(config-if)#ip address 10.10.10.1/24	Configure ipv4 address on the interface xe1.
(config-if)#ip dhcp relay uplink	Configure relay uplink on the device connecting the server.
(config if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 20.20.20.1/24	Configure ipv4 address on the interface xe2.
(config-if)#ip dhcp relay	Relay should be configured on the interface connecting to the client.
(config if)#exit	Exit interface mode.

### Validation Commands

```

#show running-config dhcp

ip dhcp relay address 10.10.10.2
interface xe2
  
```

```
ip dhcp relay
!
interface xe1
ip dhcp relay uplink
!

#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
Option 82: Disabled
DHCP Servers configured: 10.10.10.2
Interface                Uplink/Downlink
-----
xe2                      Downlink
xe1                      Uplink

#show ip dhcp relay address
VRF Name: default
DHCP Servers configured: 10.10.10.2
```

---

## DHCP Relay for IPv6 Configuration

---

### DHCP Agent

#configure terminal	Enter configure mode.
(config)#feature dhcp	Enable the feature dhcp. This is enabled in default.
(config)#ipv6 dhcp relay	By default this will be enabled. It starts the ipv6 dhcp relay service.
(config)#ipv6 dhcp relay address 2001::2	The relay address configured should be server interface address connected to DUT machine.
(config)#interface xe1	Enter interface mode.
(config-if)#ipv6 address 2001::1/64	Configure ipv6 address on the interface xe1.
(config-if)#ipv6 dhcp relay uplink	Configure relay uplink on the device connecting the server.
(config if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ipv6 address 2002::1/64	Configure ipv6 address on the interface xe2.
(config-if)#ipv6 dhcp relay	Relay should be configured on the interface connecting to the client.
(config if)#exit	Exit interface mode.

---

### Validation Commands

```
#sh ipv6 dhcp relay address

VRF Name: default
DHCPv6 Servers configured: 2001::2

#show running-config dhcp
```

```
Ipv6 dhcp relay address 2001::2
interface xe2
ipv6 dhcp relay
!
interface xe1
ipv6 dhcp relay uplink
!
```

---

## DHCP Relay option 82

This section contains examples of DHCP Relay option-82 configuration. DHCP option 82 (Agent Information Option) provides additional security when DHCP is used to allocate network addresses. It enables the DHCP relay agent to prevent DHCP client requests from untrusted sources. Service Providers use remote identifier (option 82 sub option 2) for troubleshooting, authentication, and accounting. The **DHCP Option 82 Remote ID** Format feature adds support for the interpretation of **remote-IDs** that are inserted by end users. On the relay agent, you can configure information option to add option 82 information to DHCP requests from the clients before forwarding the requests to the DHCP server. When configured with option 82 and remote-id, the server will receive the DHCP request packet with Agent Circuit ID and remote-id.

The two examples below, show how to configure the DHCP Relay option 82:

- Configuration of DHCP Relay option 82 on a physical interface with Agent information and remote-id.
- Configuration of DHCP Relay option 82 on a VLAN interface with Agent information and remote-id.

---

## Topology

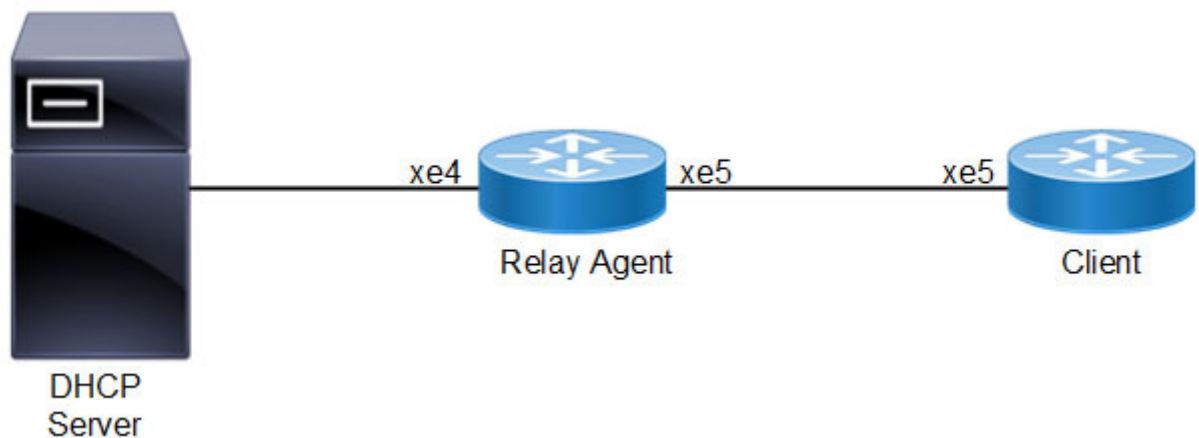


Figure 4-10: DHCP 82 interface topology

---

## Physical Interface Configuration

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnet 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for `DHCP OFFER` packets to reach the Relay Agent.

**Relay agent**

#configure terminal	Enter configure mode.
(config)#ip dhcp relay	Enable DHCP Relay
(config)#ip dhcp relay information option remote-id hostname	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82. String support is also provided for remote-id.
(config)#interface xe5	Enter interface mode.
(config-if)#ip address 10.10.20.2/24	Add IP address
(config-if)#ip dhcp relay	Configure DHCP relay for the interface connecting to client.
(config-if)#exit	Exit from interface mode
(config)#interface xe4	Enter interface mode
(config-if)#ip dhcp relay uplink	Configure DHCP relay uplink for the interface connecting to server.
(config-if)#exit	Exit interface mode.

**Client**

#configure terminal	Enter configure mode.
(config)#interface xe5	Enter interface mode.
(config-if)#ip address dhcp	Configure IP address DHCP
(config-if)#exit	Exit from interface mode

**Validation****Relay Agent**

```
#show running-config dhcp
!
ip dhcp relay information option remote-id hostname
ip dhcp relay address 192.168.1.2
interface xe5
  ip dhcp relay
!
interface xe4
  ip dhcp relay uplink
!
```

```
#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
Option 82: Enabled
Remote Id: OcNOS
DHCP Servers configured: 192.168.1.2
Interface                Uplink/Downlink
-----
xe5                        Downlink
xe4                        Uplink
```

**Client**

```
#show ip interface brief | include xe5
xe5                *10.10.20.10      up
```

Packet captured at DHCP Server

**Bootstrap Protocol (Discover)**

```
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 1
Transaction ID: 0x4e61176c
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
    0... .... = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 10.10.20.2 (10.10.20.2)
Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
    Length: 1
    DHCP: Discover (1)
Option: (55) Parameter Request List
    Length: 3
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (28) Broadcast Address
    Parameter Request List Item: (3) Router
Option: (60) Vendor class identifier
    Length: 39
    Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
Option: (82) Agent Information Option
    Length: 12
    Option 82 Suboption: (1) Agent Circuit ID
        Length: 3
        Agent Circuit ID: 786535
    Option 82 Suboption: (2) Agent Remote ID
        Length: 5
        Agent Remote ID: 4f634e4f53
Option: (255) End
    Option End: 255
Padding
```

---

**Physical Interface Configuration with non-default vrf.**

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnet 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for DHCP OFFER packets to reach the Relay Agent.

**Relay agent**

#configure terminal	Enter configure mode.
(config)#ip dhcp relay	Enable DHCP Relay.
(config)#ip vrf vrf_dhcp	Configuring non default vrf vrf_dhcp
(config-vrf)#ip dhcp relay information option remote-id hostname	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82 on non default vrf.. String support is also provided for remote-id.
(config-vrf)#ip dhcp relay address 192.168.1.2	Configure DHCP relay address in non default vrf.
(config)#interface xe5	Enter interface mode.
(config-if)#ip vrf forwarding vrf_dhcp	Configure vrf forwarding for vrf_dhcp.
(config-if)#ip address 10.10.20.2/24	Add IP address.
(config-if)#ip dhcp relay	Configure DHCP relay for the interface connecting to client.
(config-if)#exit	Exit from interface mode
(config)#interface xe4	Enter interface mode
(config-if)#ip vrf forwarding vrf_dhcp	Configure vrf forwarding for vrf_dhcp.
(config-if)#ip dhcp relay uplink	Configure DHCP relay uplink for the interface connecting to server.
(config-if)#ip address 192.168.1.4/24	Add IP address.
(config-if)#exit	Exit interface mode.

**Client**

#configure terminal	Enter configure mode.
(config)#interface xe5	Enter interface mode.
config-if)#ip vrf forwarding vrf_dhcp	Configure ip vrf forwarding for non default vrf.
(config-if)#ip address dhcp	Configure IP address DHCP.
(config-if)#exit	Exit from interface mode.

**Validation****Relay Agent**

```
#show running-config dhcp
!
ip vrf vrf_dhcp
  ip dhcp relay information option remote-id hostname
  ip dhcp relay address 192.168.1.2
interface xe5
  ip dhcp relay
!
interface xe4
  ip dhcp relay uplink
!
```

```
#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: vrf_dhcp
Option 82: Enabled
Remote Id: OcNOS
DHCP Servers configured: 192.168.1.2
Interface          Uplink/Downlink
-----
xe5                 Downlink
xe4                 Uplink
```

## Client

```
#show ip interface brief | include xe5
xe5          *10.10.20.10      up          up
```

Packet captured at DHCP Server

```
Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x4e61176c
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
    0... .... = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 10.10.20.2 (10.10.20.2)
  Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type (Discover)
    Length: 1
    DHCP: Discover (1)
  Option: (55) Parameter Request List
    Length: 3
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (28) Broadcast Address
    Parameter Request List Item: (3) Router
  Option: (60) Vendor class identifier
    Length: 39
    Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
  Option: (82) Agent Information Option
    Length: 12
    Option 82 Suboption: (1) Agent Circuit ID
      Length: 3
      Agent Circuit ID: 786535
    Option 82 Suboption: (2) Agent Remote ID
      Length: 5
      Agent Remote ID: 4f634e4f53
```

Option: (255) End  
Option End: 255  
Padding

Sample DHCP configuration for using Remote-id

```
class "remote-id" {  
    match if option agent.remote-id = OcNOS  
} # remote-id  
  
subnet 10.10.20.0 netmask 255.255.255.0 {  
    pool {  
        allow members of                "remote-id";  
        default-lease-time                600;  
        max-lease-time                    7200;  
        range                            10.10.20.3 10.10.10.100;  
        option routers                    10.10.20.2;  
        option broadcast-address          10.10.20.255;  
        option subnet-mask                255.255.255.0;  
        option domain-name-servers        4.2.2.2;  
    }  
}
```

VLAN Interface Configuration

Topology



Figure 4-11: DHCP 82 vlan topology

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnets 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for DHCP OFFER packets to reach the Relay Agent. In the above topology, vlan 20 is part of interface xe5 in relay Agent and xe5 in Client.

Relay Agent

#configure terminal	Enter configure mode.
(config)#ip dhcp relay	Enable DHCP Relay



(config)#ip dhcp relay information option remote-id hostname	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82. String support is also provided for remote-id.
(config)#ip dhcp relay address 192.168.1.2	Configure DHCP relay address
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge
(config)#vlan 2-100 bridge 1 state enable	Enable some VLANs
(config)#interface xe5	Enter interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode hybrid	Configure switchport mode
(config-if)#switchport hybrid allowed vlan all	Enable vlan
(config-if)#exit	Exit from interface mode
(config)#interface vlan1.20	Enter interface mode for the vlan interface towards client.
(config-if)#ip address 10.10.20.2/24	Add IP address
(config-if)#ip dhcp relay	Configure DHCP relay on the vlan interface connecting to client.
(config-if)#exit	Exit from interface mode
(config)#interface xe4	Enter interface mode
(config-if)#ip dhcp relay uplink	Configure DHCP relay uplink for the interface connecting to server.
(config-if)#ip address 192.168.1.4/24	Add IP address
(config-if)#exit	Exit interface mode.

## Client

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge
(config)#vlan 2-100 bridge 1 state enable	Enable VLANs
(config)#interface xe5	Enter interface mode.
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode hybrid	Configure switchport mode
(config-if)#switchport hybrid allowed vlan add 20 egress-tagged enable	Enable vlan
(config-if)#exit	Exit from interface mode
(config)#interface vlan1.20	Enter interface mode for the vlan interface which connects relay.
(config-if)#ip address dhcp	Configure IP address DHCP
(config-if)#exit	Exit from interface mode

---

## Validation

### Relay Agent

```
#show running-config dhcp
!
ip dhcp relay information option remote-id hostname
ip dhcp relay address 192.168.1.2
!
interface vlan1.20
 ip dhcp relay
!
interface xe4
 ip dhcp relay uplink
!
```

```
#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
Option 82: Enabled
Remote Id: ocnos
DHCP Servers configured: 192.168.1.2
Interface          Uplink/Downlink
-----
Vlan1.20           Downlink
xe4                Uplink
```

### Client

```
#show ip interface brief |include vlan1.20
vlan1.20          *10.10.20.10      up          up
```

Packet captured at DHCP Server

```
Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x59591459
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
    0... .... = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 10.10.20.2 (10.10.20.2)
  Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type (Discover)
    Length: 1
```

```
DHCP: Discover (1)
Option: (55) Parameter Request List
  Length: 3
  Parameter Request List Item: (1) Subnet Mask
  Parameter Request List Item: (28) Broadcast Address
  Parameter Request List Item: (3) Router
Option: (60) Vendor class identifier
  Length: 39
  Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
Option: (82) Agent Information Option
  Length: 17
  Option 82 Suboption: (1) Agent Circuit ID
    Length: 8
    Agent Circuit ID: 766c616e312e3230
  Option 82 Suboption: (2) Agent Remote ID
    Length: 5
    Agent Remote ID: 4f634e4f53

Option: (255) End
  Option End: 255
```



## CHAPTER 5 DHCP Relay Agent Over L3VPN Configuration

The DHCP Relay feature was designed to forward DHCP broadcast requests as unicast packets to a configured DHCP server or servers for redundancy. In the L3VPN case, there is a special tunnel which gets created through which all the communication happens. In OcNOS, the interface created is named as tunmpls. This tunnel name is not exposed to the OcNOS control plane. This interface is directly created in the kernel.

### DHCP Relay Over L3 VPN for IPv4

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.

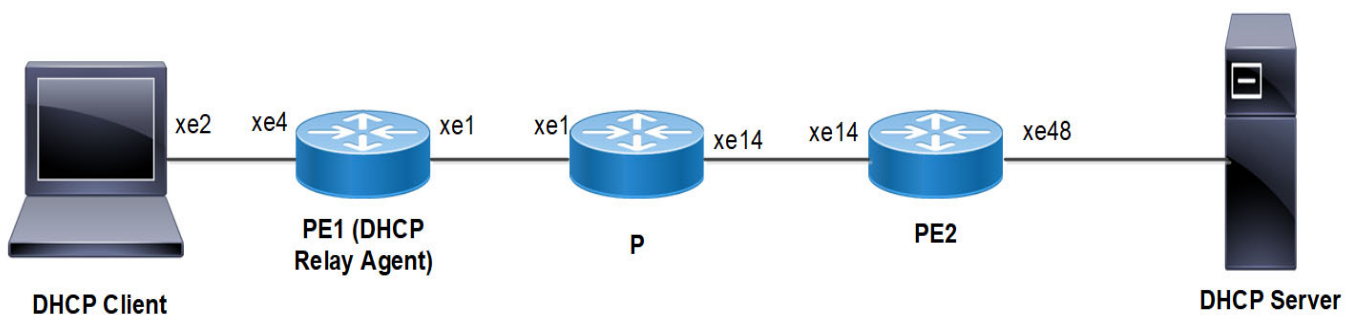


Figure 5-12: DHCP Relay Over L3 VPN Configuration

#### DHCP Client

#configure terminal	Enter configure mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip address dhcp	Enable DHCP on interface
(config-if)#commit	Commit the candidate configuration to the running configuration

**PE1(DHCP Relay Agent)**

#configure terminal	Enter configure mode.
(config)#ip dhcp relay	By default this will be enabled. It starts the ip dhcp relay service.
(config)#ip vrf vrf1	Configuring non default vrf vrf1
(config-vrf)# rd 10:10	Assign a route distinguisher to VRF
(config-vrf)# route-target both 10:10	Configure a route target for vrf1.
(config-vrf)#ip dhcp relay address 11.11.0.1	Configure DHCP server address.
(config-vrf)# ip dhcp relay uplink l3vpn	configure IPv4 DHCP Relay over L3VPN.
(config)#interface xe4	Enter interface mode.
(config-if)#ip vrf forwarding vrf1	Configure vrf forwarding for vrf1
(config-if)#ip address 50.50.50.1/24	Add IP address.
(config-if)#ip dhcp relay	Configure DHCP relay for the interface connecting to client.
(config-if)#exit	Exit from interface mode
(config)#interface lo	Enter interface mode
(config-if)#ip address 1.1.1.1/32 secondary	Set an IP address on the interface
(config-if)#exit	Exit from interface mode
(config)#router ldp	Enter the Router LDP mode.
(config-router)#router-id 1.1.1.1	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode
(config)#interface xel	Enter interface mode
(config-if)# ip address 10.1.1.1/24	Add IP address.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#network 1.1.1.1/32 area 0.0.0.0	Advertise loopback address in OSPF.
(config-router)#network 10.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.
(config)# router bgp 100	Enter the Router BGP mode, ASN: 100
(config-router)# bgp router-id 1.1.1.1	Configure a fixed Router ID (1.1.1.1)
(config-router)# neighbor 3.3.3.3 remote-as 100	Configuring PE2 as iBGP neighbor using it's loopback IP
(config-router)# neighbor 3.3.3.3 update-source lo	Source of routing updates as loopback
(config-router)# address-family ipv4 unicast	Entering into IPV4 unicast address family
(config-router-af)# neighbor 3.3.3.3 activate	Activate the neighbor in the IPV4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family vpnv4 unicast	Entering into address family mode as vpnv4

(config-router-af)# neighbor 3.3.3.3 activate	Activate the neighbor in the vpnv4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv4 vrf vrf1	Entering into address family mode as ipv4 vrf vrf1
(config-router-af)# redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# commit	Commit the candidate configuration to the running configuration

**P**

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 2.2.2.2/32 secondary	Set an IP address on the interface
(config-if)#exit	Exit from interface mode
(config)#router ldp	Enter the Router LDP mode.
(config-router)#router-id 2.2.2.2	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode
(config)#interface xe14	Enter interface mode
(config-if)# ip address 20.1.1.1/24	Add IP address.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#interface xe1	Enter interface mode
(config-if)# ip address 10.1.1.2/24	Add IP address.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#network 3.3.3.3/32 area 0.0.0.0	Advertise loopback address in OSPF.
(config-router)#network 20.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#network 10.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.
(config)# commit	Commit the candidate configuration to the running configuration

**PE2**

#configure terminal	Enter configure mode.
(config)#ip vrf vrf1	Configuring non default vrf vrf1
(config-vrf)# rd 10:10	Assign a route distinguisher to VRF
(config-vrf)# route-target both 10:10	Configure a route target for vrf1.
(config)#interface xe48	Enter interface mode.
(config-if)#ip vrf forwarding vrf1	Configure vrf forwarding for vrf1
(config-if)# commit	Commit the candidate config
(config-if)#ip address 11.11.0.2/24	Add IP address.
(config-if)#exit	Exit from interface mode
(config)#interface lo	Enter interface mode
(config-if)#ip address 3.3.3.3/32 secondary	Set an IP address on the interface
(config-if)#exit	Exit from interface mode
(config)#router ldp	Enter the Router LDP mode.
(config-router)#router-id 3.3.3.3	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode
(config)#interface xe14	Enter interface mode
(config-if)# ip address 20.1.1.2/24	Add IP address.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#network 3.3.3.3/32 area 0.0.0.0	Advertise loopback address in OSPF.
(config-router)#network 20.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.
(config)# router bgp 100	Enter the Router BGP mode, ASN: 100
(config-router)# bgp router-id 3.3.3.3	Configure a fixed Router ID (3.3.3.3)
(config-router)# neighbor 1.1.1.1 remote-as 100	Configuring PE1 as iBGP neighbor using it's loopback IP
(config-router)# neighbor 1.1.1.1 update-source lo	Source of routing updates as loopback
(config-router)# address-family ipv4 unicast	Entering into IPV4 unicast address family
(config-router-af)# neighbor 1.1.1.1 activate	Activate the neighbor in the IPV4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family vpnv4 unicast	Entering into address family mode as vpnv4
(config-router-af)# neighbor 1.1.1.1 activate	Activate the neighbor in the vpnv4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv4 vrf vrf1	Entering into address family mode as ipv4 vrf vrf1



---

(config-router-af)# redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# commit	Commit the candidate configuration to the running configuration

---



---

## Validation

### PE1 (DHCP Relay Agent)

```
PE1#show running-config dhcp
```

```
ip vrf vrf1
  ip dhcp relay address 11.11.0.1
  ip dhcp relay uplink l3vpn
interface xe4
  ip dhcp relay
```

```
PE1#show ip dhcp relay
```

```
DHCP relay service is Enabled.
```

```
VRF Name: vrf1
```

```
Option 82: Disabled
```

```
DHCP Servers configured: 11.11.0.1
```

Interface	Uplink/Downlink
-----	-----
xe4	Downlink
l3vpn	uplink

```
Incoming DHCPv4 packets which already contain relay agent option are FORWARDED unchanged.
```

### PE1#show ip dhcp relay address

```
VRF Name: vrf1
```

```
DHCP Servers configured: 11.11.0.1
```

```
Incoming DHCPv4 packets which already contain relay agent option are FORWARDED unchanged.
```

### DHCP Client

```
#show ip interface brief | include xe2
xe5    *50.50.50.2 up    up
```

## DHCP Relay Over L3 VPN for IPv6

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.

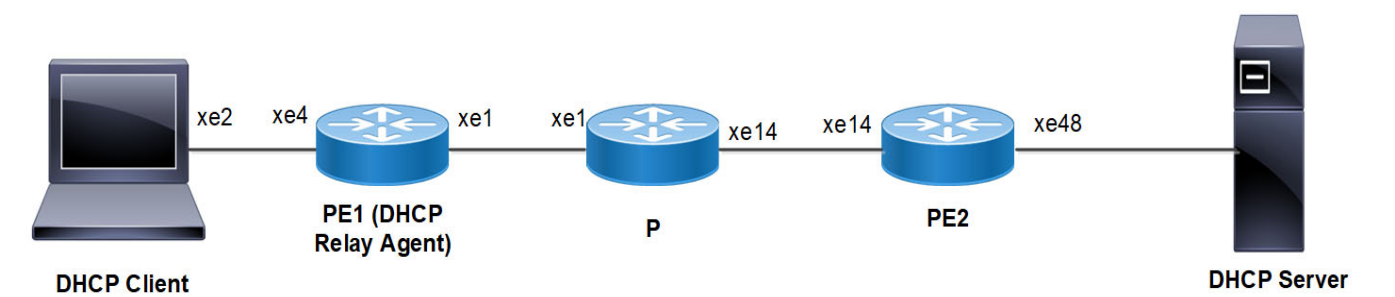


Figure 5-13: DHCP Relay Over L3 VPN Configuration

### DHCP Client

#configure terminal	Enter configure mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ipv6 address dhcp	Enable DHCP on interface
(config-if)#commit	Commit the candidate configuration to the running configuration

**PE1(DHCP Relay Agent)**

#configure terminal	Enter configure mode.
(config)#ipv6 dhcp relay	By default this will be enabled. It starts the ipv6 dhcp relay service.
(config)#ip vrf vrf1	Configuring non default vrf vrf1
(config-vrf)# rd 10:10	Assign a route distinguisher to VRF
(config-vrf)# route-target both 10:10	Configure a route target for vrf1.
(config-vrf)# ipv6 dhcp relay address 2002::1	Configure DHCP server address.
(config-vrf)# ipv6 dhcp relay uplink l3vpn	configure IPv6 DHCP Relay over L3VPN.
(config)#interface xe4	Enter interface mode.
(config-if)#ip vrf forwarding vrf1	Configure vrf forwarding for vrf1
(config-if)# ipv6 address 2001::1/64	Add IPv6 address.
(config-if)#ipv6 dhcp relay	Configure DHCP relay for the interface connecting to client.
(config-if)#exit	Exit from interface mode
(config)#interface lo	Enter interface mode
(config-if)#ip address 1.1.1.1/32 secondary	Set an IP address on the interface
(config-if)#exit	Exit from interface mode
(config)#router ldp	Enter the Router LDP mode.
(config-router)#router-id 1.1.1.1	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode
(config)#interface xe1	Enter interface mode
(config-if)# ip address 10.1.1.1/24	Add IP address.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#network 1.1.1.1/32 area 0.0.0.0	Advertise loopback address in OSPF.
(config-router)#network 10.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.
(config)# router bgp 100	Enter the Router BGP mode, ASN: 100
(config-router)# bgp router-id 1.1.1.1	Configure a fixed Router ID (1.1.1.1)
(config-router)# neighbor 3.3.3.3 remote-as 100	Configuring PE2 as iBGP neighbor using it's loopback IP
(config-router)# neighbor 3.3.3.3 update-source lo	Source of routing updates as loopback
(config-router)# address-family ipv4 unicast	Entering into IPV4 unicast address family
(config-router-af)# neighbor 3.3.3.3 activate	Activate the neighbor in the IPV4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family vpnv4 unicast	Entering into address family mode as vpnv4

## DHCP Relay Agent Over L3VPN Configuration

(config-router-af)# neighbor 3.3.3.3 activate	Activate the neighbor in the vpv4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family vpv6 unicast	Entering into address family mode as vpv6
(config-router-af)# neighbor 3.3.3.3 activate	Activate the neighbor in the vpv6 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv4 vrf vrf1	Entering into address family mode as ipv4 vrf vrf1
(config-router-af)# redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv6 vrf vrf1	Entering into address family mode as ipv6 vrf vrf1
(config-router-af)# redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# commit	Commit the candidate configuration to the running configuration

**P**

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 2.2.2.2/32 secondary	Set an IP address on the interface
(config-if)#exit	Exit from interface mode
(config)#router ldp	Enter the Router LDP mode.
(config-router)#router-id 2.2.2.2	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode
(config)#interface xe14	Enter interface mode
(config-if)# ip address 20.1.1.1/24	Add IP address.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#interface xe1	Enter interface mode
(config-if)# ip address 10.1.1.2/24	Add IP address.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#network 3.3.3.3/32 area 0.0.0.0	Advertise loopback address in OSPF.
(config-router)#network 20.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#network 10.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.
(config)# commit	Commit the candidate configuration to the running configuration

**PE2**

#configure terminal	Enter configure mode.
(config)#ip vrf vrf1	Configuring non default vrf vrf1
(config-vrf)# rd 10:10	Assign a route distinguisher to VRF
(config-vrf)# route-target both 10:10	Configure a route target for vrf1.
(config)#interface xe48	Enter interface mode.
(config-if)#ip vrf forwarding vrf1	Configure vrf forwarding for vrf1
(config-if)# commit	Commit the candidate config
(config-if)# ipv6 address 2002::2/64	Add IPv6 address.
(config-if)#exit	Exit from interface mode
(config)#interface lo	Enter interface mode
(config-if)#ip address 3.3.3.3/32 secondary	Set an IP address on the interface
(config-if)#exit	Exit from interface mode
(config)#router ldp	Enter the Router LDP mode.
(config-router)#router-id 3.3.3.3	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode
(config)#interface xe14	Enter interface mode
(config-if)# ip address 20.1.1.2/24	Add IP address.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#network 3.3.3.3/32 area 0.0.0.0	Advertise loopback address in OSPF.
(config-router)#network 20.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.
(config)# router bgp 100	Enter the Router BGP mode, ASN: 100
(config-router)# bgp router-id 3.3.3.3	Configure a fixed Router ID (3.3.3.3)
(config-router)# neighbor 1.1.1.1 remote-as 100	Configuring PE1 as iBGP neighbor using it's loopback IP
(config-router)# neighbor 1.1.1.1 update-source lo	Source of routing updates as loopback
(config-router)# address-family ipv4 unicast	Entering into IPV4 unicast address family
(config-router-af)# neighbor 1.1.1.1 activate	Activate the neighbor in the IPV4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family vpnv4 unicast	Entering into address family mode as vpnv4
(config-router-af)# neighbor 1.1.1.1 activate	Activate the neighbor in the vpnv4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family vpnv6 unicast	Entering into address family mode as vpnv6

---

(config-router-af)# neighbor 1.1.1.1 activate	Activate the neighbor in the vpnv6 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv4 vrf vrf1	Entering into address family mode as ipv4 vrf vrf1
(config-router-af)# redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv6 vrf vrf1	Entering into address family mode as ipv6 vrf vrf1
(config-router-af)# redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# commit	Commit the candidate configuration to the running configuration

---

## Validation

---

### PE1 (DHCP Relay Agent)

```
PE1#show running-config dhcp
ip vrf vrf1
  ipv6 dhcp relay address 2002::1
  ipv6 dhcp relay uplink l3vpn
interface xe4
  ipv6 dhcp relay
```

```
PE1#show ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: vrf1
  Option 82: Enabled
  DHCPv6 Servers configured: 2002::1
  DHCPv6 IA_PD Route injection: Disabled
  Interface                Uplink/Downlink
  -----                -
  xe4                      Downlink
  l3vpn                    uplink
PE1#show ip dhcp relay address
VRF Name: vrf1
  DHCPv6 Servers configured: 2002::1
```

### DHCP Client

```
#show ipv6 interface brief | include xe2
xe5    *2001::200  up    up
```





---

## CHAPTER 6 DHCP Snooping

---

---

### Overview

DHCP snooping is a series of techniques applied to ensure the security of an existing DHCP infrastructure. It is a security feature that acts like a fire wall between untrusted hosts and trusted DHCP servers. It is a layer-2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable.

The fundamental use case of DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. Rogue DHCP servers are often used in 'man-in the middle' or 'Denial of Service' attacks from malicious purpose. Similarly DHCP clients (rogue) can also cause 'Denial of Service' attacks by continuously requesting for IP addresses causing address depletion in the DHCP server.

The DHCP snooping feature performs the following activities:

- Validates DHCP messages received from un-trusted sources and filters out invalid messages.
- Rate-limits DHCP traffic from trusted and un-trusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about un-trusted hosts with leased IP addresses.
- Utilizes the DHCP snooping binding database to validate subsequent requests from un-trusted hosts.
- To retain the DHCP snooping bindings database across reloads, it is stored in a persistent file on switch itself. Upon reload, the switch restores binding database from the persistent file. On NTP sync, the lease time of the binding entries gets re-adjusted based on the timestamp that was written in the persistent file. The switch keeps the file updated by writing to the file periodically (default interval 300 seconds).

Note: To ensure the accuracy of lease time adjustment, NTP should be configured on the snooper.

- When DHCP snooping is used over MLAG, the DHCP snooping binding database syncing will be happening among the peers via IDL.

DHCP snooping with provider bridge is not supported.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

## Topology

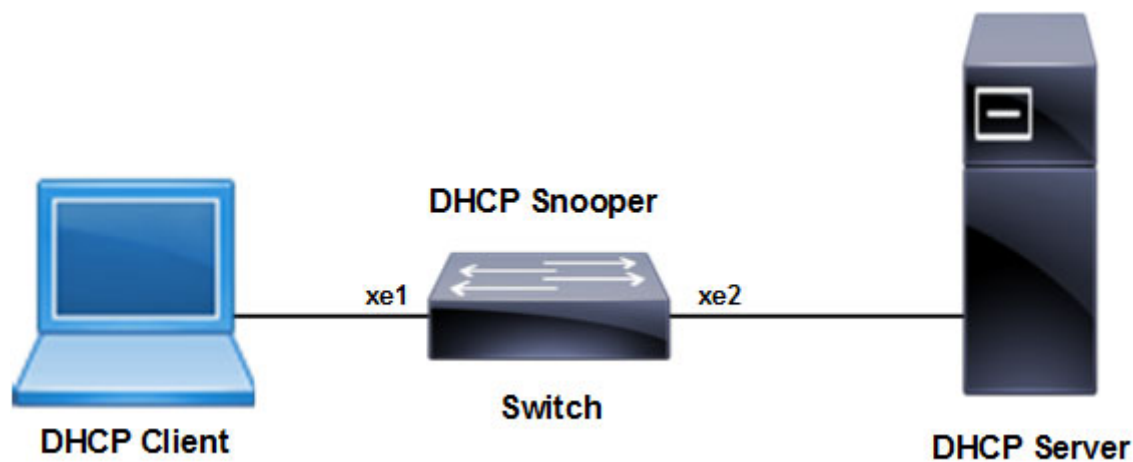


Figure 6-14: DHCP snooping

## Configuration Guidelines

When configuring DHCP snooping, follow these guidelines:

- DHCP snooping is not active until you enable the feature on at least one VLAN, and enable DHCP snooping globally on the switch.
- Before globally enabling DHCP snooping on the switch, make sure that the device acting as the DHCP server is configured and enabled.
- If a Layer 2 LAN port is connected to a DHCP server, configure the port as trusted by entering the `ip dhcp snooping trust interface` configuration command.
- If a Layer 2 LAN port is connected to a DHCP client, configure the port as un-trusted by entering the `no ip dhcp snooping trust interface` configuration command.

## Procedures

The following subsections provide examples of how to enable and configure DHCP Snooping.

### Enable DHCP Snooping Globally

<code>#configure terminal</code>	Enter configure mode.
<code>(config)#bridge 1 protocol mstp</code>	Create mstp or ieee vlan-bridge.
<code>(config)#ip dhcp snooping bridge 1</code>	Enable DHCP Snooping on the bridge

## Enable DHCP Snooping on a VLAN

configure terminal	Enter configure mode.
(config)#vlan 2 bridge 1	Configure a vlan for the bridge.
(config)#ip dhcp snooping vlan 2 bridge 1	Enable DHCP Snooping on the vlan 2

## Configure Ports connected to DHCP Sserver and DHCP Client

#configure terminal	Enter the configure mode
(config)#interface xe1	Specify the interface xe1 to be configured, and Enter interface mode
(config-if)#switchport	Configure the interface as a switch port.
(config-if)#bridge-group 1	Associate the interface xe1 with bridge-group 1 .
(config-if)#switchport mode access	Configure the port as an access port
(config-if)#switchport access vlan 2	Bind the interface vlan 2 to the port.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Specify interface xe2 to be configured connected to server.
(config-if)#switchport	Configure the interface as a switch port.
(config-if)#bridge-group 1	Associate interface xe2 with bridge-group 1.
(config-if)#switchport mode access	Configure the port as an access port.
(config-if)#switchport access vlan 2	Bind the interface vlan 2 to the port.
(config-if)#exit	Exit interface mode.
(config)#exit	Exit the config mode.

## Configure Trusted and Untrusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as untrusted port

In this example, xe1 is connected to the DHCP client and xe2 is connected to the DHCP server.

- Configure xe1 connected to DHCP client as un-trusted port.
- Configure xe2 connected to the DHCP server as trusted port.

#configure terminal	Enter configure mode.
(config)#interface xe1	Specify the interface to be configured
(config-if)#no ip dhcp snooping trust	Disable the port as trusted.

## DHCP Snooping Operation

1. Configure DHCP server that is connected to DHCP Snooper through trusted port.
2. Request an ip address from the DHCP client connected through the un-trusted port.

3. DHCP client broadcast the DHCP DISCOVER message to the switch.
4. DHCP server responds to the DHCP DISCOVER message with DHCP offer message to the client.
5. Once the DHCP OFFER is received by the client, it sends an DHCP REQUEST to the server.
6. DHCP server validates the request from the client and sends DHCP ACK with the offered ip address to the client with the lease time.
7. DHCP Snooper creates an entry for the above operation into the binding table which includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.
8. DHCP Snooper clears the entry in the binding table once the client sends the DHCP RELEASE or lease time is expired.

Note: On snooper once lease time becomes 0 for an entry, it is removed from the bind table within 10 sec.

---

## Validation

The `show running-config ip dhcp snooping` command displays the DHCP snooping commands configured on the device in question.

```
#show running-config ip dhcp snooping
!
!
ip dhcp snooping bridge 1
ip dhcp snooping vlan 2 bridge 1
interface xe2
  ip dhcp snooping trust
!
```

The `show ip dhcp snooping bridge 1` command displays the configured information about DHCP Snooping.

```
#show ip dhcp snooping bridge 1
```

```
Bridge Group                               : 1
DHCP snooping is                           : Enabled
DHCP snooping option82 is                  : Disabled
Verification of hwaddr field is             : Disabled
Strict validation of DHCP packet is         : Disabled
Rate limit(pps)                           : 200
DB Write Interval(secs)                    : 300
DHCP snooping is configured on following VLANs : 2
DHCP snooping is operational on following VLANs : 2
```

DHCP snooping IP Source Guard is configured on the following Interface

Interface	Trusted
-----	-----
xe2	Yes

The `show ip dhcp snooping binding bridge 1` command displays the binding table entries associated with un-trusted interfaces.

```
#show ip dhcp snooping bridge 1
```

```
Bridge Group                : 1
DHCP snooping is            : Enabled
DHCP snooping option82 is   : Disabled
Verification of hwaddr field is : Disabled
Strict validation of DHCP packet is : Disabled
Rate limit(pps)             : 200
DB Write Interval(secs)     : 300
DHCP snooping is configured on following VLANs : 2
DHCP snooping is operational on following VLANs : 2
DHCP snooping trust is configured on the following Interfaces
Interface  Trusted
-----
xe2        Yes
DHCP snooping IP Source Guard is configured on the following Interfaces
Interface          Source Guard
-----
```

## DHCP Snooping with Option-82

When DHCP snooping with Option-82 is enabled on the switch, following behavior is expected:

1. The host generates a DHCP request and broadcasts it on the network.
2. When the switch receives DHCP request, it adds option-82 information in the packet.
3. If the IP address of the relay agent is configured, the switch adds the IP address in the DHCP packet.
4. The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
5. The DHCP server receives the packet. If the server is option-82 capable, it can use the information in the option-82 fields to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. The DHCP server then echoes the option-82 field in the DHCP reply.
6. The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch verifies that it originally inserted the option-82 data by inspecting the remote id and circuit id fields. The switch removes the option-82 field and forwards the packet to the switch port that connects to DHCP client that sent the DHCP request.

## Procedures

The following subsections provide examples of how to configure DHCP snooping with option-82.

The topology is the same as [Figure 6-14](#).

## Enable DHCP Snooping Globally

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol mstp	Create mstp or ieee vlan-bridge.
(config)#ip dhcp snooping bridge 1	Enable DHCP Snooping on the bridge

## Enable DHCP Snooping on a VLAN

configure terminal	Enter configure mode.
(config)#vlan 2 bridge 1	Configure a vlan for the bridge.
(config)#ip dhcp snooping vlan 2 bridge 1	Enable DHCP Snooping on the vlan 2

## Configure Ports connected to DHCP Server and DHCP Client

#configure terminal	Enter the configure mode
(config)#interface xe1	Specify the interface xe1 to be configured, connected to client and Enter interface mode
(config-if)#switchport	Configure the interface as a switch port.
(config-if)#bridge-group 1	Associate the interface xe1 with bridge-group 1.
(config-if)#switchport mode access	Configure the port as an access port
(config-if)#switchport access vlan 2	Bind the interface vlan 2 to the port.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Specify interface xe2 to be configured connected to server.
(config-if)#switchport	Configure the interface as a switch port.
(config-if)#bridge-group 1	Associate interface xe2 with bridge-group 1.
(config-if)#switchport mode access	Configure the port as an access port.
(config-if)#switchport access vlan 2	Bind the interface vlan 2 to the port.
(config-if)#exit	Exit interface mode.
(config)#exit	Exit the config mode.

## Configure Trusted and Untrusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as untrusted port

In this example, xe1 is connected to the DHCP client and xe2 is connected to the DHCP server.

- Configure xe1 connected to DHCP client as un-trusted port.
- Configure xe2 connected to the DHCP server as trusted port.

#configure terminal	Enter configure mode.
(config)#interface xe1	Specify the interface to be configured
(config-if)#no ip dhcp snooping trust	Disable the port as trusted.
#configure terminal	Enter configure mode.
(config)#interface xe2	Specify the interface to be configured
(config-if)#ip dhcp snooping trust	Enable the port as trusted.

## Enable option-82

#configure terminal	Enter configure mode.
(config)# ip dhcp snooping information option bridge 1	Configure DHCP snooping information option-82

## Validation

The `show running-config ip dhcp snooping` command displays the DHCP snooping commands configured on the device.

```
#show running-config ip dhcp snooping
!
!
ip dhcp snooping bridge 1
ip dhcp snooping information option bridge 1
ip dhcp snooping vlan 2 bridge 1
interface xe2
    ip dhcp snooping trust
!
```

```
#show ip dhcp snooping bridge 1
```

```
Bridge Group                : 1
DHCP snooping is            : Enabled
DHCP snooping option82 is   : Enabled
Verification of hwaddr field is : Disabled
Strict validation of DHCP packet is : Disabled
Rate limit(pps)             : 200
DB Write Interval(secs)     : 300
DHCP snooping is configured on following VLANs : 2
DHCP snooping is operational on following VLANs : 2
```

DHCP snooping trust is configured on the following Interfaces

Interface	Trusted
-----	-----
xe2	Yes

DHCP snooping IP Source Guard is configured on the following Interfaces

Interface	Source Guard
-----	-----

```
#show ip dhcp snooping binding bridge 1
```

```
Total number of static IPV4 entries      : 0
Total number of dynamic IPV4 entries      : 1
Total number of static IPV6 entries       : 0
Total number of dynamic IPV6 entries      : 0
```

---

MacAddress	IpAddress	Lease (sec)	Type	VLAN	Interface
-----	-----	-----	-----	-----	---
-----	-----	-----	-----	-----	---
6400.6afc.3ba1	192.168.1.2	600	dhcp-snooping	2	xe1

---

## Sample server dhcpd.conf for option-82

This example shows a server dhcpd.conf file for option-82 with remote-id and circuit-id suboptions.

```
Remote-id :
class "remote-id" {
match if option agent.remote-id = cc:37:ab:56:6d:80;--->Points to Snooping switch eth0
Mac address.
} # remote-id
subnet 192.168.1.0 netmask 255.255.255.0 {
pool {
    option subnet-mask 255.255.255.0;
    allow members of "remote-id";
    range 192.168.1.2 192.168.1.100;
    default-lease-time 600;
    max-lease-time 600;
    option subnet-mask 255.255.255.0;
    option domain-name "Domain1.com";
    option domain-name-servers 23.32.23.32,4.4.4.2;
    option ntp-servers 19.91.19.91,45.54.45.54,localhost1,19.91.19.91;
    option log-servers 10.12.16.17,10.12.16.16;
    option bootfile-name "Bootfile1";
    option tftp-server-name "Tftpserver1";
    option host-name "Omega";
}
}
```

Circuit-id:

```
class "circuit-id" {
match if option agent.circuit-id = 00:00:13:b6:00:02;---->Points to vlan and interface
index value.
} # circuit-id

subnet 192.168.1.0 netmask 255.255.255.0 {
pool {
    option subnet-mask 255.255.255.0;
    allow members of "circuit-id";
    range 192.168.1.2 192.168.1.100;
    default-lease-time 600;
    max-lease-time 600;
    option subnet-mask 255.255.255.0;
    option domain-name "Domain1.com";
    option domain-name-servers 23.32.23.32,4.4.4.2;
    option ntp-servers 19.91.19.91,45.54.45.54,localhost1,19.91.19.91;
```



---

```
    option log-servers 10.12.16.17,10.12.16.16;  
    option bootfile-name "Bootfile1";  
    option tftp-server-name "Tftpserver1";  
    option host-name "Omega";  
}  
}
```



## CHAPTER 7 DHCP Snooping IP Source Guard

### Overview

IPSG is a security feature that restricts IP traffic on non-routed, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database. Use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor. Enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP DHCP snooping binding table and denies all other traffic.

### Topology

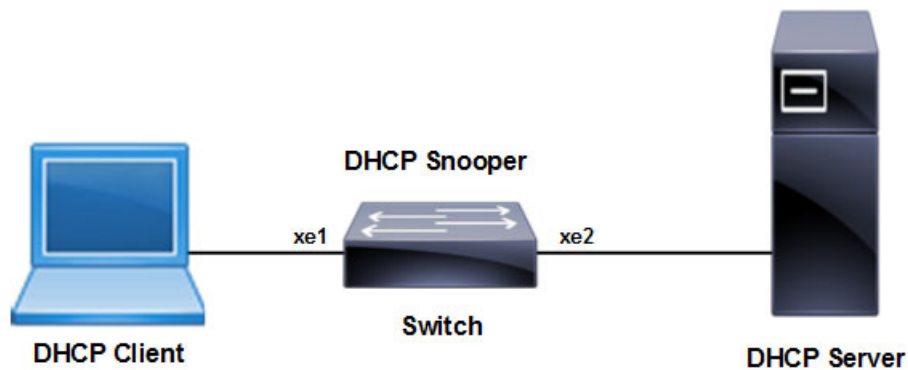


Figure 7-15: IP Source Guard Topology

### Configuration

#configure terminal	Enter the configure mode
(config)#bridge 1 protocol ieee vlan-bridge	Create IEEE VLAN bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#ip dhcp snooping bridge 1	Configure DHCP snooping for bridge 1
(config)#ip dhcp snooping information option bridge 1	Configure DHCP snooping information option 82
(config)#cpu-queue vrrp-rip-dhcp rate 0	Configure DHCP snooping ratelimit. Default value is 100
(config)#ip dhcp snooping vlan 2 bridge 1	Configure DHCP snooping for vlan 2 for bridge 1
(config)#ip dhcp snooping verify mac-address bridge 1	Configure DHCP snooping verify mac-address
(config)#interface xe2	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.

## DHCP Snooping IP Source Guard

(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip dhcp snooping trust	Configuring the interface as Trust. Basically this is configured on the interface which is connected to Server Side.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip verify source dhcp-snooping-vlan	Configuring IP source guard at Interface level and configured on the interface which is connected to client side
(config-if)#ip verify source access-group mode merge	Merge IPSG policy with other ACL
(config-if)#exit	Exit interface mode
(config)#ip dhcp snooping binding bridge 1 0011.1111.2222 2 ipv4 1.1.1.1 xe1	Configure Ipv4 Static Entry For DHCP snooping with MAC address and Source Address for an interface and vlan configured
(config)#ip dhcp snooping binding bridge 1 0022.2222.3333 2 ipv6 3ffe::1 xe1	Configure Ipv6 Static Entry For DHCP snooping with MAC address and Source Address for an interface and vlan configured
(config)#exit	Exit config mode
#clear ip dhcp snooping binding bridge 1	Clear DHCP binding tables which are learned dynamically

## Validation

Verify that DHCP snooping is enabled on the bridge:

```
#sh ip dhcp snooping bridge 1
Bridge Group                               : 1
DHCP snooping is                           : Enabled
DHCP snooping option82 is                  : Enabled
Verification of hwaddr field is             : Enabled
DHCP snooping is configured on following VLANs : 2
DHCP snooping is operational on following VLANs : 2
DHCP snooping trust is configured on the following Interfaces
Interface      Trusted
-----
xe2             Yes
DHCP snooping IP Source Guard is configured on the following Interfaces
Interface      Source Guard
-----
xe1             Yes
```

## Configuring Trusted and Un-trusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as untrusted port

In this example, xe1 is connected to the DHCP client and xe2 is connected to the DHCP server.

- Configure xe1 connected to DHCP client as un-trusted port.
- Configure xe2 connected to the DHCP server as trusted port.

#configure terminal	Enter configure mode.
(config)#interface xe1	Specify the interface to be configured
(config-if)#no ip dhcp snooping trust	Disable the port as trusted.
(config-if)#exit	Exit interface mode
(config)#interface xe2	Specify the interface to be configured
(config-if)#ip dhcp snooping trust	Enable the port as trusted.
(config-if)#exit	Exit interface mode

## Validation

Verify that static DHCP snooping entries are configured for the bridge:

```
#sh ip dhcp snooping binding bridge 1
Total number of static IPV4 entries           : 1
Total number of dynamic IPV4 entries          : 0
Total number of static IPV6 entries           : 1
Total number of dynamic IPV6 entries          : 0
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
0011.1111.2222	1.1.1.1	0	static	2	xe1
0022.2222.3333	3ffe::1	0	static	2	xe1

## Configuring IP Source Guard on LAG Port

In this example, the LAG port (sa2) is created, then physical interfaces are added.

#configure terminal	Enter the configure mode
(config)#bridge 1 protocol ieee vlan-bridge	Create IEEE VLAN bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#ip dhcp snooping bridge 1	Configure DHCP snooping for bridge 1
(config)#ip dhcp snooping information option bridge 1	Configure DHCP snooping information option 82
(config)#cpu-queue vrrp-rip-dhcp rate 0	Configure DHCP snooping ratelimit. Default value is 100
(config)#ip dhcp snooping vlan 2 bridge 1	Configure DHCP snooping for vlan 2 for bridge 1

## DHCP Snooping IP Source Guard

(config)#ip dhcp snooping verify mac-address bridge 1	Configure DHCP snooping verify mac-address
(config)#interface sa2	Enter Interface Mode
switchport	Configure the interface as Layer 2
bridge-group 1	Associate the interface with bridge group 1.
(config-if)#ip verify source dhcp-snooping-vlan	Configuring IP source guard at Interface level and configured on the interface which is connected to client side
(config-if)#ip verify source access-group mode merge	Merge IPSG policy with other ACL
(config-if)#exit	Exit interface mode
(config)#interface xe2	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip dhcp snooping trust	Configuring the interface as Trust. Basically this is configured on the interface which is connected to Server Side.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#static-channel-group 2	Configure Static Channel lag on the interface
(config-if)#exit	Exit interface mode
(config)#ip dhcp snooping binding bridge 1 0011.1111.2222 2 ipv4 1.1.1.1 sa2	Configure Ipv4 Static Entry For DHCP snooping with MAC address and Source Address for lag interface and vlan configured
(config)#ip dhcp snooping binding bridge 1 0022.2222.3333 2 ipv6 3ffe::1 sa2	Configure Ipv6 Static Entry For DHCP snooping with MAC address and Source Address for lag interface and vlan configured
(config)#exit	Exit config mode
#clear ip dhcp snooping binding bridge 1	Clear DHCP binding tables which are learned dynamically

## Validation

Verify that DHCP snooping is enabled on the bridge with the static LAG interface:

```
#sh ip dhcp snooping bridge 1
Bridge Group                : 1
DHCP snooping is            : Enabled
DHCP snooping option82 is    : Enabled
Verification of hwaddr field is : Enabled
DHCP snooping is configured on following VLANs : 2
DHCP snooping is operational on following VLANs : 2
```

---

DHCP snooping trust is configured on the following Interfaces

Interface	Trusted
-----------	---------

-----

-----

Xe2	Yes
-----	-----

DHCP snooping IP Source Guard is configured on the following Interfaces

Interface	Source Guard
-----------	--------------

-----

-----

sa2	Yes
-----	-----

Verify that static DHCP snooping or source guard entries are configured for the bridge with the LAG interface:

```
#sh ip dhcp snooping binding bridge 1
```

```
Total number of static IPV4 entries           : 1
```

```
Total number of dynamic IPV4 entries          : 0
```

```
Total number of static IPV6 entries           : 1
```

```
Total number of dynamic IPV6 entries          : 0
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
-----	-----	-----	-----	----	-----
0011.1111.2222	1.1.1.1	0	static	2	sa2
0022.2222.3333	3ffe::1	0	static	2	sa2





---

## CHAPTER 8 DHCP Snooping over MLAG

---

---

### Overview

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. It is a layer-2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. With DHCP snooping, the physical location of hosts can be tracked, only the IP addresses assigned for the hosts can be used, only the authorized DHCP servers are accessible. DHCP snooping can prevent attackers from adding their own DHCP servers to the network. DHCP snooping allows only clients with specific IP/MAC addresses to have access to the network.

The DHCP snooping over MLAG feature synchronizes the DHCP snooping binding database between the MLAG peers. If one of the MLAG peer node or MLAG link is down, the DHCP request / reply messages should be honoured by the partner.

DHCP snooping is supported over Active-Active MLAG mode using Static & Dynamic Channel group while Active-Standby MLAG mode using Static Channel group.

## Topology

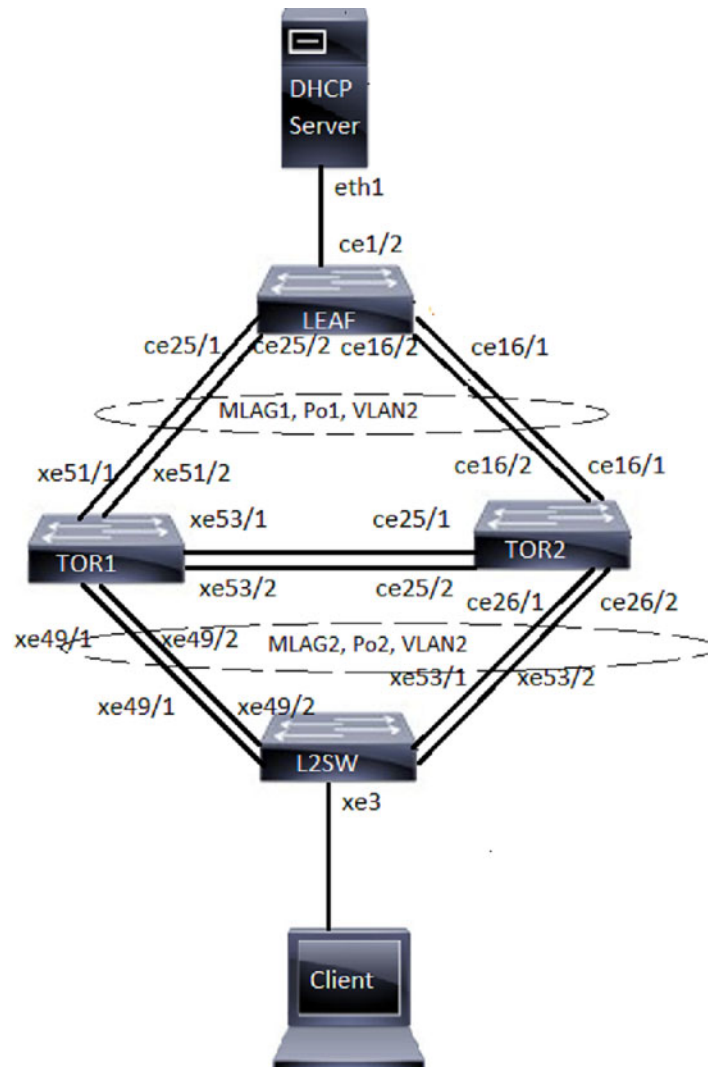


Figure 8-16: DHCP Snooping over MLAG

## Configuration

### LEAF:

#configure terminal	Configure terminal.
(config)#bridge 1 protocol rstp vlan-bridge	Configuring the rstp vlan bridge
(config)#vlan 2 bridge 1 state enable	Configure VLAN for the bridge
(config)#interface po1	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#interface ce1/2	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#interface ce16/1	Enter interface mode
(config-if)#channel-group 1 mode active	Enable channel-group 1
(config-if)#exit	Exit interface mode
(config)#interface ce16/2	Enter interface mode
(config-if)#channel-group 1 mode active	Enable channel-group 1
(config-if)#exit	Exit interface mode
(config)#interface ce25/1	Enter interface mode
(config-if)#channel-group 1 mode active	Enable channel-group 1
(config-if)#exit	Exit interface mode
(config)#interface ce25/2	Enter interface mode
(config-if)#channel-group 1 mode active	Enable channel-group 1
(config-if)#exit	Exit the configure mode

### TOR1:

#configure terminal	Configure terminal.
(config)#bridge 1 protocol rstp vlan-bridge	Configuring the rstp vlan bridge
(config)#vlan 2 bridge 1 state enable	Configure VLAN for the bridge
(config)#ip dhcp snooping bridge 1	Enable DHCP Snooping on the bridge
(config)#ip dhcp snooping vlan 2 bridge 1	Enable DHCP Snooping on the vlan 2
(config)#interface mlag1	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2

## DHCP Snooping over MLAG

(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#ip dhcp snooping trust	Enable the port as trusted.
(config-if)#exit	Exit interface mode
(config)#interface mlag2	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 trunk	Configure the mode as trunk
(config-if)# switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#interface po1	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#mlag 1	Map po1 to mlag1
(config-if)#exit	Exit interface mode
(config)#interface po2	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#mlag 2	Map po2 to mlag2
(config-if)#exit	Exit interface mode
(config)#interface po5	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#interface xe49/1	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit interface mode
(config)#interface xe49/2	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit interface mode
(config)#interface xe51/1	Enter Interface mode
(config-if)#channel-group 1 mode active	Enable channel-group 1
(config-if)#exit	Exit interface mode
(config)#interface xe51/2	Enter Interface mode
(config-if)#channel-group 1 mode active	Enable channel-group 1
(config-if)#exit	Exit interface mode
(config)#interface xe53/1	Enter Interface mode
(config-if)#channel-group 5 mode active	Enable channel-group 5

---

(config-if)#exit	Exit interface mode
(config)#interface xe53/2	Enter Interface mode
(config-if)#channel-group 5 mode active	Enable channel-group 5
(config-if)#exit	Exit interface mode
(config)#mcec domain configuration	Enter MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the mlag domain
(config-mcec-domain)#domain-system-number 2	Configure the domain system number
(config-mcec-domain)#intra-domain-link po5	Specify the intra domain link for MLAG communication
config-mcec-domain)#end	Exit the configure mode

---

**TOR2:**

#configure terminal	Configure terminal.
(config)#bridge 1 protocol rstp vlan-bridge	Configuring the rstp vlan bridge
(config)#vlan 2 bridge 1 state enable	Configure VLAN for the bridge
(config)#ip dhcp snooping bridge 1	Enable DHCP Snooping on the bridge
(config)#ip dhcp snooping vlan 2 bridge 1	Enable DHCP Snooping on the vlan 2
(config)#interface mlag1	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#ip dhcp snooping trust	Enable the port as trusted.
(config-if)#exit	Exit interface mode
(config)#interface mlag2	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#interface po1	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#mlag 1	Map po1 to mlag1
(config-if)#exit	Exit interface mode
(config)#interface po2	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#mlag 2	Map po2 to mlag2
(config-if)#exit	Exit interface mode
(config)#interface po5	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#interface cel6/1	Enter Interface mode
(config-if)#channel-group 1 mode active	Enable channel-group 1
(config-if)#exit	Exit interface mode
(config)#interface cel6/2	Enter Interface mode
(config-if)#channel-group 1 mode active	Enable channel-group 1
(config-if)#exit	Exit interface mode

(config)#interface ce25/1	Enter Interface mode
(config-if)#channel-group 5 mode active	Enable channel-group 5
(config-if)#exit	Exit interface mode
(config)#interface ce25/2	Enter Interface mode
(config-if)#channel-group 5 mode active	Enable channel-group 5
(config-if)#exit	Exit interface mode
(config)#interface ce26/1	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit interface mode
(config)#interface ce26/2	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit interface mode
(config)#mcec domain configuration	Enter MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the mlag domain
(config-mcec-domain)#domain-system-number 1	Configure the domain system number
(config-mcec-domain)#intra-domain-link po5	Specify the intra domain link for MLAG communication
(config-mcec-domain)#end	Exit the configure mode

**L2SW:**

#configure terminal	Configure terminal.
(config)#bridge 1 protocol rstp vlan-bridge	Configuring the rstp vlan bridge
(config)#vlan 2 bridge 1 state enable	Configure VLAN for the bridge
(config-if)#interface po2	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#interface xe3	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#interface xe49/1	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit interface mode
(config)#interface xe49/2	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit interface mode
(config)#interface xe53/1	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit interface mode
(config)#interface xe53/2	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit the configure mode

**Static MLAG configuration for TOR1 and TOR2**

Note: Only mlag related configs for static MLAG is provided. While rest of the configuration is similar to dynamic.



**TOR1:**

#configure terminal	Configure terminal.
(config)#interface mlag1	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#mode active-standby	Configure mlag mode for mlag1
(config-if)#ip dhcp snooping trust	Enable the port as trusted.
(config-if)#exit	Exit interface mode
(config)#interface mlag2	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#mode active-active	Configure mlag mode for mlag2
(config-if)#exit	Exit interface mode
(config)#interface sa1	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#mlag 1	Map sa1 to mlag1
(config-if)#exit	Exit interface mode
(config)#interface sa2	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#mlag 2	Map sa2 to mlag2
(config-if)#exit	Exit interface mode
(config)#interface sa5	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#mcec domain configuration	Enter MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the mlag domain
(config-mcec-domain)#domain-system-number 1	Configure the domain system number
(config-mcec-domain)#intra-domain-link sa5	Specify the intra domain link for MLAG communication
(config-mcec-domain)#end	Exit the configure mode

**TOR2:**

#configure terminal	Configure terminal.
(config)#interface mlag1	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#mode active-standby	Configure mlag mode for mlag1
(config-if)#ip dhcp snooping trust	Enable the port as trusted.
(config-if)#exit	Exit interface mode
(config)#interface mlag2	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#mode active-active	Configure mlag mode for mlag2
(config-if)#exit	Exit interface mode
(config)#interface sa1	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#mlag 1	Map sa1 to mlag1
(config-if)#exit	Exit interface mode
(config)#interface sa2	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#mlag 2	Map sa2 to mlag2
(config-if)#exit	Exit interface mode
(config)#interface sa5	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 trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#mcec domain configuration	Enter MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the mlag domain
(config-mcec-domain)#domain-system-number 2	Configure the domain system number
(config-mcec-domain)#intra-domain-link sa5	Specify the intra domain link for MLAG communication
(config-mcec-domain)#end	Exit the configure mode

---

## Validation

### 1. Verify Dhcps Sync PDUs:

```
TOR1#show mcec statistics
```

```
Unknown MCCPDU received on the system          : 0
```

```
-----  
IDP po5  
-----
```

```
Valid RX Hello PDUs          : 2373  
Valid TX Hello PDUs          : 2373  
Valid RX Info PDUs           : 12  
Valid TX Info PDUs           : 20
```

```
Valid RX Mac Sync PDUs       : 20  
Valid TX Mac Sync PDUs       : 20
```

```
Valid RX Dhcps Sync PDUs     : 1  
Valid TX Dhcps Sync PDUs     : 3
```

```
MLAG 1
```

```
Valid RX Info PDUs           : 6  
Valid TX Info PDUs           : 10
```

```
MLAG 2
```

```
Valid RX Info PDUs           : 6  
Valid TX Info PDUs           : 10
```

```
TOR1#
```

```
TOR2#show mcec statistics
```

```
Unknown MCCPDU received on the system          : 0
```

```
-----  
IDP po5  
-----
```

```
Valid RX Hello PDUs          : 2384  
Valid TX Hello PDUs          : 2385  
Valid RX Info PDUs           : 18  
Valid TX Info PDUs           : 12
```

```
Valid RX Mac Sync PDUs       : 20  
Valid TX Mac Sync PDUs       : 16
```

```
Valid RX Dhcps Sync PDUs     : 3  
Valid TX Dhcps Sync PDUs     : 1
```

```
MLAG 1
Valid RX Info PDUs      : 9
Valid TX Info PDUs      : 6

MLAG 2
Valid RX Info PDUs      : 9
Valid TX Info PDUs      : 6
```

2. Verify dhcp binding entires:

```
TOR2#
TOR1# show ip dhcp snooping binding bridge 1
```

```
Total number of static IPV4 entries      : 0
Total number of dynamic IPV4 entries      : 1
Total number of static IPV6 entries       : 0
Total number of dynamic IPV6 entries      : 0
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interfa ce
-----	-----	-----	-----	----	-----
80a2.35e9.8323	20.20.20.2	315	dhcp-snooping	2	m1ag2

```
TOR1#
TOR2#show ip dhcp snooping binding bridge 1
```

```
Total number of static IPV4 entries      : 0
Total number of dynamic IPV4 entries      : 1
Total number of static IPV6 entries       : 0
Total number of dynamic IPV6 entries      : 0
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
-----	-----	-----	-----	----	-----
80a2.35e9.8323	20.20.20.2	315	dhcp-snooping	2	m1ag2

3. Verify that DHCP snooping is enabled on the bridge

```
TOR2#
TOR1#show ip dhcp snooping bridge 1
```

```
Bridge Group      : 1
DHCP snooping is  : Enabled
DHCP snooping option82 is : Disabled
Verification of hwaddr field is : Disabled
Strict validation of DHCP packet is : Disabled
DB Write Interval(secs) : 300
```

---

```
DHCP snooping is configured on following VLANs      : 2
DHCP snooping is operational on following VLANs     : 2
```

```
DHCP snooping trust is configured on the following Interfaces
```

Interface	Trusted
-----	-----
mlag1	Yes
po5	Yes

```
DHCP snooping IP Source Guard is configured on the following Interfaces
```

Interface	Source Guard
-----	-----

```
TOR1#
```

```
TOR2#show ip dhcp snooping bridge 1
```

```
Bridge Group                : 1
DHCP snooping is            : Enabled
DHCP snooping option82 is   : Disabled
Verification of hwaddr field : Disabled
Strict validation of DHCP packet is : Disabled
DB Write Interval(secs)     : 300
DHCP snooping is configured on following VLANs : 2
DHCP snooping is operational on following VLANs : 2
```

```
DHCP snooping trust is configured on the following Interfaces
```

Interface	Trusted
-----	-----
mlag1	Yes
po5	Yes

```
DHCP snooping IP Source Guard is configured on the following Interfaces
```

Interface	Source Guard
-----	-----

```
TOR2#
```

#### 4. Verify dhcp snooping running configs

```
TOR1#show running-config ip dhcp snooping
!
debug ip dhcp snooping all
!
ip dhcp snooping bridge 1
ip dhcp snooping vlan 2 bridge 1
interface mlag1
```

```
ip dhcp snooping trust
!
interface po5
ip dhcp snooping trust
!
TOR1#

TOR2#show running-config ip dhcp snooping
!
debug ip dhcp snooping all
!
ip dhcp snooping bridge 1
ip dhcp snooping vlan 2 bridge 1
interface mlag1
ip dhcp snooping trust
!
interface po5
ip dhcp snooping trust
!
TOR2#
```

### 5. Verify mlag details:

```
TOR2#show mlag domain details
```

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

```
Domain System Number      : 1
Domain Address             : 1111.2222.3333
Domain Priority            : 32768
Intra Domain Interface     : po5
```

```
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         : po1
Admin Key                  : 16385
Oper Key                   : 16385
Physical properties Digest : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22
```

---

```
Neigh Admin Key           : 32769
Neigh Physical Digest     : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22
Info RCV State            : Current
Info Periodic Time State  : Standby
Total Bandwidth           : 40g
Mlag Sync                 : IN_SYNC
Mlag Mode                 : Active-Active
Mlag State                 : UP
```

## MLAG-2

```
Mapped Aggregator        : po2
Admin Key                 : 16386
Oper Key                  : 16386
Physical properties Digest : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22
```

```
Neigh Admin Key           : 32770
Neigh Physical Digest     : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22
Info RCV State            : Current
Info Periodic Time State  : Standby
Total Bandwidth           : 40g
Mlag Sync                 : IN_SYNC
Mlag Mode                 : Active-Active
Mlag State                 : UP
```

## TOR2#

TOR1#show mlag domain details

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

```
Domain System Number      : 2
Domain Address             : 1111.2222.3333
Domain Priority            : 32768
Intra Domain Interface     : po5
```

```
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        : po1
Admin Key                 : 32769
```

## DHCP Snooping over MLAG

---

Oper Key : 16385  
Physical properties Digest : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22

Neigh Admin Key : 16385  
Neigh Physical Digest : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22

Info RCV State : Current  
Info Periodic Time State : Standby  
Total Bandwidth : 40g  
Mlag Sync : IN\_SYNC  
Mlag Mode : Active-Active  
Mlag State : UP

### MLAG-2

Mapped Aggregator : po2  
Admin Key : 32770  
Oper Key : 16386  
Physical properties Digest : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22

Neigh Admin Key : 16386  
Neigh Physical Digest : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22

Info RCV State : Current  
Info Periodic Time State : Standby  
Total Bandwidth : 40g  
Mlag Sync : IN\_SYNC  
Mlag Mode : Active-Active  
Mlag State : UP

### TOR1#



## CHAPTER 9 DHCPv6 Prefix Delegation

### Overview

The prefix delegation feature lets a DHCP server assign prefixes chosen from a global pool to DHCP clients, that is how the Customer Premise Equipment (CPE) learns the prefix. The learnt prefix shall be used by the user to configure the IPv6 address on its LAN interface along with subnet prefix. The LAN hosts are learning the subnetted prefix through router advertisement (NDP protocol) messages, which enables the device to auto configure its own IPv6 addresses.

This feature would enable service providers to assign IP for the Customer Premise Equipment acting as a router between the service providers core network and subscribers internal network.

### Topology

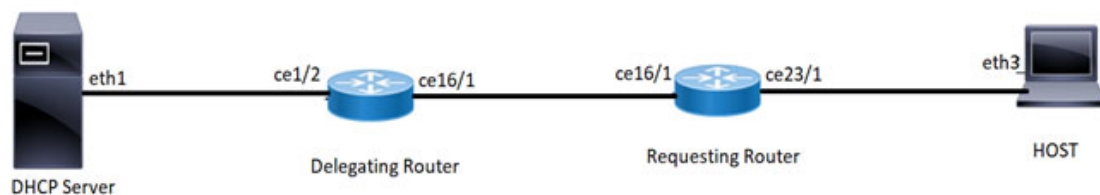


Figure 9-17: DHCPv6 Prefix Delegation

## Configuration

### DHCP RELAY-Delegating router(DR):

#configure terminal	configure terminal.
(config)#feature dhcp	Enable the feature dhcp. This is enabled in default.
(config)#ipv6 dhcp relay	By default, this will be enabled. It starts the ipv6 dhcp relay service.
(config)#ipv6 dhcp relay address 2001:101:0:1::131	The relay address configured should be server interface address connected to Delegating router.
(config)#interface ce1/2	Enter interface mode.
(config-if)#ipv6 address 2001:101:0:1::130/64	Configure ipv6 address on the interface ce1/2
(config-if)#ipv6 dhcp relay uplink	Configure relay uplink on the device connecting the server.
(config if)#exit	Exit interface mode.
(config)#interface ce16/1	Enter interface mode.
(config-if)#ipv6 address 3001:101:0:1::135/64	Configure ipv6 address on the interface ce16/1
(config-if)#ipv6 dhcp relay	Relay should be configured on the interface connecting to the client.
(config if)#exit	Exit interface mode.
(config)#ipv6 route 1212:501:102:1::/64 3001:101:0:1::254	Configure static route towards Host where next-hop address is address allocated on RR is learnt from DHCP server(IA_NA) and destination network configured by the user using learnt prefix(IA_PD)

### Requesting Router(RR):

#configure terminal	configure terminal.
(config)#interface ce16/1	Enter interface mode.
(config-if)#ipv6 dhcp address-prefix-len 64	Addition of address length option
(config-if)#ipv6 address dhcp	Configure IPv6 address DHCP.
(config-if)# ipv6 dhcp prefix-delegation DHCPv6_PREFIX	Include DHCPv6 prefix option in the DHCPv6 client request
(config if)#exit	Exit interface mode.
(config)#interface ce23/1	Enter interface mode.
(config-if)#ipv6 address DHCPv6_PREFIX ::1:0:0:0:1/64	Configure IPv6 address from the prefix learnt where "::1" is the subnet ID and last 64 bits are host ID.
(config if)#exit	Exit interface mode.
(config)#ipv6 route 2001:101:0:1::/64 3001:101:0:1::135	Configure static route towards server.

### HOST :

**Note:** CLI "ipv6 address autoconfig" is hidden and experimental as the host portion of ipv6 autoconfiguration using NDP is not fully implemented.

#configure terminal	configure terminal.
(config)#interface ce23/1	Enter interface mode.

(config-if)#ipv6 address autoconfig	Configure IPv6 autoconfig
(config if)#exit	Exit interface mode.

Linux host:

IPV6_AUTOCONF=yes	IPv6 autoconfig should be set to yes in interface config file.
-------------------	--

DHCP SERVER:

ifconfig eth1 inet6 add 2001:101:0:1::131/64	Configure ipv6 address on client facing interface
dhcpd -d -6 -cf /etc/dhcp/dhcpd6.conf eth1	Start server
ipv6 route 1212:501:102:1::/64 2001:101:0:1::130	Configure static route towards Requesting Router

Sample dhcpd6.conf file:

Note: Preferred and Max lifetimes must not be configured with same values.

```
#
# DHCPv6 Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd6.conf.sample
#   see dhcpd.conf(5) man page
#
preferred-lifetime 600;
default-lease-time 600;

subnet6 2001:101:0:1::/64 {
  range6 2001:101:0:1::129 2001:101:0:1::254;
}
subnet6 3001:101:0:1::/64 {
  range6 3001:101:0:1::129 3001:101:0:1::254;
  prefix6 1212:501:101:: 1212:501:102:: /48;
  option dhcp6.name-servers fec0:0:0:1::1;
  option dhcp6.domain-search "domain.example";
}
```

Validation

Delegation Router:

```
DR#show ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: default
DHCPv6 Servers configured: 2001:101:0:1::131
Interface          Uplink/Downlink
-----
ce1/2              Uplink
ce16/1             Downlink
```

### Requesting Router:

```
RR#show ipv6 dhcp interface
```

```
ce16/1 is in client mode
prefix name: DHCPv6_PREFIX
learned prefix: 1212:501:102::/48
preferred lifetime 600, valid lifetime 600
interfaces using the learned prefix
    ce23/1    1212:501:102:1::1
```

```
RR#show int ce23/1
Interface ce23/1
Scope: both
Flexport: Breakout Control Port (Active): Break Out Enabled
Hardware is ETH Current HW addr: cc37.abc9.7426
Physical:cc37.abc9.743f Logical:(not set)
Port Mode is Router
Interface index: 10025
Metric 1 mtu 1500 duplex-full link-speed 1g
Debounce timer: disable
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2021 Mar 02 09:44:05 (00:03:55 ago)
Statistics last cleared: 2021 Mar 02 09:44:05 (00:03:55 ago)
inet6 1212:501:102:1::1/64
inet6 fe80::ce37:abff:fec9:7426/64
ND router advertisements are sent approximately every 571 seconds
ND next router advertisement due in 434 seconds.
    ND router advertisements live for 1800 seconds
    Hosts use stateless autoconfig for addresses.
    5 minute input rate 2 bits/sec, 0 packets/sec
    5 minute output rate 23 bits/sec, 0 packets/sec
```

### HOST:

```
[root@localhost ~]# ifconfig -a
eth3      Link encap:Ethernet  HWaddr 00:07:E9:A5:23:4C
inet6 addr: 1212:501:102:1:207:e9ff:fea5:234c/64 Scope:Global
inet6 addr: fe80::207:e9ff:fea5:234c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:196985 errors:0 dropped:0 overruns:0 frame:0
TX packets:5733 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:23542362 (22.4 MiB)  TX bytes:710558 (693.9 KiB)
```

## CHAPTER 10 DHCPv6 Relay Prefix Delegation Route Injection Configuration

### Overview

The prefix delegation feature lets a DHCP server assign prefixes chosen from a global pool to DHCP clients. The DHCP client can then configure an IPv6 address on its LAN interface using the prefix it received. It will then send router advertisements including the prefix, allowing other devices to auto-configure their own IPv6 addresses.

If the network topology where Prefix Delegation is running has a Relay agent, then a route needs to be injected in Delegating Router, so that the traffic from the DHCP server-side shall be forwarded towards the Requesting Router.

### Topology

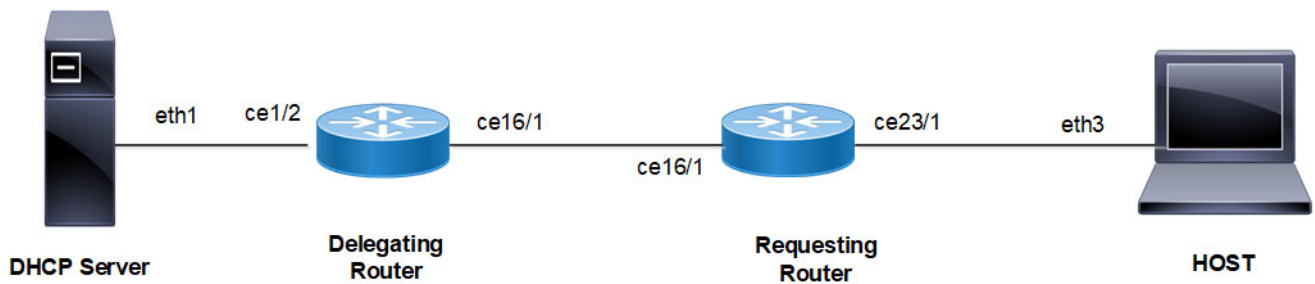


Figure 10-18: DHCPv6 Relay Delegating Configuration

### DHCP Relay - Delegating Router (DR)

#configure terminal	Enter configure mode.
(config)#feature dhcp	Enable the feature DHCP. This is enabled by default.
(config)#ipv6 dhcp relay	By default, this will be enabled. It starts the IPv6 DHCP relay service.
(config)#ipv6 dhcp relay address 2001:101:0:1::131	The relay address configured should be server interface address connected to Delegating Router.
(config)#interface ce1/2	Enter interface mode.
(config-if)#ipv6 address 2001:101:0:1::130/64	Configure IPv6 address on the interface ce1/2
(config-if)#ipv6 dhcp relay uplink	Configure relay uplink on the device connecting the server.
(config-if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running
(config)#interface ce16/1	Enter interface mode.
(config-if)#ipv6 address 3001:101:0:1::135/64	Configure IPv6 address on the interface ce16/1

## DHCPv6 Relay Prefix Delegation Route Injection Configuration

(config-if)#ipv6 dhcp relay	Relay should be configured on the interface connecting to the client.
(config-if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running
(config)#ipv6 dhcp relay pd-route-injection	Configure to enable auto route injection.

### Requesting Router (RR)

#configure terminal	Enter configure mode.
(config)#interface ce16/1	Enter interface mode.
(config-if)#ipv6 address dhcp	Configure IPv6 address DHCP.
(config-if)#ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER	Configure IPv6 DHCP prefix-delegation
(config-if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running configuration
(config)#interface ce23/1	Enter interface mode.
(config-if)#ipv6 address PREFIX_FROM_SERVER ::1:0:0:0:1/64	Configure IPv6 address from the prefix learnt
(config-if)#ipv6 nd ra-interval 4	Configure ra-interval
(config-if)#exit	Exit interface mode.
(config)#ipv6 route 2001:101:0:1::/64 3001:101:0:1::135	Configure static route towards server
(config)#commit	Commit the candidate configuration to the running configuration

### HOST

#configure terminal	Enter configure mode.
(config)#interface ce23/1	Enter interface mode.
(config-if)#ipv6 address autoconfig	Configure IPv6 autoconfig
(config if)#exit	Exit interface mode.
(config)#ipv6 route 2001:101:0:1::/64 fe80::ce37:abff:fec9:7426 ce23/1	Configure static route towards server
(config)#commit	Commit the candidate configuration to the running

### Linux Host

IPV6_AUTOCONF=yes	IPv6 autoconfig should be set to yes in interface config file.
-------------------	--

### DHCP Server

ifconfig eth1 inet6 add 2001:101:0:1::131/64	Configure IPv6 address on client facing interface
dhcpd -d -6 -cf /etc/dhcp/dhcpd6.conf eth1	Start server
ipv6 route 1212:501:102:1::/64 2001:101:0:1::130	Configure static route towards Requesting Router

**Sample dhcpd6.conf file**

```
#
#DHCPv6 Server Configuration file.
#see /usr/share/doc/dhcp*/dhcpd6.conf.sample
#see dhcpd.conf(5) man page
#
preferred-lifetime 400;
default-lease-time 600;

subnet6 2001:101:0:1::/64 {
range6 2001:101:0:1::129 2001:101:0:1::254;
}
subnet6 3001:101:0:1::/64 {
range6 3001:101:0:1::129 3001:101:0:1::254;
prefix6 1212:501:101:: 1212:501:102:: /48;
option dhcp6.name-servers fec0:0:0:1::1;
option dhcp6.domain-search "domain.example";
}
```

**Validation****Delegation Router (DR)**

```
DR#sh ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: default
  DHCPv6 Servers configured: 2001:101:0:1::131
  DHCPv6 IA_PD Route injection: Enabled
  Interface                      Uplink/Downlink
  -----                      -
  cel/2                          Downlink
  cel6/1                         Uplink

DR#sh ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, D- DHCP, R - RIP,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 19:24:04
D      1212:501:102::/48 [80/0] via fe80::eac5:7aff:fe64:4a20, cel6/1, 00:00:01
C      2001:101:0:1::/64 via ::, xe4, 03:42:58
C      3001:101:0:1::/64 via ::, xe2, 02:51:04
C      4001:101:0:1::/64 via ::, xe5, 03:14:41
C      fe80::/64 via ::, xe9, 00:41:39

#sh ipv6 dhcp pd-route
VRF : default
```

1212:501:102::/48 via fe80::eac5:7aff:fe64:4a20, ce16/1, (2019-05-30 14:02:50 - 2019-05-30 14:04:50)

### Requesting Router (RR)

```
RR#show ipv6 dhcp interface
```

```
ce16/1 is in client mode
prefix name: PREFIX_FROM_SERVER1
learned prefix: 1212:501:102::/48
preferred lifetime 600, valid lifetime 600
interfaces using the learned prefix
ce23/1      1212:501:102:1::1
```

```
RR#sh ipv6 interface ce23/1 brief
```

Interface	IPv6-Address	Admin-Status
Ce23/1	*1212:501:102:1::1 fe80::ce37:abff:fec9:7426	[up/up]

```
RR#show int ce23/1
```

```
Interface ce23/1
Scope: both
Flexport: Breakout Control Port (Active): Break Out Enabled
Hardware is ETH Current HW addr: cc37.abc9.7426
Physical:cc37.abc9.743f Logical:(not set)
Port Mode is Router
Interface index: 10025
Metric 1 mtu 1500 duplex-full link-speed 1g
Debounce timer: disable
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2021 Mar 02 09:44:05 (00:03:55 ago)
Statistics last cleared: 2021 Mar 02 09:44:05 (00:03:55 ago)
inet6 1212:501:102:1::1/64
inet6 fe80::ce37:abff:fec9:7426/64
ND router advertisements are sent approximately every 571 seconds
ND next router advertisement due in 434 seconds.
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
5 minute input rate 2 bits/sec, 0 packets/sec
5 minute output rate 23 bits/sec, 0 packets/sec
```

### HOST

```
[root@localhost ~]#ifconfig -a
eth3      Link encap:Ethernet  HWaddr 00:07:E9:A5:23:4C
inet6 addr: 1212:501:102:1:207:e9ff:fea5:234c/64 Scope:Global
inet6 addr: fe80::207:e9ff:fea5:234c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:196985 errors:0 dropped:0 overruns:0 frame:0
```



TX packets:5733 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:23542362 (22.4 MiB) TX bytes:710558 (693.9 KiB)

N4#show ipv6 interface xe7 brief

Interface	IPv6-Address	Admin-Status
ce23/1	*1212:501:102:1:6821:5fff:fe55:4a27	
	fe80::6a21:5fff:fe55:4a27	[up/up]



# CHAPTER 11 DHCP Server Configuration

## Overview

A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

## DHCP Server Configuration for IPv4

Before configuring make sure that DHCP server is ready.

## Topology

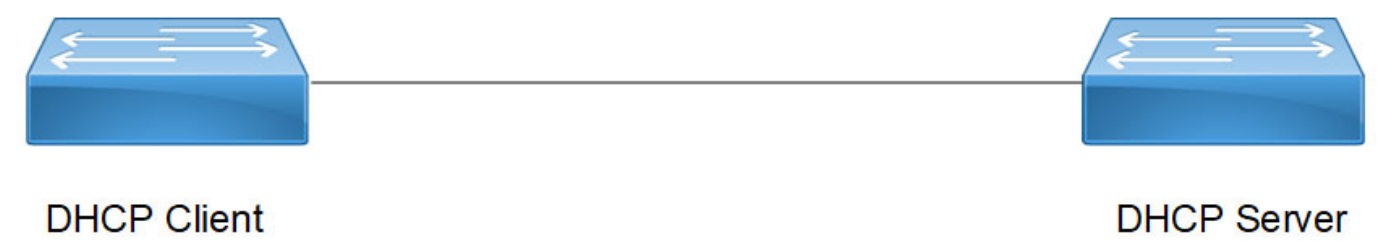


Figure 11-19: DHCP IPv4 topology

## Configuration

### DHCP IPv4 Client Interface

#configure terminal	Enter Configure mode.
(config)#interface xe1	Specify the interface (xe1) to be configured and enter the interface mode.
(config-if)#ip address dhcp	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
(config-if)#ip dhcp client request dns-nameserver	The client requests for the DNS name server.
(config-if)#ip dhcp client request ntp-server	The client requests for the NTP server .
(config-if)#ip dhcp client request host-name	The client requests for the Name of the client.
(config-if)#ip dhcp client request log-server	The client requests for the log server.
(config if)#exit	Exit interface mode.

## DHCP IPv4 Server Interface

#configure terminal	Enter Configure mode.
(config)#interface xe2	Specify the interface (xe2) to be configured and enter the interface mode.
(config-if)#ip address 10.10.10.1/24	Configure the IP address to the server interface.
(config-if)#ip address dhcp	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
(config if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running configuration.

## DHCP IPv4 Server Feature

#configure terminal	Enter Configure mode.
(config)#ip vrf vrf1	Configure IP VRF name.
(config-vrf)#ip dhcp server max-lease-time 100	Configure max lease time.
(config-vrf)#ip dhcp server default-lease-time 100	Configure default lease time.
(config-vrf)#ip dhcp server pool test	Configure DHCP server pool name.
(dhcp-config)#network 3.3.3.0 netmask 255.255.255.0	Configure network and netmask.
(dhcp-config)#address range low-address 3.3.3.1 high-address 3.3.3.4	Configure address IPv4 range.
(dhcp-config)#boot-file test	Configure boot-file name.
(dhcp-config)#host-name dhcp-server	Configure host name.
(dhcp-config)#ntp-server 4.4.4.5	Configure NTP server.
(dhcp-config)#log-server 5.5.5.6	Configure log server.
(dhcp-config)#dns-server 5.5.5.5	Configure DNS server.
(dhcp-config)#tftp-server 5.5.5.6	Configure TFTP server.
(dhcp-config)#boot-file test	Configure boot-file name.

## Validation

### Client

```
OcNOS#show running-config dhcp
interface eth0
  ip address dhcp
!
interface xe47
  ip address dhcp
ip dhcp client request dns-nameserver
ip dhcp client request host-name
ip dhcp client request log-server
```

```
ip dhcp client request ntp-server
!  
!
```

```
OcNOS#show ip int br
```

'\*' - address is assigned by dhcp client

Interface	IP-Address	Admin-Status	Link-Status
ce54	unassigned	up	down
eth0	*10.12.122.114	up	up
lo	127.0.0.1	up	up
lo.management	127.0.0.1	up	up
xe47	*10.10.10.2	up	up
xe48	unassigned	up	down

```
OcNOS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#int xe6
OcNOS(config-if)#ip dhcp client request host-name
OcNOS(config-if)#commit
OcNOS(config-if)#
OcNOS(config-if)#
OcNOS(config-if)#end
dhcp-client#
dhcp-client#
dhcp-client#
dhcp-client#sh hostname
*dhcp-client
```

\* - Hostname learnt by DHCP Client.  
dhcp-client#

## Server

```
OcNOS#show run dhcp
interface eth0
 ip address dhcp
!  
!  
  
ip dhcp server max-lease-time 100
ip dhcp server default-lease-time 100
ip dhcp server pool test
 network 10.10.10.0 netmask 255.255.255.0
 address range low-address 10.10.10.1 high-address 10.10.10.5
 host-name dhcp-client
 boot-file test
 tftp-server 5.5.5.6
 ntp-server 4.4.4.5
 log-server 5.5.5.6
```

```
dns-server 5.5.5.5
interface ge5
ip dhcp server
```

## DHCP Server Configuration for IPv6

Before configuring make sure that DHCP server is ready.

### Topology



Figure 11-20: DHCP IPv6 topology

### Configuration

#### DHCP IPv6 Client Interface

#configure terminal	Enter Configure mode.
(config)#interface xe47	Specify the interface (xe47) to be configured and enter the interface mode.
(config-if)#ipv6 address dhcp	The client requests for the IPv6 address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
(config-if)#ipv6 dhcp client request dns-nameserver	The client requests for the DNS name server.
(config-if)#ipv6 dhcp client request ntp-server	The client requests for the NTP server.
(config-if)#ipv6 dhcp client request domain-search	The client request for IPv6 domain search.
(config-if)#ipv6 dhcp client request vendor-specific-information	The client request for IPv6 vendor-specific-information.
(config-if)#ipv6 dhcp client request rapid-commit	The client request to enable rapid-commit.
(config if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running configuration.

## DHCP IPv6 Server Interface

#configure terminal	Enter Configure mode.
(config)#interface xe2	Specify the interface (xe2) to be configured and enter the interface mode.
(config-if)#ipv6 address dhcp	The client requests for the IPv6 address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
(config-if)#ipv6 address 2001::1/64	Configure the IPv6 address to the server interface.
(config if)#ipv6 dhcp server	Configure an interface as a DHCP server starting interface.
(config if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running configuration.

## DHCP IPv6 Server Feature

#configure terminal	Enter Configure mode
(config)#ip vrf vrf1	Configure IP VRF name
(config-vrf)#ipv6 dhcp server preference	Configure IPv6 DHCP server preference
(config-vrf)#ipv6 dhcp server rapid-commit	Configure IPv6 DHCP server rapid-commit
(config-vrf)#ipv6 dhcp server pool test	Configure IPv6 DHCP server pool name
(dhcp6-config)#network 2001:: netmask 64	Configure IPv6 network and netmask
(dhcp6-config)#address range low-address 2001::1 high-address 2001::124	Configure IPv6 address range
(dhcp6-config)#vendor-options 00:00:09:bf:63	Configure IPv6 vendor option
(dhcp6-config)#ntp-server 4001::1	Configure IPv6 NTP server
(dhcp6-config)#dns-server 3001::1	Configure IPv6 DNS server
(dhcp6-config)#log-server 5.5.5.6	Configure log server
(dhcp6-config)#domain-name abcd	Configure domain name
(dhcp6-config)#tftp-server 5.5.5.6	Configure TFTP server
(dhcp6-config)#boot-file test	Configure boot-file name

## Validation

### Client

```
OcNOS#sh running-config dhcp
interface eth0
  ip address dhcp
!
interface xe2
  ipv6 dhcp client request dns-nameserver
  ipv6 dhcp client request domain-search
  ipv6 dhcp client request ntp-server
  ipv6 dhcp client request rapid-commit
```

## DHCP Server Configuration

---

```
ipv6 dhcp client request vendor-specific-information
ipv6 address dhcp
!
```

```
OcNOS#show ipv6 int br
Interface                IPv6-Address                Admin-Status
-----
tun0                      unassigned                   [up/down]
eth0                      fe80::e69d:73ff:fe05:8100    [up/up]
lo                         ::1                           [up/up]
lo.management             ::1                           [up/up]
xe45                      unassigned                   [up/down]
xe46                      unassigned                   [up/down]
xe47                      *2001::124
                          fe80::e69d:73ff:fe84:8137    [up/up]
xe48                      unassigned                   [up/down]
```

### Server

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ipv6 dhcp server rapid-commit
ipv6 dhcp server preference
ipv6 dhcp server pool test
 network 2001:: netmask 64
 address range low-address 2001::1 high-address 2001::124
 vendor-options 00:00:09:bf:63
 ntp-server 4001::1
 dns-server 3001::1
 domain-name abcd
interface xe2
 ipv6 dhcp server
!
```



## CHAPTER 12 DNS Configuration

### Overview

The Domain Name System (DNS) is an Internet service that translates domain names into IP addresses. When a domain name is used, DNS service translates the name into the corresponding IP address. If one DNS server does not know how to translate a particular domain name, it gathers information from other Domain Name Systems to obtain the correct IP address.

### Support for In-band Management over default VRF

OcNOS offers support for DNS over default and management VRFs via in-band management interface & OOB management interface, respectively.

The feature can be enabled to run on default and management VRF simultaneously. By default, it runs on management VRF.

### Topology

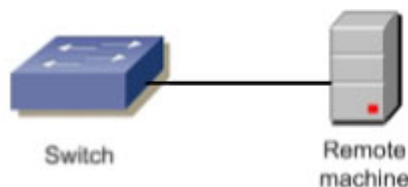


Figure 12-21: DNS sample topology

### Configuration

#configure terminal	Enter Configure mode.
(config)#ip name-server vrf management 10.12.17.11	This add a IPv4 Name Server to the DNS.
(config)#ip name-server vrf management 10.1.1.2	This add a IPv4 Name Server to the DNS.
(config)#ip host vrf management BINGO 10.1.1.1	This will add IPv4 host to the DNS
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode.

### Validation Commands

```
#show hosts vrf management
VRF: default
```

```
DNS lookup is disabled
Default domain is empty
```

```
DNS domain list is empty

Name Servers      : 10.12.17.11 10.1.1.2
Host              Address
-----
BINGO             10.1.1.1

* - Values assigned by DHCP Client.
```

Configuration

#configure terminal	Enter Configure mode.
(config)#ip name-server vrf management 3001::1	This add a IPv6 Name Server to the DNS.
(config)#ip host vrf management bingo 5001::1	This will add IPv6 host to the DNS
(config)#commit	Commit the Candidate configuration to the running configuration
(config)#exit	Exit configure mode.

Validation Commands

```
OcNOS#show hosts vrf management
      VRF: management

DNS lookup is enabled
Default domain is empty
DNS domain list is empty

Name Servers      : 3001::1
Host              Address
-----
bingo             5001::1

* - Values assigned by DHCP Client.
OcNOS#
```

## CHAPTER 13 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).

Note:

- 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 13-22: 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

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.

```
#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

```
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.

To get the log messages displayed , change the logging leve 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

```
#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
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 xel1	Enter into interface level
(config-if)#no link-flap errdisable	Disable link-flap errdisable for interface

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 xel1
!
interface xel1
  description *1/2 member of PO3 - Connected to IXIA 6/6*
  channel-group 3 mode active
  no link-flap errdisable
!
```

## CHAPTER 14 Ethernet Interface Loopback Support Configurations

This section contains the Ethernet Interface Loopback Support configuration example.

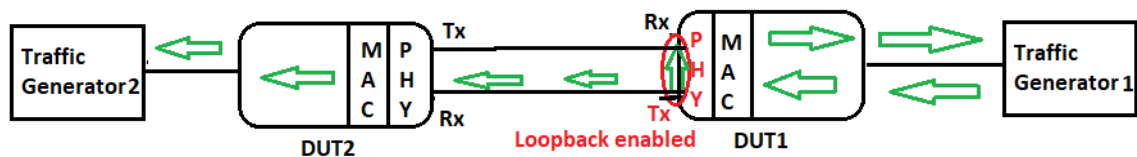
### Overview

This feature support is to provide additional hardware diagnostic functionality for physical ports on boards. This feature will enable the user to determine if there are any issues in the physical port at the MAC and the PHY layer.

To achieve this functionality, the Ethernet interfaces can be configured as the loopback interfaces. Looping back the packets are possible either at MAC layer or at PHY layer. Also packets can be looped either from Egress to Ingress or Ingress to Egress. On enabling this feature, if all the TX packets are looped back to RX, it indicates there is no issue with the hardware at the particular layer configured, either MAC or PHY.

### Local Loopback

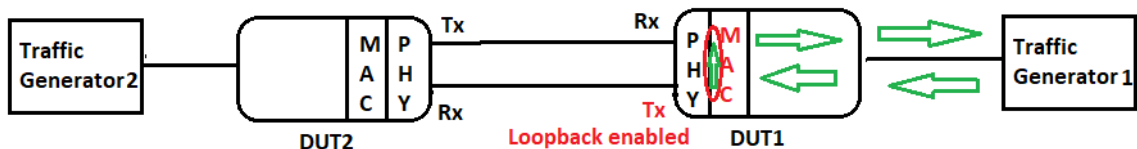
#### Tx PHY Loopback



When the loopback Tx PHY is enabled on an Ethernet interface, packets that the traffic generator receives on such an interface are loop-backed to the originator and forwarded to the destination.

Because loopback is enabled as the Tx PHY in the diagram above, packets will loop at the physical layer, and the same number of packets will be returned to the traffic generator from the DUT's Egress to Ingress side. Thus, the Tx and Rx counts of receiving and transmitting interfaces are the same. The packets are looped and also forwarded to their next destination.

#### Tx MAC Loopback

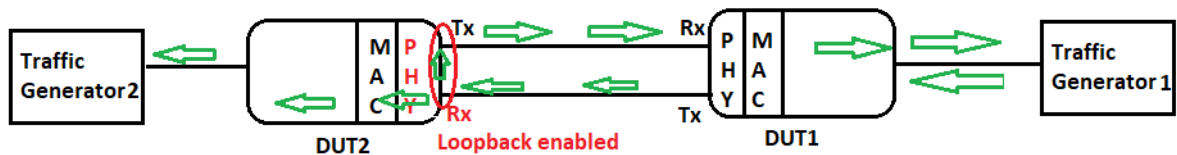


Loopback Tx MAC is enabled on the Ethernet interface, and when packets from the traffic generator arrive on such an interface, they are loop-backed to the originator rather than being forwarded.

In the above diagram, as loopback is enabled as a Tx MAC, the packets will loop at the MAC layer (data link layer), and the same number of packets are returned from the egress side to the ingress side of the DUT to the traffic generator. Thus, the Tx and Rx counts of receiving and transmitting interfaces are the same. The packets are looped but not forwarded further.

## Remote Loopback

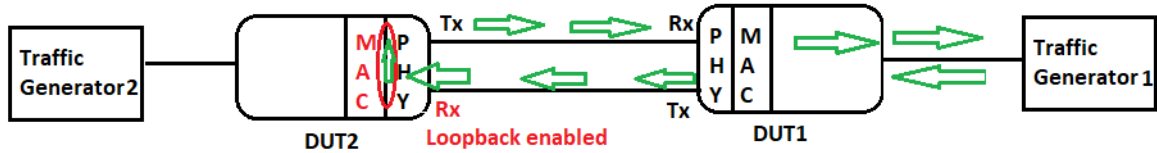
### Rx PHY Loopback



Loopback Rx PHY is enabled on the ethernet interface, and when packets from the traffic generator arrive at a remote node via such an interface, they are loop-backed to the originator and forwarded to the next route.

In the above diagram, as loopback is enabled as Rx PHY on DUT2, the packets will loop at the physical layer of the DUT2, and the same number of packets are returned from the ingress to the egress side of the DUT2 to DUT1 and the traffic generator. Thus, the Tx and Rx counts of receiving and transmitting interfaces are the same. The packets are looped back to Traffic Generator1 as well as forwarded to Traffic Generator2.

### Rx MAC Loopback



Loopback Rx MAC is enabled on the ethernet interface, and when packets from the traffic generator arrive at a remote node via such an interface, they are loop-backed to the originator but not forwarded to the next route.

In the above diagram, as loopback is enabled as Rx MAC on DUT2, the packets will loop at the MAC layer (data link layer) of the DUT2, and the same number of packets are returned from the ingress to the egress side of the DUT2 to DUT1 and the traffic generator. Thus, the Tx and Rx counts of receiving and transmitting interfaces are the same. The packets are looped back to Traffic Generator1, but not forwarded to Traffic Generator2.

## Topology



Figure 14-23: Ethernet Interface Loopback Support



**Scenario-1: PHY level Tx Loopback****Configuration of ROUTER-1 device**

#configure terminal	Enter Configure mode.
(config)#hostname ROUTER-1	Configure the hostname
(config)#commit	Commit the configuration
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge
(config)#vlan database	Enter into VLAN database
(config-vlan)#vlan 2 bridge 1	Configure VLAN
(config-vlan)#exit	Exit the VLAN database mode
(config)#interface ce1/1	Enter into interface ce1/1
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode trunk	Configure switchport mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Add all the VLANs to the interface
(config-if)#exit	Exit the interface mode
(config)#interface ce5/1	Enter into interface ce1/1
(config-if)# port breakout enable 4*10g	Configure port breakout
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode trunk	Configure switchport mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Add all the VLANs to the interface
(config-if)#loopback tx phy	Configure loopback Tx PHY
(config-if)#exit	Exit the interface level
(config)#no mac-address-table learning bridge 1 interface ce1/1	Disable the MAC-learning on the device
(config)#no mac-address-table learning bridge 1 interface ce5/1	Disable the MAC-learning on the device
(config)#commit	Commit the configuration
(config)#exit	Exit from configuration mode

**Configuration of ROUTER-2 device**

#conf terminal	Enter into the configure terminal mode
(config)#hostname ROUTER-2	Configure the hostname
(config)#commit	Commit the configuration
(config)#exit	Exit configuration mode
#conf terminal	Enter into the configure terminal mode
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge
(config)#vlan database	Enter into VLAN database

## Ethernet Interface Loopback Support Configurations

(config-vlan)#vlan 2 bridge 1	Configure VLAN
(config-vlan)#exit	Exit the VLAN database mode
(config)#interface ce3/1	Enter into interface ce3/1
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode trunk	Configure switchport mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Add the VLAN to the interface
(config-if)#exit	Exit the interface mode
(config-if)#interface ce29/1	Enter into interface ce29/1
(config-if)# Port breakout enable 4*10g	Configure port breakout
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode trunk	Configure switchport mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Add the VLAN to the interface
(config-if)#exit	Exit from interface level
(config)#no mac-address-table learning bridge 1 interface ce3/1	Disable the MAC-learning on the device
(config)#no mac-address-table learning bridge 1 interface ce29/1	Disable the MAC-learning on the device
(config)#commit	Commit the configuration
(config)#exit	Exit from configuration mode

### Validation

On ROUTER-1 Device:

```
#show running-config interface ce1/1
!
interface ce1/1
  switchport
  bridge-group 1
  switchport mode trunk
  switchport trunk allowed vlan add 2
!

#show running-config interface ce5/1
!
interface ce5/1
  port breakout enable 4X10g
  switchport
  bridge-group 1
  switchport mode trunk
  switchport trunk allowed vlan add 2
  loopback tx phy
!

#show interface ce5/1
Interface ce5/1
  Flexport: Breakout Control Port (Active): Break Out Enabled
```

```

Hardware is ETH Current HW addr: 34ef.b689.e04a
Physical:34ef.b689.e04a Logical:(not set)
Forward Error Correction (FEC) configured is Auto (default)
FEC status is N/A
Port Mode is trunk
Interface index: 5045
Metric 1 mtu 1500 duplex-full link-speed 10g
Debounce timer: disable
Loopback Type: PHY
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2021 Oct 23 15:57:01 (00:08:51 ago)
Statistics last cleared: 2021 Oct 23 15:54:44 (00:11:08 ago)
5 minute input rate 255 bits/sec, 0 packets/sec
5 minute output rate 255 bits/sec, 0 packets/sec
RX
  unicast packets 0 multicast packets 2272 broadcast packets 0
  input packets 2272 bytes 153730
  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 4333 broadcast packets 0
  output packets 4333 bytes 293304
  jumbo packets 0
  output errors 0 collision 0 deferred 0 late collision 0
  output discard 0
  Tx pause 0

```

```
# show interface brief
```

Ethernet Interface	Type	PVID	Mode	Status	Reason	Speed	Port Ch #	Ctl	Br/Bu	Loopbk
ce5/1	ETH	1	trunk	up	none	10g	--		Br	Yes PHY

#### On ROUTER-2 Device:

```

#show running-config interface ce3/1
!
interface ce3/1
  switchport
  bridge-group 1
  switchport mode trunk
  switchport trunk allowed vlan add 2
!

#show running-config interface ce29/1
!
interface ce29/1
  port breakout enable 4X10g
  switchport
  bridge-group 1
  switchport mode trunk
  switchport trunk allowed vlan add 2

```

!

Interface counters before configuring loopback on both the devices:

```
=====
#show interface counters rate gbps
+-----+-----+-----+-----+
| Interface | Rx gbps | Rx pps | Tx gbps | Tx pps |
+-----+-----+-----+-----+
| ce1/1     | 8.65    | 8446138 | 0.00    | 0      |
| ce5/1     | 0.00    | 0       | 8.65    | 8446125|

#show interface counters rate gbps
+-----+-----+-----+-----+
| Interface | Rx gbps | Rx pps | Tx gbps | Tx pps |
+-----+-----+-----+-----+
| ce3/1     | 0.00    | 0       | 8.65    | 8446188|
| ce29/1    | 8.65    | 8446254 | 0.00    | 0      |
```

Interface counters after configuring loopback Tx PHY on ROUTER-1 device:

```
#show interface counters rate gbps
+-----+-----+-----+-----+
| Interface | Rx gbps | Rx pps | Tx gbps | Tx pps |
+-----+-----+-----+-----+
| ce1/1     | 8.65    | 8446147 | 8.65    | 8446319|
| ce5/1     | 8.65    | 8446194 | 8.65    | 8446194|

#show interface counters rate gbps
+-----+-----+-----+-----+
| Interface | Rx gbps | Rx pps | Tx gbps | Tx pps |
+-----+-----+-----+-----+
| ce3/1     | 0.00    | 0       | 0.00    | 0      |
```

Un-Config the Loopback

#configure terminal	Enter into configure terminal mode
(config)#in ce5/1	Enter into interface level
(config-if)#no loopback	Un-configure the loopback
(config-if)#commit	Commit the configuration
(config-if)#end	Exit from the configuration mode

## Scenario-2 Loopback Tx MAC

#configure terminal	Enter into configure terminal mode
(config)#in ce5/1	Enter into interface level
(config-if)# loopback tx mac	Configure loopback Tx MAC
(config-if)#commit	Commit the configuration
(config-if)#end	Exit from the configuration mode

### Validation

#### On ROUTER-1 Device:

```
#show running-config interface ce1/1
!
interface ce1/1
  switchport
  bridge-group 1
  switchport mode trunk
  switchport trunk allowed vlan add 2
!

#show running-config interface ce5/1
!
interface ce5/1
  port breakout enable 4X10g
  switchport
  bridge-group 1
  switchport mode trunk
  switchport trunk allowed vlan add 2
  loopback tx mac
!

#show interface ce5/1
Interface ce5/1
  Flexport: Breakout Control Port (Active): Break Out Enable
  Hardware is ETH  Current HW addr: 34ef.b689.e04a
  Physical:34ef.b689.e04a  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Interface index: 5045
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
  Loopback Type: MAC
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2021 Oct 23 15:57:01 (00:08:51 ago)
  Statistics last cleared: 2021 Oct 23 15:54:44 (00:11:08 ago)
  5 minute input rate 255 bits/sec, 0 packets/sec
  5 minute output rate 255 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 2272 broadcast packets 0
    input packets 2272 bytes 153730
    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 4333 broadcast packets 0
output packets 4333 bytes 293304
jumbo packets 0
output errors 0 collision 0 deferred 0 late collision 0
output discard 0
Tx pause 0
```

#show interface brief

Ethernet Interface	Type	PVID	Mode	Status	Reason	Speed	Port Ch #	Ctl	Br/Bu	Loopbk
ce5/1	ETH	1	trunk	up	none	10g	--		Br	Yes MAC

On ROUTER-2 device:

```
#show running-config interface ce3/1
!
interface ce3/1
  switchport
  bridge-group 1
  switchport mode trunk
  switchport trunk allowed vlan add 2
!

#show running-config interface ce29/1
!
interface ce29/1
  switchport
  bridge-group 1
  switchport mode trunk
  switchport trunk allowed vlan add 2
!
```

Interface counters before configuring loopback on both the devices:

```
#show interface counters rate gbps
+-----+-----+-----+-----+
| Interface | Rx gbps | Rx pps | Tx gbps | Tx pps |
+-----+-----+-----+-----+
| ce1/1     | 8.65    | 8432138 | 0.00    | 0      |
| ce5/1     | 0.00    | 0       | 8.65    | 8430125|
+-----+-----+-----+-----+

#show interface counters rate gbps
+-----+-----+-----+-----+
| Interface | Rx gbps | Rx pps | Tx gbps | Tx pps |
+-----+-----+-----+-----+
| ce3/1     | 0.00    | 0       | 8.65    | 8429188|
| ce29/1    | 8.65    | 8430254 | 0.00    | 0      |
+-----+-----+-----+-----+
```

Interface counters after configuring loopback Tx PHY on ROUTER-1 devices:

```
#sh interface counters rate gbps
+-----+-----+-----+-----+
+
+   Interface   | Rx gbps | Rx pps | Tx gbps | Tx pps
+-----+-----+-----+-----+
+
+   ce1/1       | 8.65    | 8446147 | 8.65    | 8446319
+   ce5/1       | 8.65    | 8446194 | 8.65    | 8446194

#show interface counters rate gbps
+-----+-----+-----+-----+
+
+   Interface   | Rx gbps | Rx pps | Tx gbps | Tx pps
+-----+-----+-----+-----+
+
+   ce3/1       | 0.00    | 0       | 0.00    | 0
+   ce29/1      | 0.00    | 0       | 0.00    | 0
```

### Un-Config the Loopback

#configure terminal	Enter into configure terminal mode
(config)#in ce5/1	Enter into interface level
(config-if)#no loopback	UnConfigure loopback
(config-if)#commit	Commit the configuration
(config-if)#end	Exit from the configuration mode

### Scenario-3 Loopback Rx PHY

#configure terminal	Enter into configure terminal mode
(config)#in ce29/1	Enter into interface level
(config-if)#loopback rx phy	Configure loopback Rx PHY
(config-if)#commit	Commit the configuration
(config-if)#end	Exit from the configuration mode

### Validation

On ROUTER-2 device:

```
#show interface ce29/1
Interface ce29/1
  Flexport: Breakout Control Port (Active): Break Out Enabled
  Hardware is ETH  Current HW addr: 80a2.357f.4ebd
  Physical:80a2.357f.4ebd  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
```

```
Loopback Type: R-PHY
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2019 Apr 30 10:03:23 (00:00:58 ago)
Statistics last cleared: 2019 Apr 30 09:43:30 (00:20:51 ago)
30 second input rate 8648972937 bits/sec, 8446291 packets/sec
30 second output rate 20723 bits/sec, 38 packets/sec
RX
  unicast packets 3390485528 multicast packets 6205 broadcast packets 0
  input packets 3390494721 bytes 433982963744
  jumbo packets 0
  undersize 0 oversize 0 CRC 0 fragments 1 jabbers 0
  input error 1
  input with dribble 0 input discard 39330
  Rx pause 0
TX
  unicast packets 0 multicast packets 6009 broadcast packets 0
  output packets 6009 bytes 408564
  jumbo packets 0
  output errors 0 collision 0 deferred 0 late collision 0
  output discard 0
  Tx pause 0
```

#show interface brief

-----								
--								
Ethernet	Type	PVID	Mode	Status	Reason	Speed	Port	
Ctl Br/Bu	Loopbk							
Interface							Ch	#
-----								
--								
ce29/1	ETH	1	trunk	up	none	10g	--	
Br Yes		R-PHY						

Interface counters after configuring loopback Rx PHY on ROUTER-2 device

#show interface counters rate gbps

+-----+-----+-----+-----+					
+					
	Interface		Rx gbps		Rx pps
+-----+-----+-----+-----+					
+					
	ce1/1		8.65		8446140
	ce5/1		8.65		8446058

#show interface counters rate gbps

+-----+-----+-----+-----+					
+					
	Interface		Rx gbps		Rx pps
+-----+-----+-----+-----+					
+					
	ce3/1		0.00		0
	ce29/1		8.65		8446222



## CHAPTER 15 LAG with RTAG7 Hashing

### Overview

Traffic can be load balanced within an LACP trunk group and within an ECMP in a controlled manner using the RTAG7 hashing algorithm.

### Topology

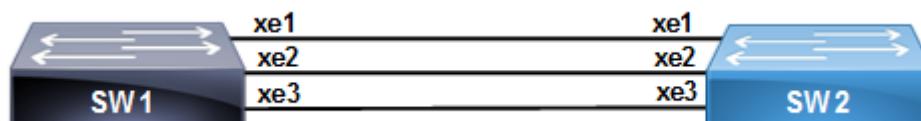


Figure 15-24: LACP with RTAG7 Configuration

### Dynamic LAG with RTAG7

#### SW1

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)#vlan 2-10 bridge 1	Configure VLANs.
(config)#load-balance rtag7	Enable load-balance for rtag7 globally.
(config)#load-balance rtag7 l2 src-mac dest-mac ether-type vlan	Enabling load-balance rtag7 for l2 with all options.
(config)#load-balance rtag7 ipv4 dest-ipv4 src-ipv4 destl4-port srcl4-port protocol-id	Enabling load-balance rtag7 for ipv4 with all options.
(config)#interface po1	Enter into port channel interface po1.
(config-if)#switchport	Configure po1 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 all	Allow all the VLANs on the xe1 interface.
(config-if)#port-channel load-balance rtag7	Enable rtag7 load-balancing method.
(config-if)#exit	Exit the po1 interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#switchport	Configure xe1 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 all	Allow all the VLANs on the xe1 interface.

(config-if)#channel-group 1 mode active	Make port as part of port channel
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 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 all	Allow all the VLANs on the xe2 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel..
(config-if)#exit	Exit the xe2 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 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 all	Allow all the VLANs on the xe3 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel.
(config-if)#exit	Exit the xe3 interface mode.

**SW2**

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)#vlan 2-10 bridge 1	Configure VLANs.
(config)#interface po1	Enter interface mode
(config-if)#switchport	Configure po1 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 all	Allow all the VLANs on the po1 interface
(config-if)#exit	Exit the interface mode
(config)#interface xe1	Enter interface mode.
(config-if)#switchport	Configure xe1 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 all	Allow all the VLANs on the xe1 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel.
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 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 all	Allow all the VLANs on the xe2 interface.

(config-if)#channel-group 1 mode active	Make port as part of port channel.
(config-if)#exit	Exit the xe2 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 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 all	Allow all the VLANs on the xe3 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel.

## Validation

```
SW1#show etherchannel summary
Aggregator po1 100010
Aggregator Type: Layer2
Admin Key: 0010 - Oper Key 0010
Link: xe1 (5061) sync: 1
Link: xe2 (5062) sync: 1
Link: xe3 (5063) sync: 1
```

```
SW2#show etherchannel summary
Aggregator po1 7
Aggregator Type: Layer2
Admin Key: 0010 - Oper Key 0010
Link: xe1 (5013) sync: 1
Link: xe2 (5014) sync: 1
Link: xe3 (5015) sync: 1
```

```
SW1#show etherchannel detail
Aggregator po1 100001
Aggregator Type: Layer2
Mac address: 3c:2c:99:28:52:1e
Admin Key: 0001 - Oper Key 0001
Actor LAG ID- 0x8000,3c-2c-99-7a-b2-e0,0x0001
Receive link count: 3 - Transmit link count: 3
Individual: 0 - Ready: 1
Partner LAG ID- 0x8000,00-18-23-30-20-ce,0x0001
Link: xe1 (5061) sync: 1
Link: xe2 (5062) sync: 1
Link: xe3 (5063) sync: 1
Collector max delay: 5
```

## Static LAG with RTAG7

### SW1

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)#vlan 2-10 bridge 1	Configure VLANs
(config)#load-balance rtag7	Enable load-balance for rtag7 globally.
(config)#load-balance rtag7 l2 src-mac dest-mac ether-type vlan	Enabling load-balance rtag7 for l2 with all options.
(config)#load-balance rtag7 ipv4 dest-ipv4 src-ipv4 destl4-port srcl4-port protocol-id	Enabling load-balance rtag7 for ipv4 with all options .
(config)#interface sa1	Enter into port channel interface sa1.
(config-if)#switchport	Configuresa1 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 all	Allow all the VLANs on the sa1 interface.
(config-if)#port-channel load-balance rtag7	Enable rtag7 load-balancing method.
(config)#interface xe1	Enter interface mode.
(config-if)#switchport	Configure xe1 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 all	Allow all the VLANs on the xe1 interface.
(config-if)#static-channel-group 1	Make port as part of Static port channel.
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 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 all	Allow all the VLANs on the xe2 interface.
(config-if)#static-channel-group 1	Make port as part of Static port channel.
(config-if)#exit	Exit the xe2 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 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 all	Allow all the VLANs on the xe3 interface.
(config-if)#static-channel-group 1	Make port as part of Static port channel.
(config-if)#exit	Exit the xe3 interface mode.

**SW2**

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)#vlan 2-10 bridge 1	Configure VLANs.
(config)#interface sa1	Enter interface mode
(config-if)#switchport	Configure sa1 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 all	Allow all the VLANs on the sa1 interface.
(config-if)#exit	Exit interface mode
(config)#interface xe1	Enter interface mode.
(config-if)#switchport	Configure xe1 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 all	Allow all the VLANs on the xe1 interface.
(config-if)#static-channel-group 1	Make port as part of Static port channel.
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 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 all	Allow all the VLANs on the xe2 interface.
(config-if)#static-channel-group 1	Make port as part of Static port channel.
(config-if)#exit	Exit the xe2 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 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 all	Allow all the VLANs on the xe3 interface.
(config-if)#static-channel-group 1	Make port as part of Static port channel.
(config-if)#exit	Exit the xe3 interface mode.

**Validation**

```
SW1#show static-channel-group
Static Aggregator: sa1
Member Status
xe1          up
xe2          up
xe3          up
SW1#
```

```
#show running-config interface sa1
!
interface sa1
load-interval 30
ip address 14.4.1.2/24
mtu 1600
port-channel load-balance rtag7
port-channel min-links 4
ip ospf network point-to-point
ip ospf cost 1000
```

## CHAPTER 16 Link Detection Debounce Timer

The link debounce timer avoids frequent updates (churn) to higher layer protocols during flapping of an interface. The initial link state is UP. The link goes DOWN. And if the Link comes UP and goes DOWN, The link DOWN AND link UP timer is started and being restarted on each flap (link comes up and goes down again). For each link DOWN, link down timer will start and it restarts on flap within the link debounce interval. For each link UP, link up timer will start and it restarts on flap within the link debounce interval.

Note: Keep the following in mind when using the Link detection debounce timer:

- Link debounce timer is supported only for physical L2 and L3 interfaces.
- When debounce timer is configured we won't be able to configure the link-debounce-timer config and viceversa.
- The link debounce flap-count refers to the number of flaps OcNOS receives while the debounce timer is running:
- The flap-count is only updated if the timer is still running and OcNOS receives a link status event for the interface.
- The flap-count is reset at the subsequent start of the link debounce timer.
- Protocol-specific timers such as BFD which depend on the link status should be configured to minimum of 1.5 times the value of the link debounce time. Otherwise it could affect the protocol states if the link debounce timer is still running.
- Protocols such as PO, OSPF, BFD, ISIS, BGP which depends on the link status, in this case we should ensure on both the connected interfaces we need to configure the link-debounce timer.

### Topology

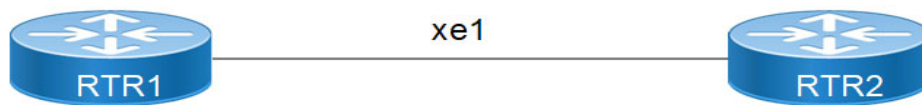


Figure 16-25: Link detection debounce timer topology

### Configuration

#### RTR 1

#configure terminal	Enter Configure mode.
(config)#interface xe1	Enter into interface mode
(config)#link-debounce-time 4000 5000	Configure link-debounce-time where link-up timer is 4000ms and link-down timer is 5000ms
(config)#exit	Exit configure mode

#### RTR 2

#configure terminal	Enter Configure mode.
(config)#interface xe1	Enter into interface mode
(config)# link-debounce-time 4000 5000	Configure link-debounce-time where link-up timer is 4000ms and link-down timer is 5000ms
(config)#exit	Exit configure mode.

### Validation

```
#show running-config | i debounce link-debounce-time 4000 5000
```

```
#show interface xe1 | i Debounce Link Debounce timer: enable
Linkup Debounce time 4000 ms Linkdown Debounce time 5000 ms
Linkup Debounce status : idle
Linkdown Debounce status : idle
```

RTR1 and RTR2 outputs after interface flap:

```
#show interface xe1 | i debounce Link Debounce timer: enable
Linkup Debounce time 4000 ms Linkdown Debounce time 5000 ms
Flap Count: 1
Last Debounce Flap :
Linkup Debounce status : idle
Linkdown Debounce status : idle
```

```
#show interface xe1 | i debounce
Link Debounce timer: enable
Linkup Debounce time 4000 ms Linkdown Debounce time 5000 ms
Flap Count: 1
Last Debounce Flap :      Linkup Debounce status : idle
Linkdown Debounce status : idle
```

---

### Log Messages

The following is a configuration example to log link debounce timer activity:

#configure terminal	Enter Configure mode
(config)#logging level nsm 7	Enable operational log to display debounce start and end.

---

### Example Log Messages

```
2019 Feb 28 02:50:40.761 : OcNOS : NSM : INFO : Start UP->DOWN Link Debounce Timer on
interface xe1
2019 Feb 28 02:50:40.761 : OcNOS : NSM : NOTIF : [DEBOUNCE_EVENT_4]: Interface xe1
changed state from up to down
2019 Feb 28 02:50:43.543 : OcNOS : NSM : INFO : Start DOWN->UP Link Debounce Timer on
interface xe1
2019 Feb 28 02:50:43.543 : OcNOS : NSM : INFO : Interface xe1 Flapped, prev_state DOWN
new_state UP, flap count 1
2019 Feb 28 02:50:43.543 : OcNOS : NSM : NOTIF : [DEBOUNCE_EVENT_4]: Interface xe1
changed state from down to up
2019 Feb 28 02:50:45.761 : OcNOS : NSM : INFO : Link Debounce Timer Expired on interface
xe1 (initiated transition up->down), prev_state UP, new_state UP

2019 Feb 28 02:50:47.544 : OcNOS : NSM : INFO : Link Debounce Timer Expired on interface
xe1 (initiated transition down->up), prev_state UP, new_state UP
```



# CHAPTER 17 Max Session and Session Limit Configuration

## Overview

User can configure session-limit for Telnet and SSH sessions separately but this max-session parameter value takes the precedence to restrict the maximum number of sessions. If user configured this max-session to be 4, then the device would allow only maximum of 4 SSH and Telnet sessions collectively irrespective of the individual SSH and Telnet max-session configuration. Active sessions won't be disturbed even if the configured max-session limit is lesser than the current active sessions. Default value for max-session value is 40 in line mode. There is no default value for the telnet-server-limit and ssh-server-limit.

After configuring max-session parameter if user tries to configure SSH/Telnet sessions then the total value of Telnet and SSH session limit should be lesser than the max-session value otherwise error will be thrown.

If already Telnet and SSH session-limits configured, now if user is configuring max-session then there won't be any error but maximum number of sessions will be limited to max-session value.

## Topology

The procedures in this section use the topology as mentioned below. Setup consists of one node acting as Telnet server.



Figure 17-26: Telnet topology

### Configuration of Telnet Session Limit Lesser than Max-Session

#configure terminal	Enter configure mode
(config)#no feature telnet vrf management	Disable Feature Telnet in VRF Management
(config)#telnet server session-limit 12 vrf management	Configure the Session limit as 12 which is less than Max-Session parameter in line VTY
(config)#commit	Perform commit to submit the changes done
(config)#feature telnet vrf management	Enable telnet feature in VRF management
(config)#commit	Perform commit to submit the changes done
(config)#exit	Exit configure mode

### Validation

Check that the maximum telnet session possible are 12 which is lesser than Max-Session limit parameter value in line VTY.

```
#show running-config telnet server
telnet server session-limit 12 vrf management
feature telnet vrf management
no feature telnet
```

## Configuration of SSH Server Session Limit Lesser than Max-Session

Configure SSH Server Session limit to be lesser than Max-Session.

### Topology

Setup consists of one node acting as SSH server.



Figure 17-27: SSH Server topology

### Configuration of SSH Server Session Limit Lesser than Max-Session

#configure terminal	Enter configure mode
(config)#no feature ssh vrf management	Disable feature SSH
(config)#ssh server session-limit 12 vrf management	Configure SSH server session-limit to be lesser than Max-Session limit
(config)#commit	Perform Commit to submit changes done
(config)#feature ssh vrf management	Enable feature SSH
(config)#commit	Perform commit to submit changes
(config)#exit	Exit configure mode

### Validation

Check that the maximum SSH session possible are 12 which is lesser than Max-Session limit parameter value in line VTY.

```
#show running-config ssh server
feature ssh vrf management
ssh server session-limit 12 vrf management
```

```
no feature ssh
```

# Configuration of Telnet Session Limit Greater than Max-Session

In the below section, configure Telnet Session limit to be greater than Max-Session limit.

## Topology

Setup consists of one node acting as Telnet server.



Figure 17-28: Telnet Session Topology

## Configuration of Telnet server Session-Limit to be greater than line-VTY max-session

#configure terminal	Enter configure mode
(config)#no feature telnet vrf management	Disable feature telnet
(config)#telnet server session-limit 12 vrf management	Configure Session-limit as 12 for telnet server
(config)#commit	Perform commit to submit changes
(config)#feature telnet vrf management	Enable Telnet server
(config)#commit	Perform commit to submit changes
(config)#line vty	Enter line VTY mode
(config-line)#max-session 10	Configure max-session as 10
(config-line)#commit	Perform commit to submit changes
(config)#exit	Exit configure mode

## Validation

Check that the total telnet sessions possible is 10 even though telnet server session limit is configured as 12.

```
#show running-config telnet server
telnet server session-limit 12 vrf management
feature telnet vrf management
no feature telnet

#show running-config | grep max-session
max-session 10
```

## Configuration of SSH Session Limit Greater than Max-Session

In the below section, configure SSH Session limit to be greater than Max-Session limit.

### Topology

Setup consists of one node acting as SSH server.



### Configuration of SSH server Session-Limit to be greater than line-vty max-session

#configure terminal	Enter configure mode
(config)#no feature ssh vrf management	Disable feature SSH
(config)#ssh server session-limit 12 vrf management	Configure Session-limit as 12 for SSH server
(config)#commit	Perform commit to submit changes
(config)#feature ssh vrf management	Enable SSH server
(config)#commit	Perform commit to submit changes
(config)#line vty	Enter line VTY mode
(config-line)#max-session 10	Configure max-session as 10
(config-line)#commit	Perform commit to submit changes
(config)#exit	Exit configure mode

### Validation

Check that the total SSH sessions possible is 10 even though SSH server session limit is configured as 12.

```
#show running-config ssh server
feature ssh vrf management
ssh server session-limit 12 vrf management
no feature ssh

#show running-config | grep max-session
max-session 10
```

---

## CHAPTER 18 NTP Client Configuration

---

---

### Overview

NTP modes differ based on how NTP allows communication between systems. NTP communication consists of time requests and control queries. Time requests provide the standard client/server relationship in which a client requests time synchronization from an NTP server. Control queries provide ways for remote systems to get configuration information and reconfigure NTP servers.

---

### Support for Default VRF via In-band Management

OcNOS supports NTP over the default and management VRFs via in-band management interface and OOB management interface, respectively.

By default, NTP runs on the management VRF.

---

### NTP Modes

The following describes the various NTP node types.

---

#### Client

An NTP client is configured to let its clock be set and synchronized by an external NTP timeserver. NTP clients can be configured to use multiple servers to set their local time and are able to give preference to the most accurate time sources. They do not, however, provide synchronization services to any other devices.

---

#### Server

An NTP server is configured to synchronize NTP clients. Servers can be configured to synchronize any client or only specific clients. NTP servers, however, will accept no synchronization information from their clients and therefore will not let clients update or affect the server's time settings.

---

#### Peer

With NTP peers, one NTP-enabled device does not have authority over the other. With the peering model, each device shares its time information with the others, and each device can also provide time synchronization to the others.

---

### Authentication

For additional security, you can configure your NTP servers and clients to use authentication. Routers support MD5 authentication for NTP. To enable a router to do NTP authentication:

1. Enable NTP authentication with the `ntp authenticate` command.
2. Define an NTP authentication key with the `ntp authentication-key vrf management` command. A unique number identifies each NTP key. This number is the first argument to the `ntp authentication-key vrf management` command.

- 3. Use the `ntp trusted-key vrf management` command to tell the router which keys are valid for authentication. If a key is trusted, the system will be ready to synchronize to a system that uses this key in its NTP packets. The trusted key should already be configured and authenticated.

## NTP Configuration

NTP client, user can configure an association with a remote server. In this mode the client clock can synchronize to the remote server

After configuring the NTP servers, wait a few minutes before you verify that clock synchronization is successful. When clock synchronization has actually happened, there will be an asterisk “\*” symbol along with the interface when you give the `show ntp peers` command.

### Topology

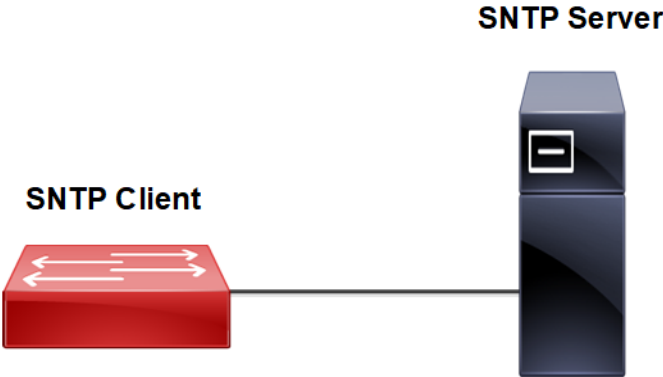


Figure 18-29: NTP Client and Server

### NTP Client

<code>#configure terminal</code>	Enter configure mode.
<code>(config)#feature ntp vrf management</code>	Configure feature on default or management VRF. By default this feature runs on management VRF.
<code>(config)# ntp enable vrf management</code>	This feature enables ntp. This will be enabled in default.
<code>(config)#ntp server 10.1.1.1 vrf management</code>	Configure ntp server ip address.
<code>(config)#exit</code>	Exit from the Configure Mode.

### Validation Commands

```
#show ntp peers
-----
Peer IP Address Serv/Peer
-----
10.1.1.1 Server (configured)

#show ntp peer-status
Total peers : 1
```

```

* - selected for sync, + - peer mode(active),
- - peer mode(passive), = - polled in client mode
  remote          refid          st t when poll reach    delay    offset    jitter
=====
*10.1.1.1          LOCAL(0)          7 u   14   32   37      0.194    -4.870    3.314

```

## Maxpoll and Minpoll Configuration

The maximum poll interval are specified in defaults to 6 (64 seconds), but can be increased by the `maxpoll` option to an upper limit of 16 (18.2 hours). The minimum poll interval defaults to 4 (16 seconds), and this is also the minimum value of the `minpoll` option.

The client will retry between `minpoll` and `maxpoll` range configured for synchronization with the server.

## Client

#configure terminal	Enter configure mode.
(config)#feature ntp vrf management	Configure feature on default or management VRF. By default this feature runs on management VRF.
(config)#ntp server 10.1.1.1 maxpoll 7 minpoll 5 vrf management	Configure minpoll and maxpoll range for ntp server.
(config)#exit	Exit from the Configure Mode.

## Validation Commands

```
#show ntp peers
```

```

-----
Peer IP Address Serv/Peer
-----
10.1.1.1 Server (configured)

```

```
#show ntp peer-status
```

```

Total peers : 1
* - selected for sync, + - peer mode(active),
- - peer mode(passive), = - polled in client mode
  remote          refid          st t when poll reach    delay    offset    jitter
=====
*10.1.1.1          LOCAL(0)          7 u   14   32   37      0.194    -4.870    3.314

```

## NTP Authentication

When you enable NTP authentication, the device synchronizes to a time source only if the source carries the authentication keys specified with the source by key identifier. The device drops any packets that fail the authentication check, and prevents them from updating the local clock.

Client

#configure terminal	Enter configure mode.
(config)#feature ntp vrf management	Enable feature on default or management VRF. By default this feature runs on management VRF..
(config)#ntp server 10.1.1.1 vrf management	Configure ntp server ip address.
(config)#ntp authenticate vrf management	Enable NTP Authenticate. NTP authentication is disabled by default.
(config)#ntp authentication-key 1234 md5 text vrf management	Configure ntp authentication key along with md5 value.
(config)#ntp trusted-key 1234 vrf management	Configure trusted key <1-65535>
(config)#exit	Exit from the Configure Mode.

Validation Commands

```
#show ntp authentication-status
Authentication enabled

#show ntp authentication-keys
-----
Auth Key      MD5 String
-----
1234          SWWX

#show ntp trusted-keys
Trusted Keys:
1234
```



---

## CHAPTER 19 Port Breakout Configuration

---

This chapter contains an overview of splitting single 40G port to 4x10G ports.

---

### Overview

Port Breakout system enables numerous 40GbE/100GbE ports to be broken out into 4x10GbE, 4x25GbE, 2x50GbE ports through a secure, highly reliable breakout cabling solution. Today's large-scale virtualized datacenter networks require a mix of 10Gb, 25Gb, 40Gb and 100Gb Ethernet interface speeds able to utilize the widest range of flexible connectivity options. These same networks require a variety of cost-effective cabling options for both addressing connectivity and allowing for simple migrations as network speeds and density requirements evolve. As data centers scale and bandwidth demands increase, the networking infrastructure must be capable of scaling with it. Port Breakout feature provides flexibility in splitting 40G to 4x10G and 100G to 4x10G, 4x25G, 2x50G cabling and vice-versa whenever requires, and hence provide Administrator a great flexibility in choosing the port speed as per their requirement. A Port Breakout group consists of 4 ports, first port will be control port and the rest 3 are subsidiary ports. Naming of Control port and its subsidiary port is as below

xe50/1, xe50/2, xe50/3, xe50/4

In xe50, numeral 50 indicates the slot of the port on a board and numerals after "/" indicates port numbers on that slot. First port (interface 50/1 in above example) is always control port whereas the rest 3 ports (ports 50/2, 50/3 and 50/4) are subsidiary ports. Only Control port can become 40G or 100G port. For Transceiver types mentioned in [fec](#) command will be enabled by default for both control port and the rest 3 subsidiary ports. If Peer is not supporting FEC, fec off needs to be configured on the ports manually.

Currently below breakout options are available

- 40G ports
  - 40G to 4x10G breakout ports
- 100G ports
  - 100G to 4x10G breakout ports
  - 100G to 4x25G breakout ports (due to HW limitation Autoneg isn't supported)
  - 100G to 2x50G breakout ports (due to HW limitation Autoneg isn't supported).

Note: There are some configuration restrictions for Subsidiary ports such as:

1. Port breakout enable/disable is not allowed on Subsidiary ports.
2. Speed, Duplex configurations are not allowed on InActive Subsidiary ports.
3. One control port and subsidiary ports will be supported in 100g to 2x50G breakout  
For Example: Port XE1/1(control port) and XE1/3(subsidiary port) will be active out of 4 ports.

---

### Terminology

Following is a brief description of terms and concepts used to describe port breakout.

#### Ctl: Control port

A 40G or 100G split-able port is called Control port.

## Brk: Port Breakout

A control port which is split into 4x10G 4x25G or 2x50 ports.

### Subsidiary ports

Ports which are members of Control Port, A subsidiary port can be Active or InActive

### IA: InActive Ports

Subsidiary ports whose control port is not configured for “Port Breakout”

---

## Pre-Requisite

From OcNOS version 5.1 onwards, before doing the Port breakout we need to reserve the VLANs using the CLI `vlan-reservation vlan-id/vlan-range`.

Note: Once VLANs are reserved, those vlans cannot be used for bridge configuration.

The advantage of using vlan-reservation is when port breakout is not required,

- then released VLANs can be used for bridge configuration up to maximum of 4062.
- to use the user defined vlan-range values for bridge configuration, do the following:
  1. Completely delete the user-defined vlan-ranges values as deleting subset of it is not allowed.
  2. Remove all the port breakout CLIs configured
  3. Unconfigure the complete set of user defined vlans using `no port breakout enable` and `no vlan-reservation vlan-id/vlan-range`.
  4. Reconfigure bridge vlans, vlan-reservation and port breakout

---

## Configuring vlan-reservation

Configuring Port Breakout (40G to 4x10G) is provided in below section.

<code>#configure terminal</code>	Enter configure mode.
<code>(config)# vlan database</code>	Enter vlan database
<code>(config-if)# vlan-reservation 4050-4058</code>	Specify the vlan-range that should be reserved for interface port Breakout.
<code>(config-if)#exit</code>	Exit vlan database.

---

## Unconfiguring vlan-reservation

Configuring Port Breakout (40G to 4x10G) is provided in below section.

#configure terminal	Enter configure mode.
(config)# vlan database	Enter vlan database
(config-if)# no vlan-reservation 4050-4058	Specify the vlan-range/id that should be released
(config-if)#exit	Exit vlan database.

## Validation

Below output before applying port-breakout config on xe50/1:

```
#show vlan-reservation
VLAN ID      Status
=====
4050         free
4051         free
4052         free
4053         free
4054         free
4055         free
4056         free
4057         free
4058         free
```

## Configuring Port Breakout 40G to 4x10G

Configuring Port Breakout (40G to 4x10G) is provided in below section.

#configure terminal	Enter configure mode.
(config)#interface xe50/1	Specify the interface (xe5/1) to be configured for port Breakout.
(config-if)#port breakout enable 4X10g	Configure port breakout on interface
(config-if)#exit	Exit interface mode.

## Removing Port Breakout

Removing Port Breakout is provided in below section.

Note: Interface xe50/1 is back to back connected and interfaces are up.

#configure terminal	Enter configure mode.
(config)#interface xe50/1	Specify the interface (xe5/1) to be configured for port Breakout.
(config-if)#no port breakout	Unconfigure port breakout on interface
(config-if)#exit	Exit interface mode.

Validation

```
#show interface brief

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

-----
--
Interface      Type              Status Reason Speed
Interface
-----
--
eth0           METH              up    --    1g

-----
--
Interface      Status      Description
-----
--
lo              up          --
lo.management  up          --

-----
--
Ethernet      Type  PVID  Mode              Status Reason Speed Port    Ctl Br/
Bu
Interface                                Ch #
-----
--
xe1           ETH   --    routed            up    none   1g    --      Bu  No
xe2           ETH   --    routed            down   PD    10g   --      No  No
xe3           ETH   --    routed            down   PD    10g   --      No  No
xe4           ETH   --    routed            down   PD    10g   --      No  No
xe5           ETH   --    routed            down   PD    10g   --      Bu  No
xe6           ETH   --    routed            down   PD    10g   --      No  No
xe7           ETH   --    routed            down   PD    10g   --      No  No
xe8           ETH   --    routed            down   PD    10g   --      No  No
xe9           ETH   --    routed            down   PD    10g   --      Bu  No
xe10          ETH   --    routed            down   PD    10g   --      No  No
xe11          ETH   --    routed            down   PD    10g   --      No  No
xe12          ETH   --    routed            down   PD    10g   --      No  No
xe13          ETH   --    routed            down   PD    10g   --      Bu  No
xe14          ETH   --    routed            down   PD    10g   --      No  No
xe15          ETH   --    routed            down   PD    10g   --      No  No
xe16          ETH   --    routed            down   PD    10g   --      No  No
xe17          ETH   --    routed            down   PD    10g   --      Bu  No
```

xe18	ETH	--	routed	down	PD	10g	--	No	No
xe19	ETH	--	routed	down	PD	10g	--	No	No
xe20	ETH	--	routed	down	PD	10g	--	No	No
xe21	ETH	--	routed	down	PD	10g	--	Bu	No
xe22	ETH	--	routed	down	PD	10g	--	No	No
xe23	ETH	--	routed	down	PD	10g	--	No	No
xe24	ETH	--	routed	down	PD	10g	--	No	No
xe25	ETH	--	routed	up	none	10g	--	Bu	No
xe26	ETH	--	routed	down	PD	10g	--	No	No
xe27	ETH	--	routed	up	none	10g	--	No	No
xe28	ETH	--	routed	down	PD	10g	--	No	No
xe29	ETH	--	routed	down	PD	10g	--	Bu	No
xe30	ETH	--	routed	down	PD	10g	--	No	No
xe31	ETH	--	routed	down	PD	10g	--	No	No
xe32	ETH	--	routed	down	PD	10g	--	No	No
xe33	ETH	--	routed	down	PD	10g	--	Bu	No
xe34	ETH	--	routed	down	PD	10g	--	No	No
xe35	ETH	--	routed	down	PD	10g	--	No	No
xe36	ETH	--	routed	down	PD	10g	--	No	No
xe37	ETH	--	routed	down	PD	10g	--	Bu	No
xe38	ETH	--	routed	down	PD	10g	--	No	No
xe39	ETH	--	routed	down	PD	10g	--	No	No
xe40	ETH	--	routed	down	PD	10g	--	No	No
xe41	ETH	--	routed	down	PD	10g	--	Bu	No
xe42	ETH	--	routed	down	PD	10g	--	No	No
xe43	ETH	--	routed	down	PD	10g	--	No	No
xe44	ETH	--	routed	down	PD	10g	--	No	No
xe45	ETH	--	routed	down	PD	10g	--	Bu	No
xe46	ETH	--	routed	down	PD	10g	--	No	No
xe47	ETH	--	routed	down	PD	10g	--	No	No
xe48	ETH	--	routed	down	PD	10g	--	No	No
xe49/1	ETH	--	routed	down	PD	40g	--	Br	No
xe49/2	ETH	--	routed	down	IA	--	--	No	No
xe49/3	ETH	--	routed	down	IA	--	--	No	No
xe49/4	ETH	--	routed	down	IA	--	--	No	No
xe50/1	ETH	--	routed	up	none	40g	--	Br	No
xe50/2	ETH	--	routed	down	IA	--	--	No	No
xe50/3	ETH	--	routed	down	IA	--	--	No	No
xe50/4	ETH	--	routed	down	IA	--	--	No	

```
#show interface xe50/1
```

```
Interface xe50/1
```

```
Flexport: Breakout Control Port (Active): Break Out disabled
```

```
Hardware is ETH Current HW addr: a82b.b5ad.db6f
```

```
Physical:a82b.b5ad.dba4 Logical:(not set)
```

```
Port Mode is Router
```

```
Interface index: 10053
```

```
Metric 1 mtu 1500 duplex-full link-speed 40g
```

```
<UP,BROADCAST,RUNNING,MULTICAST>
```

```
VRF Binding: Not bound
```

```
DHCP client is disabled.
```

```
Last Flapped: 2001 Feb 13 18:42:15 (00:03:20 ago)
```

```
Statistics last cleared: Never
```

```
inet6 fe80::aa2b:b5ff:fead:db6f/64
```

```
5 minute input rate 20 bits/sec, 0 packets/sec
```

```
5 minute output rate 20 bits/sec, 0 packets/sec
```

```
RX
```

```
unicast packets 0 multicast packets 7 broadcast packets 0
input packets 7 bytes 766
jumbo packets 0
runs 0 giants 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 7 broadcast packets 0
output packets 7 bytes 766
jumbo packets 0
output errors 0 collision 0 deferred 0 late collision 0
output discard 0
Tx pause 0
```

#show interface xe50/2

Interface xe50/2

```
Flexport: Non Control Port (InActive)
Hardware is ETH Current HW addr: a82b.b5ad.db6f
Physical:a82b.b5ad.dba5 Logical:(not set)
Port Mode is Router
Interface index: 10054
Metric 1 mtu 1500
<UP,BROADCAST,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2001 Feb 13 18:42:15 (00:03:46 ago)
Statistics last cleared: Never
inet6 fe80::aa2b:b5ff:fead:db6f/64
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
runs 0 giants 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
```

#show interface xe50/3

Interface xe50/3

```
Flexport: Non Control Port (InActive)
Hardware is ETH Current HW addr: a82b.b5ad.db6f
Physical:a82b.b5ad.dba6 Logical:(not set)
Port Mode is Router
Interface index: 10055
Metric 1 mtu 1500
<UP,BROADCAST,MULTICAST>
```

```
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2001 Feb 13 18:42:15 (00:07:30 ago)
Statistics last cleared: Never
inet6 fe80::aa2b:b5ff:fead:db6f/64
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
  runs 0 giants 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

#show interface xe50/4
Interface xe50/4
  Flexport: Non Control Port (InActive)
  Hardware is ETH Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba7 Logical:(not set)
  Port Mode is Router
  Interface index: 10056
  Metric 1 mtu 1500
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:07:36 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  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
    runs 0 giants 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
```

Here xe50/1 is a control Port whereas xe50/2, xe50/3 and xe50/4 are their subsidiary ports. The out-put shows only xe50/1 is active (interface up and running) whereas other ports are inactive (interface up but not running).

Below Outputs after applying port-breakout configured on xe50/1:

VLAN-reservation validation:

```
#show vlan-reservation
VLAN ID      Status
=====
4050         allocated
4051         allocated
4052         allocated
4053         free
4054         free
4055         free
4056         free
4057         free
4058         free
```

```
#show interface brief
```

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-links) - Protocol Down Min-links  
DV - DDM Violation, NA - Not Applicable  
NOM - No operational members, PVID - Port Vlan-id  
Ctl - Control Port (Br-Breakout/Bu-Bundle)

Interface	Type	Status	Reason	Speed
Interface				
eth0	METH	up	--	1g

Interface	Status	Description
lo	up	--
lo.management	up	--

Ethernet	Type	PVID	Mode	Status	Reason	Speed	Port	Ctl	Br/
Bu									
Interface							Ch #		



xe1	ETH	--	routed	up	none	1g	--	Bu	No
xe2	ETH	--	routed	down	PD	10g	--	No	No
xe3	ETH	--	routed	down	PD	10g	--	No	No
xe4	ETH	--	routed	down	PD	10g	--	No	No
xe5	ETH	--	routed	down	PD	10g	--	Bu	No
xe6	ETH	--	routed	down	PD	10g	--	No	No
xe7	ETH	--	routed	down	PD	10g	--	No	No
xe8	ETH	--	routed	down	PD	10g	--	No	No
xe9	ETH	--	routed	down	PD	10g	--	Bu	No
xe10	ETH	--	routed	down	PD	10g	--	No	No
xe11	ETH	--	routed	down	PD	10g	--	No	No
xe12	ETH	--	routed	down	PD	10g	--	No	No
xe13	ETH	--	routed	down	PD	10g	--	Bu	No
xe14	ETH	--	routed	down	PD	10g	--	No	No
xe15	ETH	--	routed	down	PD	10g	--	No	No
xe16	ETH	--	routed	down	PD	10g	--	No	No
xe17	ETH	--	routed	down	PD	10g	--	Bu	No
xe18	ETH	--	routed	down	PD	10g	--	No	No
xe19	ETH	--	routed	down	PD	10g	--	No	No
xe20	ETH	--	routed	down	PD	10g	--	No	No
xe21	ETH	--	routed	down	PD	10g	--	Bu	No
xe22	ETH	--	routed	down	PD	10g	--	No	No
xe23	ETH	--	routed	down	PD	10g	--	No	No
xe24	ETH	--	routed	down	PD	10g	--	No	No
xe25	ETH	--	routed	up	none	10g	--	Bu	No
xe26	ETH	--	routed	down	PD	10g	--	No	No
xe27	ETH	--	routed	up	none	10g	--	No	No
xe28	ETH	--	routed	down	PD	10g	--	No	No
xe29	ETH	--	routed	down	PD	10g	--	Bu	No
xe30	ETH	--	routed	down	PD	10g	--	No	No
xe31	ETH	--	routed	down	PD	10g	--	No	No
xe32	ETH	--	routed	down	PD	10g	--	No	No
xe33	ETH	--	routed	down	PD	10g	--	Bu	No
xe34	ETH	--	routed	down	PD	10g	--	No	No
xe35	ETH	--	routed	down	PD	10g	--	No	No
xe36	ETH	--	routed	down	PD	10g	--	No	No
xe37	ETH	--	routed	down	PD	10g	--	Bu	No
xe38	ETH	--	routed	down	PD	10g	--	No	No
xe39	ETH	--	routed	down	PD	10g	--	No	No
xe40	ETH	--	routed	down	PD	10g	--	No	No
xe41	ETH	--	routed	down	PD	10g	--	Bu	No
xe42	ETH	--	routed	down	PD	10g	--	No	No
xe43	ETH	--	routed	down	PD	10g	--	No	No
xe44	ETH	--	routed	down	PD	10g	--	No	No
xe45	ETH	--	routed	down	PD	10g	--	Bu	No
xe46	ETH	--	routed	down	PD	10g	--	No	No
xe47	ETH	--	routed	down	PD	10g	--	No	No
xe48	ETH	--	routed	down	PD	10g	--	No	No
xe49/1	ETH	--	routed	down	PD	40g	--	Br	No
xe49/2	ETH	--	routed	down	IA	--	--	No	No
xe49/3	ETH	--	routed	down	IA	--	--	No	No
xe49/4	ETH	--	routed	down	IA	--	--	No	No
xe50/1	ETH	--	routed	up	none	10g	--	Br	Yes
xe50/2	ETH	--	routed	up	none	10g	--	No	No
xe50/3	ETH	--	routed	up	none	10g	--	No	No
xe50/4	ETH	--	routed	up	none	10g	--	No	

```
#show interface xe50/1
Interface xe50/1
  Flexport: Breakout Control Port (Active): Break Out Enabled
  Hardware is ETH   Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba4   Logical:(not set)
  Port Mode is Router
  Interface index: 10053
  Metric 1 mtu 1500 duplex-full link-speed 10g
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:54:58 (00:32:03 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  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 7 broadcast packets 0
  input packets 23 bytes 801
  jumbo packets 0
  runts 0 giants 0 CRC 0 fragments 0 jabbers 0
  input error 16
  input with dribble 0 input discard 0
  Rx pause 0
TX
  unicast packets 0 multicast packets 14 broadcast packets 0
  output packets 14 bytes 1532
  jumbo packets 0
  output errors 0 collision 0 deferred 0 late collision 0
  output discard 0
  Tx pause 0

#show interface xe50/2
Interface xe50/2
  Flexport: Non Control Port (Active)
  Hardware is ETH   Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba5   Logical:(not set)
  Port Mode is Router
  Interface index: 10054
  Metric 1 mtu 1500 duplex-full link-speed 10g
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:45:16 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  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 7 broadcast packets 0
  input packets 23 bytes 790
  jumbo packets 0
  runts 0 giants 0 CRC 0 fragments 0 jabbers 0
  input error 16
  input with dribble 0 input discard 0
  Rx pause 0
TX
```

```
unicast packets 0 multicast packets 7 broadcast packets 0
output packets 7 bytes 766
jumbo packets 0
output errors 0 collision 0 deferred 0 late collision 0
output discard 0
Tx pause 0
```

```
#show interface xe50/3
```

```
Interface xe50/3
```

```
Flexport: Non Control Port (Active)
Hardware is ETH Current HW addr: a82b.b5ad.db6f
Physical:a82b.b5ad.dba6 Logical:(not set)
Port Mode is Router
Interface index: 10055
Metric 1 mtu 1500 duplex-full link-speed 10g
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2001 Feb 13 18:42:15 (00:45:31 ago)
Statistics last cleared: Never
inet6 fe80::aa2b:b5ff:fead:db6f/64
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 7 broadcast packets 0
input packets 26 bytes 801
jumbo packets 0
runts 0 giants 0 CRC 0 fragments 0 jabbers 0
input error 19
input with dribble 0 input discard 0
Rx pause 0
```

```
TX
```

```
unicast packets 0 multicast packets 7 broadcast packets 0
output packets 7 bytes 766
jumbo packets 0
output errors 0 collision 0 deferred 0 late collision 0
output discard 0
Tx pause 0
```

```
#show interface xe50/4
```

```
Interface xe50/4
```

```
Flexport: Non Control Port (Active)
Hardware is ETH Current HW addr: a82b.b5ad.db6f
Physical:a82b.b5ad.dba7 Logical:(not set)
Port Mode is Router
Interface index: 10056
Metric 1 mtu 1500 duplex-full link-speed 10g
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2001 Feb 13 18:54:58 (00:33:07 ago)
Statistics last cleared: Never
inet6 fe80::aa2b:b5ff:fead:db6f/64
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 7 broadcast packets 0
input packets 22 bytes 792
jumbo packets 0
runts 0 giants 0 CRC 0 fragments 0 jabbers 0
input error 15
input with dribble 0 input discard 0
Rx pause 0
TX
unicast packets 0 multicast packets 14 broadcast packets 0
output packets 14 bytes 1532
jumbo packets 0
output errors 0 collision 0 deferred 0 late collision 0
output discard 0
Tx pause 0
```

## Configuring Port Breakout (100G to 4x10G)

Configuring Port Breakout (100G to 4x10G) is provided in below section.

#configure terminal	Enter configure mode.
(config)#interface ce1/1	Specify the interface (ce1/1) to be configured for port Breakout.
(config-if)#port breakout enable 4x10g	Configure port breakout on interface
(config-if)#exit	Exit interface mode.

Note: Interface ce1/1 is back to back connected and interfaces are up.

## Validation

### VLAN-reservation validation

```
#show vlan-reservation
VLAN ID      Status
=====
4050         allocated
4051         allocated
4052         allocated
4053         allocated
4054         allocated
4055         allocated
4056         free
4057         free
4058         free

#show interface brief

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-links) - Protocol Down Min-links  
DV - DDM Violation, NA - Not Applicable  
NOM - No operational members, PVID - Port Vlan-id  
Ctl - Control Port (Br-Breakout/Bu-Bundle)

-----										
--										
Ethernet Bu Interface	Type	PVID	Mode	Status	Reason	Speed	Port Ch #	Ctl	Br/	
-----										
--										
cel1/1	ETH	--	routed	up	none	10g	--	Br	Yes	
cel1/2	ETH	--	routed	up	none	10g	--	No	No	
cel1/3	ETH	--	routed	up	none	10g	--	No	No	
cel1/4	ETH	--	routed	up	none	10g	--	No	No	

Configuring Port Breakout (100G to 4x25G)

Configuring Port Breakout (100G to 4x25G) is provided in below section.

#configure terminal	Enter configure mode.
(config)#interface cel1/1	Specify the interface (cel1/1) to be configured for port Breakout.
(config-if)#port breakout enable 4x25g	Configure port breakout on interface
(config-if)#exit	Exit interface mode.

Note: Interface ce1/1 is back to back connected and interfaces are up.

Validation

VLAN-reservation validation

#show vlan-reservation	
VLAN ID	Status
=====	=====
4050	allocated
4051	allocated
4052	allocated
4053	allocated
4054	allocated
4055	allocated
4056	free
4057	free
4058	free

```
#show interface brief

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

-----
--
Ethernet  Type  PVID  Mode                Status  Reason  Speed Port    Ctl Br/Bu
Interface                                     Ch  #
-----
--
cel/1     ETH   --    routed              up      none    25g   --      Br
Yes
cel/2     ETH   --    routed              up      none    25g   --      No  No
cel/3     ETH   --    routed              up      none    25g   --      No  No
cel/4     ETH   --    routed              up      none    25g   --      No  No
```

## Configuring Port Breakout (100G to 2x50G)

Configuring Port Breakout (100G to 2x50G) is provided in below section.

#configure terminal	Enter configure mode.
(config)#interface cel/1	Specify the interface (cel/1) to be configured for port Breakout.
(config-if)#port breakout enable 2x50g	Configure port breakout on interface
(config-if)#exit	Exit interface mode.

Note: Interface cel/1 is back to back connected and interfaces are up.

## Validation

### VLAN-reservation validation

```
#show vlan-reservation
VLAN ID      Status
=====
4050         allocated
4051         allocated
4052         allocated
4053         allocated
4054         allocated
4055         allocated
4056         free
```

4057 free  
4058 free

#show interface brief

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-links) - Protocol Down Min-links  
DV - DDM Violation, NA - Not Applicable  
NOM - No operational members, PVID - Port Vlan-id  
Ctl - Control Port (Br-Breakout/Bu-Bundle)

-----									
--									
Ethernet	Type	PVID	Mode	Status	Reason	Speed	Port	Ctl	Br/
Bu									
Interface	Ch #								
-----									
--									
cel1/1	ETH	--	routed	up	none	50g	--		Br
Yes									
cel1/2	ETH	--	routed	down	IA	--	--	No	No
cel1/3	ETH	--	routed	up	none	50g	--	No	No
cel1/4	ETH	--	routed	down	IA	--	--	No	No

## Configuring Port Breakout at Global Configuration Level

This port breakout command at global configuration level is applicable only for Trident III and Tomahawk II platforms. The interface level breakout and global hardware-profile CLI does not work for Trident III and Tomahawk II platforms.

Configuring Port Breakout (4X10g | 4X25g | 2X50g) at global configuration level is provided in below section.

#configure terminal	Enter configure mode.
OcNOS(config)#port 49 breakout 4X10g	Specify the port interface number (49) to breakout to (2X50g or 4X10g 4X25g) at global interface, where 49 refers to ce49 interface.
OcNOS(config)#exit	Exit interface mode.

Note: After the port breakout, the interface name is changed to xe49/1-xe49/4 globally.

## Validation

### VLAN-reservation validation

```
#show vlan-reservation
VLAN ID      Status
=====
```

```
4050      allocated
4051      allocated
4052      allocated
4053      free
4054      free
4055      free
4056      free
4057      free
4058      free
```

```
#show running-config interface xe49/1
!
interface xe49/1
!
```

```
#show port-breakout details
-----
Max Brkout Avail      Max Brkout Avail

0 x4X or 0 x2X
```

```
4 x4X or 4 x2X
```

Block1			Block2		
Port		Mode	Port		Mode
1			40		
2			41		
3			43		
4			44		
5			45		
6			46		
7			47		
8			48		
9			49		4X10G
10			50		4X10G
11			51		4X10G
12			52		4X10G
13			53		
14			54		
15			55		
16			56		
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					



27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
42  
OcNOS#



## CHAPTER 20 Proxy ARP and Local Proxy ARP

### Overview

Proxy ARP (RFC 1027) is a technique by which a device on a given network answers the ARP queries for a network address that is not on that network. The Proxy ARP is aware of the location of the traffic's destination, and offers its own MAC address as destination. The captured traffic is then typically routed by the Proxy to the intended destination via another interface. Proxy ARP can help machines on a subnet reach remote subnets without the need to configure routing or a default gateway.

Use `no ip proxy-arp` to disable Proxy ARP, Proxy ARP is disabled by default.

### Topology

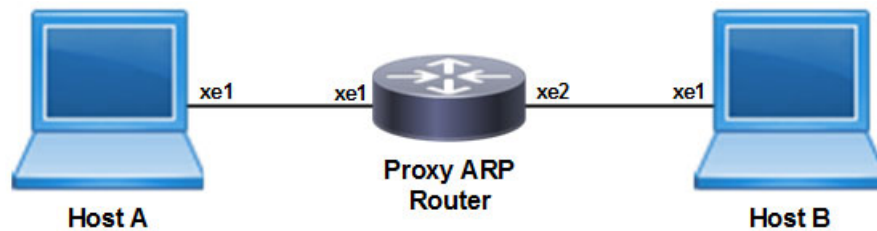


Figure 20-30: Sample topology

### Configuration

#### Host A

#configure terminal	Enter configure mode
(config)#interface xe1	Enter interface mode
(config-if)#ip address 20.20.0.2/24	Assign an IPv4 address to the interface
(config)#end	Exit interface and configure mode

#### Host B

#configure terminal	Enter configure mode
(config)#interface xe1	Enter interface mode
(config-if)#ip address 20.20.1.2/24	Assign an IPv4 address to the interface
(config)#end	Exit interface and configure mode

#### Proxy ARP Server

#configure terminal	Enter configure mode
(config)#interface xe1	Enter interface mode
(config-if)#ip address 20.20.0.1/24	Assign an IPv4 address to the interface

---

(config-if)#ip proxy-arp	Enable proxy ARP
(config-if)#exit	Exit interface mode
(config-if)#interface xe2	Enter interface mode
(config-if)#ip address 20.20.1.1/24	Assign an IPv4 address to the interface
(config)#end	Exit interface and configure mode

---

### Validation

```
#show running-config arp
!  
interface xe1  
ip proxy-arp  
!
```

The `show arp` command on the hosts shows the ARP table entries to reach different subnets. Ping Host B from Host A. The ARP table should have router's xe1 interface MAC address to reach Host B. Execute the command at Host A.

```
#show arp
```

Address	HWaddress	Interface	Type
20.20.0.2	52:54:00:24:43:23	eth1	Dynamic
192.168.52.1	fe:54:00:0d:1e:dc	eth0	Dynamic

---

### Local Proxy ARP Overview

The local proxy ARP feature enables local proxy support for ARP requests at the interface level. The router answers all ARP requests on the configured subnet, even for clients that should not normally need routing. Local proxy ARP means that the traffic comes in and goes out the same interface.

Local proxy ARP allows responding to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly.

## Topology

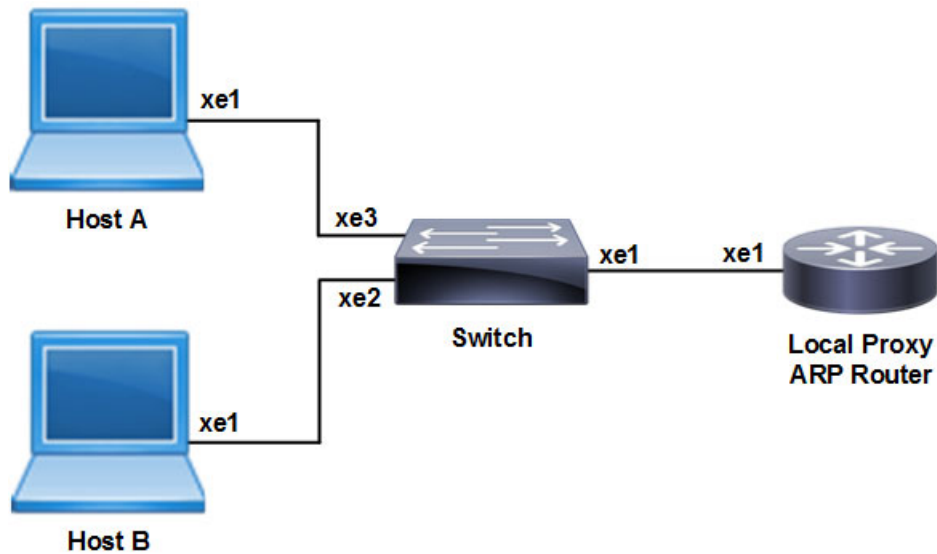


Figure 20-31: Sample topology

## Configuration

### Host A

#configure terminal	Enter configure mode
(config)#interface xe1	Enter interface mode
(config-if)#ip address 20.20.0.2/24	Assign an IPv4 address to the interface
(config)#end	Exit interface and configure mode

### Host B

#configure terminal	Enter configure mode
(config)#interface xe1	Enter interface mode
(config-if)#ip address 20.20.0.3/24	Assign an IPv4 address to the interface
(config)#end	Exit interface and configure mode

### Switch Private VLAN

#configure terminal	Enter configure mode
(config)#bridge 1 protocol ieee vlan-bridge	Create ieee vlan-bridge on switch for pvlan configuration
(config)#vlan database	Enter VLAN database mode
(config-vlan)#vlan 100-101 bridge 1 state enable	Create VLANs 100 and 101 as part of bridge 1
(config-vlan)#private-vlan 100 primary bridge 1	Configure VLAN 100 as primary VLAN
(config-vlan)#private-vlan 101 isolated bridge 1	Configure VLAN 101 as isolated VLAN

## Proxy ARP and Local Proxy ARP

(config-vlan)#private-vlan 100 association add 101 bridge 1	Associate secondary VLAN 101 to primary VLAN 100
(config-vlan)#exit	Exit VLAN database mode
(config)#interface xe1	Enter interface mode
(config-if)#switchport	Configure xe1 as a Layer 2 interface
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary VLAN to the interface
(config-if)#switchport mode private-vlan promiscuous	Make the interface a promiscuous port
(config-if)#switchport private-vlan mapping 100 add 101	Associate primary VLAN 100 and secondary VLAN 101 to a promiscuous port
(config-if)#exit	Exit interface mode
(config)#interface xe2	Enter interface mode
(config-if)#switchport	Make the interface a Layer 2 interface
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary VLAN to the interface
(config-if)#switchport mode private-vlan promiscuous	Make the interface a promiscuous port
(config-if)#switchport private-vlan mapping 100 add 101	Associate primary VLAN 100 and secondary VLAN 101 to a promiscuous port
(config-if)#exit	Exit interface mode
(config)#interface xe3	Enter interface mode
(config-if)#switchport	Make the interface a Layer 2 interface
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary VLAN to the interface
(config-if)#switchport mode private-vlan promiscuous	Make the interface a promiscuous port
(config-if)#switchport private-vlan mapping 100 add 101	Associate primary VLAN 100 and secondary VLAN 101 to a promiscuous port
(config-if)#exit	Exit interface mode

## Router Local Proxy ARP

#configure terminal	Enter configure mode
(config)#interface xe1	Enter interface mode
(config-if)#ip address 20.20.0.3/24	Assign an IPv4 address to the interface
(config-if)#ip local-proxy-arp	Enable local proxy ARP
(config)#end	Exit interface and configure mode

## Validation

The show arp command on hosts shows the arp table entries to reach different subnets. Ping Host B from Host A. The ARP table should have Router's xe1 interface MAC address to reach Host B. Execute the below command at Host A.

```
#show arp
```

Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default

Total number of entries: 2

Address	Age	MAC Address	Interface	State
20.20.0.3	00:02:39	ecf4.bbc0.3d71	xe1	STALE.





## CHAPTER 21 RADIUS Client Configuration

### Overview

Remote Authentication Dial In User Service (RADIUS) is a remote authentication protocol that is used to communicate with an authentication server.

A RADIUS server is responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

The key points for RADIUS authentication are:

- Transactions between client and server are authenticated through the use of a shared key and this key is never sent over the network.
- The password is encrypted before sending it over the network.

### RADIUS Server Authentication

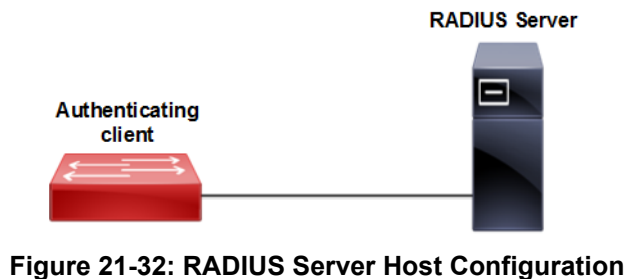


Figure 21-32: RADIUS Server Host Configuration

### Host

#configure terminal	Enter configure mode.
(config)# radius-server login key testing101 vrf management	Specify the global key for radius servers that are not configured with their respective keys for management vrf. This key should match the one present in the config file of tacacs server.
(config)# radius-server login key testing101	Specify the global key for radius servers that are not configured with their respective keys for default vrf. This key should match the one present in the config file of tacacs server
(config)# radius-server login host 10.16.19.2 vrf management seq-num 1 key testing123	Specify the radius server ipv4 address to be configured with shared local key for management vrf. The same key should be present on the server config file.
(config)# radius-server login host 10.16.19.2 seq-num 1 key testing123	Specify the radius server ipv4 address to be configured with shared local key for default vrf. The same key should be present on the server config file.
(config)# radius-server login host 10.12.30.86 vrf management seq-num 1 auth-port 1045	Specify the radius server ipv4 address to be configured with port number for management vrf. The radius server should be started with same port number.

(config)# radius-server login host 10.12.30.86 seq-num 1 auth-port 1045	Specify the radius server ipv4 address to be configured with port number for default vrf. The radius server should be started with same port number
(config)#radius-server login host 10.12.17.11 vrf management seq-num 1 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for management vrf. The radius server should be started with same port number.
(config)#radius-server login host 10.12.17.11 seq-num 1 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for default vrf. The radius server should be started with same port number. The radius server should be started with same port number
(config)#radius-server login host Radius-Server-1 vrf management seq-num 2 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 2	Specify the radius server configured with hostname, key authentication port number, accounting port number, for management VRF. The radius server should be started with same port number
radius-server login host Radius-Server-1 seq-num 2 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 2	Specify the radius server configured with hostname sequence number, key and port number for default VRF. The radius server should be started with same port number.
(config)#aaa authentication login default vrf management group radius	Enable authentication for radius server configured for management VRF. Authorization is also enabled by default
(config)#aaa authentication login default group radius	Enable authentication for radius server configured for default vrf. Authorization is also enabled by default.
(config)#aaa authentication login default vrf management group radius local	Enable authentication for radius server and fallback to local configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group radius local	Enable authentication for radius server and fallback to local configured for default vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group radius local none	Enable authentication for radius server, fallback to local followed by fallback to none, configured for management VRF. Authorization is also enabled by default
(config)#aaa authentication login default radius local none	Enable authentication for radius server, fallback to local followed by fallback to none, configured for default vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group radius none	Enable authentication for radius, fallback to none, configured for management VRF. Authorization is also enabled by default
(config)#aaa authentication login default group radius none	Enable authentication for radius, fallback to none, configured for default VRF. Authorization is also enabled by default
(config)#aaa group server radius G1 vrf management	Create aaa radius group G1 for management vrf
(config)#aaa group server radius G1	Create AAA radius group G1 for default VRF
(config-radius)#server 10.12.30.86	Make the radius server 10.12.30.86 a part of this group G1 for default VRF
(config-radius)#server Radius-Server-1	Make Radius-Server-1 a part of this group G1
(config-radius)#exit	Exit radius mode
(config)#aaa group server radius G1	Enter radius mode
(config-radius)#server 10.12.30.86	Make the radius server 10.12.30.86 a part of this group G1 for default vrf
(config-radius)#server Radius-Server-1	Make Radius-Server-1 a part of this group G1
(config)#exit	Exit radius mode.

(config)#aaa authentication login default vrf management group G1	Authenticate the tacacs+ group G1 with aaa authentication for management vrf
(config)#aaa authentication login default group G1	Authenticate the tacacs+ group G1 with aaa authentication for default vrf

## Validation

To verify the RADIUS authentication process, use SSH or Telnet from the host machine to Host IP with the authenticating user created, and provide a RADIUS server password and check whether the client validates the user with the corresponding username and password.

```
OcNOS#show radius-server vrf management
      VRF: management
Global RADIUS shared secret: *****
timeout value: 5
```

Total number of servers:3

Following RADIUS servers are configured:

```
10.12.17.11:
  available for authentication on port:60000
  available for accounting on port:60000
  timeout:6
  RADIUS shared secret:*****

10.12.30.86:
  available for authentication on port:1045
  available for accounting on port:1813

10.16.19.2:
  available for authentication on port:1812
  available for accounting on port:1813
  RADIUS shared secret:*****
```

```
#show radius-server vrf all
      VRF: management
timeout value: 5
```

Total number of servers:2

Following RADIUS servers are configured:

```
100.0.0.1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****

Radius-Server-1:
  available for authentication on port:60000
  available for accounting on port:60000
```

## RADIUS Client Configuration

---

```
        RADIUS shared secret:*****
    VRF: default
timeout value: 5
```

Total number of servers:2

Following RADIUS servers are configured:

```
Radius-Server-1:
    available for authentication on port:60000
    available for accounting on port:60000
    RADIUS shared secret:*****

100.0.0.1:
    available for authentication on port:60000
    available for accounting on port:60000
    RADIUS shared secret:*****
```

```
#show radius-server
    VRF: default
timeout value: 5
```

Total number of servers:2

Following RADIUS servers are configured:

```
Radius-Server-1:
    available for authentication on port:60000
    available for accounting on port:60000
    RADIUS shared secret:*****

100.0.0.1:
    available for authentication on port:60000
    available for accounting on port:60000
    RADIUS shared secret:*****
```

```
#show radius-server vrf management sorted
    VRF: management
timeout value: 5
```

Total number of servers:2

Following RADIUS servers are configured:

```
100.0.0.1:
    available for authentication on port:60000
    available for accounting on port:60000
    RADIUS shared secret:*****
```

```
Radius-Server-1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
#show radius-server vrf all sorted
      VRF: management
timeout value: 5
```

Total number of servers:2

Following RADIUS servers are configured:

```
100.0.0.1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
Radius-Server-1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
      VRF: default
timeout value: 5
```

Total number of servers:2

Following RADIUS servers are configured:

```
100.0.0.1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
Radius-Server-1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
#show radius-server sorted
      VRF: default
timeout value: 5
```

Total number of servers:2

Following RADIUS servers are configured:

```
100.0.0.1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
Radius-Server-1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
#show radius-server vrf management groups
```

```
VRF: management
```

```
group radius:
```

```
  server: all configured radius servers
```

```
group rad1:
```

```
  server Radius-Server-1:
    auth_port is 60000
    acct_port is 60000
    key is *****
```

```
  server 100.0.0.1:
    auth_port is 60000
    acct_port is 60000
    key is *****
```

```
#show radius-server vrf all groups
```

```
VRF: management
```

```
group radius:
```

```
  server: all configured radius servers
```

```
group rad1:
```

```
  server Radius-Server-1:
    auth_port is 60000
    acct_port is 60000
    key is *****
```

```
  server 100.0.0.1:
    auth_port is 60000
    acct_port is 60000
    key is *****
```

```
VRF: default
```

```
group radius:
```

```
  server: all configured radius servers
```

```
group rad1:
    server Radius-Server-1:
        auth_port is 60000
        acct_port is 60000
        key is *****

    server 100.0.0.1:
        auth_port is 60000
        acct_port is 60000
        key is *****
```

```
#show radius-server groups
VRF: default
```

```
group radius:
    server: all configured radius servers
```

```
group rad1:
    server Radius-Server-1:
        auth_port is 60000
        acct_port is 60000
        key is *****

    server 100.0.0.1:
        auth_port is 60000
        acct_port is 60000
        key is *****
```

```
#show radius-server vrf management groups rad1
VRF: management
```

```
group rad1:
    server Radius-Server-1
        auth_port is 60000
        acct_port is 60000
        key is *****

    server 100.0.0.1
        auth_port is 60000
        acct_port is 60000
        key is *****
```

```
#show radius-server vrf all groups rad1
VRF: management
```

```
group rad1:
    server Radius-Server-1
        auth_port is 60000
        acct_port is 60000
        key is *****
```

```
server 100.0.0.1
auth_port is 60000
acct_port is 60000
key is *****
```

VRF: default

```
group rad1:
server Radius-Server-1
auth_port is 60000
acct_port is 60000
key is *****

server 100.0.0.1
auth_port is 60000
acct_port is 60000
key is *****
```

```
#show radius-server groups rad1
VRF: default
```

```
group rad1:
server Radius-Server-1
auth_port is 60000
acct_port is 60000
key is *****

server 100.0.0.1
auth_port is 60000
acct_port is 60000
key is *****
```

```
#show radius vrf management
VRF: management
timeout value: 5
```

Total number of servers:2

Following RADIUS servers are configured:

```
100.0.0.1:
available for authentication on port:60000
available for accounting on port:60000
RADIUS shared secret:*****
```

```
Radius-Server-1:
available for authentication on port:60000
available for accounting on port:60000
```



RADIUS shared secret:\*\*\*\*\*

```
#show radius vrf all
      VRF: management
timeout value: 5
```

Total number of servers:2

Following RADIUS servers are configured:

```
100.0.0.1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
Radius-Server-1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
      VRF: default
timeout value: 5
```

Total number of servers:2

Following RADIUS servers are configured:

```
Radius-Server-1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
100.0.0.1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
#show radius
      VRF: default
timeout value: 5
```

Total number of servers:2

Following RADIUS servers are configured:

```
Radius-Server-1:
  available for authentication on port:60000
  available for accounting on port:60000
  RADIUS shared secret:*****
```

```
100.0.0.1:
```

```
available for authentication on port:60000
available for accounting on port:60000
RADIUS shared secret:*****
```

```
#show aaa authentication vrf management
      VRF: management
default: group radius
console: local
```

```
#show aaa authentication vrf all
      VRF: management
default: group radius
console: local
```

```
      VRF: default
default: group radius
console: local
```

```
#show aaa authentication
      VRF: default
default: group radius
console: local
```

```
#show aaa groups vrf management
      VRF: management
radius
rad1
```

```
rad1
```

```
#show aaa groups vrf all
      VRF: management
radius
rad1
```

```
      VRF: default
radius
rad1
```

```
#show aaa groups
      VRF: default
radius
rad1
```

```
#show running-config radius
radius-server login host 100.0.0.1 vrf management seq-num 1 key 7 wawyanb123 auth-port
600
00 acct-port 60000
radius-server login host Radius-Server-1 vrf management seq-num 1 key 7 wawyanb123
auth-po
```

```
rt 60000 acct-port 60000
```

```
radius-server login host Radius-Server-1 seq-num 1 key 7 wawyanb123 auth-port 60000  
acct-  
port 60000  
radius-server login host 100.0.0.1 seq-num 1 key 7 wawyanb123 auth-port 60000 acct-port  
6  
000
```

```
#show running-config aaa  
aaa authentication login default vrf management group radius  
aaa group server radius rad1 vrf management  
    server Radius-Server-1 vrf management  
    server 100.0.0.1 vrf management
```

```
aaa authentication login default group radius  
aaa group server radius rad1  
    server Radius-Server-1  
    server 100.0.0.1
```

```
#show running-config aaa all  
aaa authentication login default vrf management group radius  
aaa authentication login console local  
aaa accounting default vrf management local  
no aaa authentication login default fallback error local vrf management  
no aaa authentication login console fallback error local  
no aaa authentication login error-enable vrf management  
aaa local authentication attempts max-fail 3  
aaa local authentication unlock-timeout 1200  
aaa group server radius rad1 vrf management  
    server Radius-Server-1 vrf management  
    server 100.0.0.1 vrf management
```

```
aaa authentication login default group radius  
aaa authentication login console local  
aaa accounting default local  
no aaa authentication login default fallback error local  
no aaa authentication login console fallback error local  
no aaa authentication login error-enable  
aaa local authentication attempts max-fail 3  
aaa local authentication unlock-timeout 1200  
aaa group server radius rad1  
    server Radius-Server-1  
    server 100.0.0.1
```

---

## RADIUS Server Accounting

You can configure accounting to measure the resources that another user consumes during access.

User

#configure terminal	Enter configure mode.
(config)#radius-server login host 10.12.17.11 vrf management seq-num 1 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for management vrf. The radius server should be started with same port number.
(config)#radius-server login host 10.12.17.11 seq-num 1 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6	Specify the radius server ipv4 address to be configured with port number for default vrf. The radius server should be started with same port number
(config)#aaa accounting default vrf management group radius	Enable accounting for radius server configured for vrf management
(config)#aaa accounting default group radius	Enable accounting for radius server configured for default vrf

Validation

```
#show aaa accounting vrf management
      VRF: management
      default: group radius

#show aaa accounting vrf all
      VRF: management
      default: group radius

      VRF: default
      default: group radius

#show aaa accounting
      VRF: default
      default: group radius
#
#show running-config aaa
aaa authentication login default vrf management group radius
aaa accounting default vrf management group radius
aaa group server radius rad1 vrf management
    server Radius-Server-1 vrf management
    server 100.0.0.1 vrf management

aaa authentication login default  group radius
aaa accounting default  group radius
aaa group server radius rad1
    server Radius-Server-1
    server 100.0.0.1
```

Sample Radius Clients.conf File

```
client 10.12.58.20 {
    secret      = testing123
```

```
    shortname = localhost
}
client 192.168.1.2 {
    secret      = testing123
    shortname = localhost
}
client 10.12.37.196 {
    secret      = testing123
}
client 100.0.0.2 {
    secret      = testing123
    shortname = localhost
}

# IPv6 Client
#client ::1 {
#    secret      = testing123
#    shortname = localhost
#}
#
# All IPv6 Site-local clients
#client fe80::/16 {
#    secret      = testing123
#    shortname = localhost
```

---

## Sample Radius Users Configuration File

```
#
#DEFAULT
#    Service-Type = Login-User,
#    Login-Service = Rlogin,
#    Login-IP-Host = shellbox.ispdomain.com

# #
# # Last default: shell on the local terminal server.
# #
# DEFAULT
#    Service-Type = Administrative-User

# On no match, the user is denied access.

selftest Cleartext-Password := "password"
testuser1 Cleartext-Password := "user1@101"
testuser2 Cleartext-Password := "user2@202"
testuser3 Cleartext-Password := "user3@303"
```



## CHAPTER 22 sFlow Configuration

### Overview

This chapter provides the steps for configuring Sampled Flow (sFlow).

sFlow is the standard for monitoring high-speed switched and routed networks. The sFlow monitoring system consists of an sFlow Agent which is embedded in a switch or router and an sFlow Collector.

The sFlow agent samples packets as well as polling traffic statistics for the device it is monitoring. The packet sampling is performed by the switching/routing device at wire speed. The sFlow agent forwards the sampled traffic statistics in sFlow PDUs as well as sampled packets to an sFlow collector for analysis.

Note: sFlow egress sampling for multicast, broadcast, or unknown unicast packets is not supported.

The sFlow agent uses the following forms of sampling:

- Sampling packets: samples one packet out of a defined sampling rate. This sampling is done by hardware at wire speed.
- Sampling counters: polls interface statistics such as generic and Ethernet counters at a defined interval.

You must enable the sFlow feature and collector before enabling sFlow sampling on an interface.

You cannot globally enable sFlow sampling monitoring on all interfaces with a single command. Instead you must enable sFlow sampling on the required interfaces individually.

sFlow feature is supported on physical interface as well as LAG interface. Configuring sampling on a LAG interface will enable the same on all member ports part of that LAG interface.

### Topology

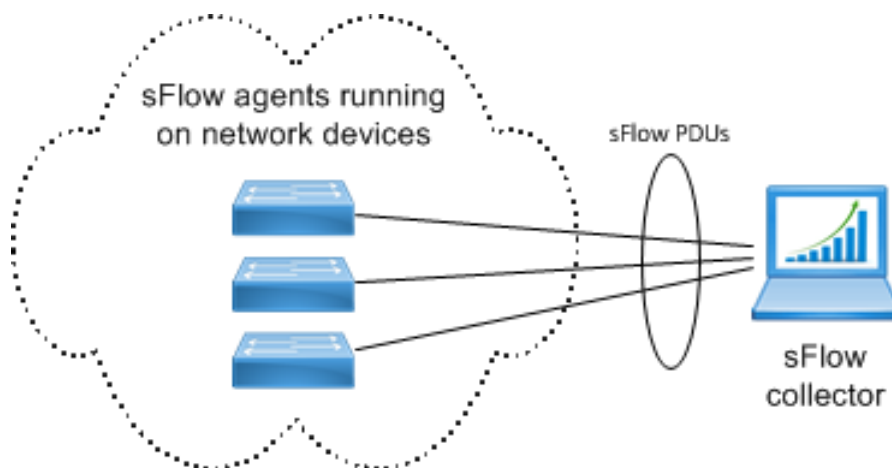


Figure 22-33: Basic sFlow topology

# Configuration

## sFlow Agent

#configure terminal	Enter configure mode.
(config)#feature sflow	Enable the sFlow feature.
(config)#sflow collector 2.2.2.2 port 6343 receiver-time-out 0 max-datagram-size 200	Configure the sFlow collector. The IP address must be reachable via the management VRF.
(config)#interface xe1	Enter interface mode
(config-if)#sflow poll-interval 5	Set the counter poll Interval on the interface.
(config-if)#sflow sampling-rate 1024 direction ingress max-header-size 200	Set the sFlow sampling interval on the interface in ingress directions.
(config-if)#sflow sampling-rate 1024 direction egress max-header-size 200	Set the sFlow sampling interval on the interface in egress directions.
(config-if)#sflow enable	Start packet sampling on the interface
(config-if)#end	Exit interface and configure mode.

# Validation

```
OcNOS#show sflow detail
sFlow Feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent      IP: 10.10.26.132
Collector IP: 10.156.159.29    Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)         : 0
```

sFlow Port Detailed Information:						
Interface	Packet-Sampling		Packet-Sampling		Counter-	
	Count	Rate	Count	Interval		
Count	Size(bytes)		Count			
Ingress	Ingress	Egress	Ingress	Egress	(sec)	
	Egress					
-----	-----	-----	-----	-----	-----	
-----	-----	-----	-----	-----	-----	
xe1/1	1024	1024	464564	414532	5	
131	200	20				



## CHAPTER 23 Show Tech Support Configurations

### Overview

OcNOS maintains a collection of consolidated information about system configurations and statistics. This information is for debugging and diagnosing system issues, and can be uploaded to a remote server. You generate a file with this information via the `show techsupport` command.

**Note:** Output is not displayed on the terminal.

The default directory (`/var/log/`) is where the stored information is saved. The filename has the form: `tech_support_YYYY_MMM_DD_HH_MM_SS.tar.gz`. If a file name is specified, the information will be saved to `filename_YYYY_MMM_DD_HH_MM_SS.tar.gz`. Date stamps are in the `YYYY_MM_DD` form, and time stamps are in the form `HH_MM_SS`.

The collected system data contains the following logs:

- Saved start-up configuration of the system.
- The `running-config`, and statistics for a specified module or all modules.
- The last 100 commands.
- Memory and CPU usage of the process.
- Process Id and process name.
- The user account running the process.

### Tech Support Samples

<code>#show techsupport all</code>	Collects system configurations and statistics for all modules, and saves it in <code>tech_support_date_timestamp.tar.gz</code> in the <code>/var/log/</code> directory.
<code>#show techsupport all log-path /home/ filename</code>	Collects system configurations and statistics for all modules, and saves it in <code>filename_date_timestamp.tar.gz</code> in the <code>/home/</code> directory.
<code>#show techsupport nsm</code>	Collects <code>nsm</code> protocol configurations and statistics, and saves it in <code>tech_support_date_timestamp.tar.gz</code> in the <code>/var/log/</code> directory.
<code>#show techsupport nsm log-path /home/ filename</code>	Collects <code>nsm</code> protocol configurations and statistics, and saves it at <code>filename_date_timestamp.tar.gz</code> in the <code>/home/</code> directory.
<code>#show techsupport hostpd authd imi</code>	Collects <code>hostpd</code> , <code>authd</code> , and <code>imi</code> protocol configurations and statistics and saves it at <code>tech_support_date_timestamp.tar.gz</code> in the <code>/var/log/</code> directory.
<code>#show techsupport hostpd authd imi log-path /home/ filename</code>	Collects <code>hostpd</code> , <code>authd</code> , <code>imi</code> protocol configurations and statistics, saves it as <code>filename_date_timestamp.tar.gz</code> in the <code>/home/</code> directory.

---

## Validation Commands

You can display the status of a `show techsupport` command given earlier which indicates the protocol modules that have completed, are in progress, or have not executed. If the command has completed, it lists the last five generated tech support files with their path.

```
#show techsupport status
```

```
Tech Support Command Execution Is Complete
##Generated Tech Support File-list
/var/log/tech_support_18_Dec_2017_20_39_02.tar.gz
#
```

**Note:** the running `show techsupport` operation has not completed, reentering the `show techsupport` command is ignored.

## CHAPTER 24 Simple Network Management Protocol

### Overview

SNMP provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- An SNMP manager: The system used to control and monitor the activities of network devices. This is sometimes called a Network Management System (NMS).
- An SNMP agent: The component within a managed device that maintains the data for the device and reports these data SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables which describe the system configuration. These variables can be queried by SNMP managers.

In SNMP, administration groups are known as communities. SNMP communities consist of one agent and one or more SNMP managers. You can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The security levels are:

- noAuthNoPriv: No authentication or encryption
- authNoPriv: Authentication but no encryption
- authPriv: Both authentication and encryption

SNMP is defined in RFCs 3411-3418.

### Topology

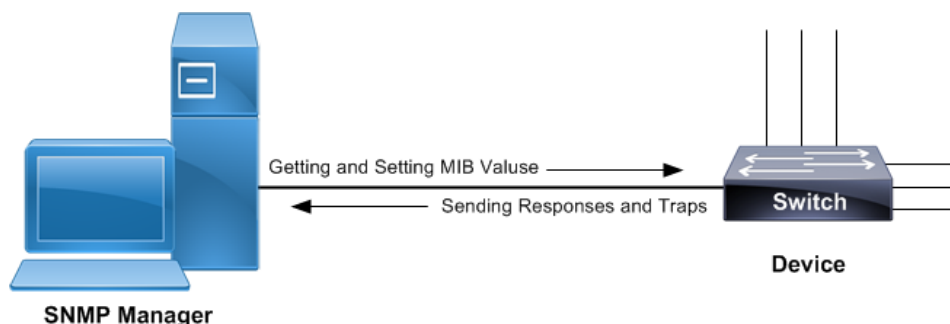


Figure 24-34: SNMP sample topology

## Standard SNMP Configurations

#configure terminal	Enter configure mode.
(config)#snmp-server view all .1 included vrf management	Creates SNMP view labeled as "all" for OID-Tree as ".1" for vrf management.
(config)#snmp-server community test group network-operator vrf management	Set community string as "test" for group of users having "network-operator" privilege.
(config)#snmp-server host 10.12.6.63 traps version 2c test udp-port 162 vrf management	Specify host "10.12.6.63" to receive SNMP version 2 notifications at udp port number 162 with community string as "test".
(config)#snmp-server enable snmp vrf management	Use this command to start the SNMP agent.
(config)#exit	Exit configure mode.

## Validation

Use the below commands to verify the SNMP configuration:

```
#show running-config snmp
snmp-server view all .1 included vrf management
snmp-server community test group network-operator vrf management
snmp-server host 10.12.6.63 traps version 2c test udp-port 162 vrf management

#show snmp group
-----
community/user      group              version  Read-View  Write-view  Notify-view
-----
test                network-operator   2c/1     all         none         all

#show snmp host
-----
Host                Port  Version  Level      Type      SecName
-----
10.12.6.63          162   2c       noauth     trap      test
```

## SNMP GET Command

```
# snmpget -v2c -c test 10.12.45.238
.1.3.6.1.2.1.6.13.1.2.10.12.45.238.22.10.12.6.63.52214

TCP-MIB::tcpConnLocalAddress.10.12.45.238.22.10.12.6.63.52214 = IPAddress:
10.12.45.238
```

## SNMP WALK Command

### SNMP WALK for particular OID

```
#snmpwalk -v2c -c test 10.12.45.238 .1.3.6.1.2.1.25.3.8.1.8
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.1 = STRING: 0-1-1,0:0:0.0
```

```
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.4 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.5 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.6 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.10 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.12 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.13 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.14 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.15 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.16 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.17 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.18 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.19 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.20 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.21 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.22 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.23 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.24 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.25 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.26 = STRING: 0-1-1,0:0:0.0
```

### **Complete SNMP WALK**

```
#snmpwalk -v2c -c test 10.12.45.238 .1
```



## CHAPTER 25 Software Monitoring and Reporting

### Overview

OcNOS provides a mechanism (called “watchdogging”) to monitor all OcNOS modules and provides the following functions.

1. Periodic heart beat check.
2. Automatic restarts of a module upon a hung state or crash detection.
3. Upon hanging or crashing of a module, a crash report (including system states) is logged.
4. A proprietary SNMP trap is sent to the trap manager, if configured, after a fault is detected in a protocol module. Similarly a trap is sent when the module recovers.

By default, the software watchdog is enabled and the keep-alive time interval is 60 seconds. All OcNOS processes periodically send keep-alive messages to a monitoring module at the configured keep-alive time interval.

This functionality can be disabled for a particular module or all OcNOS modules by using CLI commands. In order to permanently disable software monitoring functionality, the user has to disable the watchdog feature. If, however, software watchdogging is disabled the monitoring module doesn't take any action upon a hang or crash of any OcNOS module.

### Configuration

#configure terminal	Enter configure mode.
(config)#feature software-watchdog	Enable software watchdog for all OcNOS modules — This is the default.
(config)#no software-watchdog imi	To disable software watchdog for only imi modules.
(config)#software-watchdog keep-alive-time 100	The keep-alive time interval in seconds. Default is 60 seconds and applies to all OcNOS modules.
#show software-watchdog status	Display the keep-alive time interval and list of OcNOS process names with watchdog status for each OcNOS modules.

### Validation

```
#show software-watchdog status
Software Watchdog timeout in seconds : 100
Process name           Watchdog status
=====
nsm                     Enabled
ripd                   Enabled
ospfd                  Enabled
isisd                  Enabled
hostpd                 Enabled
```

ldpd	Enabled
rsvpd	Enabled
mribd	Enabled
pimd	Enabled
authd	Enabled
mstpd	Enabled
imi	Disabled
onmd	Enabled
HSL	Enabled
oam	Enabled
vlogd	Enabled
vrrpd	Enabled
ndd	Enabled
ribd	Enabled
bgpd	Enabled
l2mribd	Enabled
lagd	Enabled
sflow	Enabled



# CHAPTER 26 SSH Client Server Configuration

## Overview

SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plain text, rendering them susceptible to packet analysis.[2] The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user.

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols. SSH uses the client-server model

TCP port 22 is assigned for contacting SSH servers. This document covers the SSH server configuration to enable SSH service and key generation and SSH client configuration for remote login to server.

## In-band Management over Default VRF

OcNOS supports SSH over the default and management VRFs via the in-band management interface and out-of-band management interfaces, respectively.

SSH can run on the default and management VRFs simultaneously. By default, it runs on the management VRF.

## Topology



Figure 26-35: SSH sample topology

## Basic Configuration

#configure terminal	Enter configure mode
(config)#ssh login-attempts 2 vrf management	Set the number of login attempts to 2
(config)#exit	Exit configuration mode

## Validation

```
#show ssh server
ssh server enabled port: 22
authentication-retries 2
```

```
#show running-config ssh server
feature ssh vrf management
ssh login-attempts 2 vrf management
```

## SSH Client Session

When the device acts as an SSH client, it supports both SSH IPv4 sessions to log into the remote machine.

#ssh root@10.10.10.1 vrf management	Log into remote machine using an IPv4 address
-------------------------------------	---

## SSH Keys

Use the ssh key command to generate new RSA/DSA keys for the SSH server. By default, the system has RSA/DSA public/private key pair placed in /etc/ssh/. If you want to regenerate RSA keys, you must specify the force option.

## Configuration

#ssh keygen host rsa vrf management	Specify the <code>force</code> option to regenerate SSH RSA keys. This option overwrites the existing key.
-------------------------------------	--

## Validation

```
#sh ssh key
*****RSA KEY*****
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDMuVc0jpnGMyNzaqzIELX6LlsaK/
1q7pBixmwHAGDsZm/
dClTLb18AIB27W68YD8k0+Yw0LR0rHuPtNeSFMEsMaQxsaLkSi7yg86xSJaqgLQTyOUTS/
OC9hreXkJ73ay
n0yXa8+bre0oyJq1NWxAI9B1jEhfSSAipoDSp/
dmc93VJyV+3hgylFMTAheyebQaUveLBEMH7siRlSfyo7OHsBYSF6GzAmSuCm6PAelpHm/
3L4gChcnPL+0outQOifCSLdUOXEZhTFXrzC61l+14LGt8pR6YN+2uEnU6kq1i
aDLEffiWK4dWCp67JUief1BTOvxRurpssuRdslhJQXDFaj
bitcount: 2048 fingerprint: a4:23:5d:8a:5a:54:8b:3e:0b:38:06:79:82:e9:83:48
*****
*****DSA KEY*****
ssh-dsa AAAAB3NzaC1kc3MAAACBALpY6MFhFPYI+VcAHzHppnwVnNXv9oR/
EGHUM50BBqdQE1Qilmlt1rft4oa4tYR46P4gazKnnNfVE/
97FwEbCZaXaz9Wzfcfa3ALtsvGdyNQqk2BebYiRnmeWnS3wGV0M/D64bAiV0
2p/
LyF6D0ygMnZ3up3ttTN5QfHeyYQtwyZAAAFQD+k6wQyr51IhXIQSSQD8by8qxjUwAAAIb0LxP3ljn
fzxEXyEkNNzlxCcJ7ZZkFYUmtDJxRZlDceuSf4QipMrQVrdrgdqZNhrUiDWM/
HaCM09LdEQxfPh5TaIwPyccngn
VUS83Tx577ofBW6hellTey3B3/3I+FfiGKUXS/
mZSyf5FW3swwyZwMkF0mV0SRCYTprnFt5qx8awAAAIEAjDNqMkyxUvB6JBqfo7zbGqXjBQmJ+dE8fG
jI2znlgq4lhYcMZJVNWtTiydDIgMVNffKcldAT3zr6qMzFgV56EbK
1qUu103K5CF44XfVkyNcHJV+/
fcfAJasGU8W6oSbU5Q08abyMsIGRYTurOMkRhvif6sxvieEpVnVK2/nPVVXA=
bitcount: 1024 fingerprint: d9:7a:80:e0:76:48:20:72:a6:5b:1c:67:da:91:9f:52
*****
```

**Note:** The newly created rsa/dsa key can be verified by logging into the device from a remote machine and checking whether the newly created key's fingerprint matches with the logging session fingerprint.

---

## SSH Encryption Cipher

Specify an SSH cipher to encrypt an SSH session. By default, all the ciphers are supported for a new SSH client to connect to the SSH server.

SSH supports these encryption algorithms:

- Advanced Encryption Standard Counter:
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - aes128-cbc
- Advanced Encryption Standard Cipher Block Chaining:
  - aes192-cbc
  - aes256-cbc
- Triple Data Encryption Standard Cipher Block Chaining:
  - 3des-cbc

---

## Configuration

#configure terminal	Enter configuration mode
(config)#ssh server algorithm encryption aes128-ctr vrf management	Set the SSH server encryption algorithm to AES 128 bit counter
(config)#ssh server algorithm encryption aes128-cbc vrf management	Set the SSH server encryption algorithm to AES 128 cipher block chaining
(config)#exit	Exit configuration mode

---

## Validation

The new cipher encryption algorithm takes effect for a new incoming ssh client connection.

```
#show running-config ssh server
feature ssh vrf management
ssh server algorithm encryption aes128-ctr aes128-cbc vrf management
```

---

## SSH Client Session

#ssh cipher aes128-ctr <a href="#">root@1.1.1.1</a> vrf management	Specify AES 128-bit counter encryption to establish an SSH connection to a remote machine using an IPv4 address
--	---

---

## SSH Key Based Authentication

Enable OcnOS device SSH server to perform public key based SSH authentication, to enable machine to machine communication possible without requiring password. Public key based authentication increases the trust between two Linux servers for easy file synchronization or transfer. Public-key authentication with SSH is more secure than password authentication, as it provides much stronger identity checking through keys.

---

## Topology



Figure 26-36: SSH Key based Authentication sample topology

---

## Public Key Authentication Method

The server has the public key of the user stored; using this the server creates a random value, encrypts it with the public key and sends it to the user. If the user is who is supposed to be, he can decrypt the challenge using the private key and send it back to the server, server uses the public key again to decrypt received message to confirm the identity of the user. SSH is supported in In-band (default VRF) and Out of band (management VRF). Installed keys are stored at `~/.ssh/authorized_keys` file.

SSH key based authentication steps:

1. Login to remote machine linux desktop (ssh client) and generate the key pair using the command “ssh-keygen”.
2. Create username in OCNOS switch device (ssh server).
3. Install the public key of remote Linux ssh client in OCNOS device.
4. Display the installed key in OCNOS device using “show running-config”.
5. Login from remote Linux ssh client to OCNOS device without providing password.

---

## Useful commands on Remote Desktop Client

# ssh-keygen	To generate key pair on remote Linux machine (ssh client)
# cd /bob/.ssh/	To go to the location of saved key pair
# cat id_rsa.pub	Command to display the generated public key in remote Linux client

## Configuration commands in OCNOS

#configure terminal	Enter configure mode.
#feature ssh vrf management	Enable the SSH feature on vrf management. To enable in default vrf give the command "feature ssh"
# username fred	To create username with default role as network-user. To create user with different role specify role using command "username <username> role <role_name>"
# username fred sshkey ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/VHVgU2Y0/ ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZzUt0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxlrlve3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfRQJXriQml+QcJ9NER5O8rMS5D5NnTVhlnroqoozY8i/ qMKfhCFMbysjiDMHU9GclNsNbIF/DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgzOaVw16Cy3csoTncw0vyXVbob@localhost.localdomain	Install the public key of remote Linux client in ocnos device.
#exit	Exit configuration mode

## Validation

The new cipher encryption algorithm takes effect for a new incoming ssh client connection.

```
#show running-config

<skipped other content>
feature ssh vrf management
username fred role network-user
username fred sshkey
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZzUt0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxlrlve3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfRQJXriQml+QcJ9NER5O8rMS5D5NnTVhlnroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgzOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
<skipped other content>
OCNOS#show running-config ssh server
feature ssh vrf management
```

## SSH Key based Client Session

#ssh fred@10.10.26.186	Specify user name and ip address to access the device. Supports IPv4 and IPv6. User should be able to access without password and through key based authentication
------------------------	--

## Restrictions

1. Key generation or installation are not supported for “root” user account in OcNOS device.
2. Third party SSH utilities cannot be used for key installation, rather OcNOS CLI interface is the only way to install public keys.

Sample Use case:

### Step 1 :

```

Login to remote machine linux desktop (ssh client) and generate the key pair
using the command "ssh-keygen"
[bob@localhost ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/bob/.ssh/id_rsa):
/bob/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /bob/.ssh/id_rsa.
Your public key has been saved in /bob/.ssh/id_rsa.pub.
The key fingerprint is:
b2:d0:cc:d2:dd:db:3d:05:c1:33:fc:4a:df:8e:85:af bob@localhost.localdomain
The key's randomart image is:
+--[ RSA 2048 ]-----+
|           o.  |
|           =.  |
|          .+  |
|         = . .  |
|        o * S .  |
|       o o  o .o.+|
|      .   . . o= |
|             ..o|
|            E.  |
+-----+
[bob@localhost ~]# cd /bob/.ssh/
[bob@localhost .ssh]# cat id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQBAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0Sb
cU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZzut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlv
e3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jxlSE8UI98WyIcwuq44tzuIaUYAICIfRQJXriQml
+QcJ9NER5O8rMS5D5NnTVhlnroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
[bob@localhost .ssh]#

```

### Step 2 :

```

Create username in OCNOS switch device (ssh server)
OCNOS(config)#username fred
Note : By default user role will be network-user

```

### Step 3 :

```

Install the public key of remote Linux ssh client in OCNOS device.
OCNOS(config)#username fred sshkey
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQBAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0Sb
cU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZzut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlv

```

```
e3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfRQJXriQml
+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgzkOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
```

**Step 4 :**

Display the installed key in OCNOS device using "show running-config"

```
OCNOS#show running-config
<skipped other content>
username fred role network-user
username fred sshkey
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQAC8XhFiGlZP6yY6qIWUkew884NvqXqMPSow3fQe5kgpXvX0Sb
cU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlv
e3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfRQJXriQml
+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgzkOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
<skipped other content>
```

**Step 5 :**

Login from remote Linux ssh client to OCNOS device without providing password  
[bob@localhost .ssh]# ssh fred@10.10.26.186

```
OCNOS >en
OCNOS #
```





## CHAPTER 27 Syslog Configuration

Syslog is a standard for logging system messages. Logging helps for fault notification, network forensics, and security auditing.

OcNOS supports logging messages to a syslog server in addition to logging to a file or on the VTY terminal (ssh/telnet connection) and on the TTY serial console device. OcNOS messages can be logged to a local syslog server (the system on which OcNOS executes) into `/var/log/messages` by default as well as to one or multiple remote syslog servers (maximum of 8 remote syslog server is supported). Remote syslog servers can either be configured with IPv4 addresses or host names.

### Support for In-band management over default VRF

OcNOS shall stream logs to remote syslog server through the interfaces associated with management VRF by default. Also OcNOS provides configurable option to stream the logs through interfaces associated with default VRF. At any point of time OcNOS shall stream logs through only one VRF.

### Topology



Figure 27-37: Syslog sample topology

### Enabling rsyslog

<code>#configure terminal</code>	Enter configure mode.
<code>config)#feature rsyslog vrf management</code>	Enable syslog feature on default or management VRF. By default this feature runs on the management VRF.
<code>config)#exit</code>	Exit configuration mode

### Logging to a File

The below configurations enable debug logs for a particular protocol. In this case, OSPF is shown.

<code>#debug ospf all</code>	This enables the debugging on OSPF.
<code>#configure terminal</code>	Enter configure mode
<code>(config)#router ospf 1</code>	Enable OSPF process 1
<code>(config-router)#exit</code>	Exit router mode
<code>(config)#feature rsyslog</code>	Enable syslog feature on default or management VRF. By default this feature runs on the management VRF.
<code>(config)#logging level ospf 7</code>	This enable debug messages for OSPF module. This is configurable either if default of management VRF.

```
(config)#logging logfile ospf1 7
```

This creates the log file where the logs will be saved. The path of the file will be in the directory /log/ospf1. Log File size 4096-4194304 bytes.

```
(config)#exit
```

Exit configure mode

To verify this, do some OSPF configuration and view the messages in the log file or with the show logging logfile command.

## Validation Commands

```
#show logging logfile
```

```
File logging : enabled File Name : /log/ospf1 Size : 419430400 Severity : (7)
```

```
2019 Jan 05 20:10:52.202 : OcNOS : OSPF : INFO : NSM Message Header
2019 Jan 05 20:10:52.202 : OcNOS : OSPF : INFO : VR ID: 0
2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO : VRF ID: 0
2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO : Message type:
NSM_MSG_LINK_ADD
(5)
2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO : Message length: 232
2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO : Message ID: 0x00000000
2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO : NSM Interface
2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO : Interface index: 100001
2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO : Name: po1
2019 Jan 05 20:10:52.204 : OcNOS : OSPF : INFO : Flags: 536875010
2019 Jan 05 20:10:52.204 : OcNOS : OSPF : INFO : Status: 0x00000804
2019 Jan 05 20:10:52.204 : OcNOS : OSPF : INFO : Metric: 1
2019 Jan 05 20:10:52.207 : OcNOS : OSPF : INFO : MTU: 1500
2019 Jan 05 20:10:52.207 : OcNOS : OSPF : INFO : Type: L3
2019 Jan 05 20:10:52.207 : OcNOS : OSPF : INFO : HW type: 9
2019 Jan 05 20:10:52.208 : OcNOS : OSPF : INFO : HW len: 6
2019 Jan 05 20:10:52.209 : OcNOS : OSPF : INFO : HW address: ecf4.bb5c.a2b0
2019 Jan 05 20:10:52.210 : OcNOS : OSPF : INFO : Bandwidth: 0.000000
2019 Jan 05 20:10:52.211 : OcNOS : OSPF : INFO : Interface lacp key flag 0
2019 Jan 05 20:10:52.212 : OcNOS : OSPF : INFO : Interface lacp aggregator
upda
te flag 0
```

```
#show logging level
```

Facility	Default	Severity	Current	Session	Severity
nsm		3		3	
ripd		3		3	
ospfd		3		7	
ospf6d		3		3	
isisd		3		3	
hostpd		3		3	
ldpd		2		2	
rsvpd		2		2	
mribd		2		2	
pimd		2		2	
authd		2		2	
mstpd		2		2	
imi		2		2	
onmd		2		2	

---

oamd	2	2
vlogd	2	2
vrrpd	2	2
ribd	2	2
bgpd	3	3
l2mribd	2	2
lagd	2	2
sflow	2	2
pservd	2	2

---

## Logging to the Console

#configure terminal	Enter configure mode.
(config)#logging level ospf 7	This enable debug messages for OSPF module.
(config)#logging console 7	This enables the console logs.
(config)#debug ospf	This enables the debugging on OSPF configurations.
(config)#router ospf	Enabling ospf for process 1.
(config-router)#exit	Exit router mode.
(config)#exit	Exit configure mode.

To verify this, do some OSPF configuration and view the messages in the console.

---

## Validation Commands

```
#show logging console
      Console logging      : enabled Severity: (debugging)
```

```
#show logging level
```

Facility	Default	Severity	Current Session Severity
nsm		3	3
ripd		3	3
ospfd		3	7
ospf6d		3	3
isisd		3	3
hostpd		3	3
ldpd		2	2
rsvpd		2	2
mribd		2	2
pimd		2	2
authd		2	2
mstpd		2	2
imi		2	2
onmd		2	2
oamd		2	2
vlogd		2	2
vrrpd		2	2
ribd		2	2
bgpd		3	3
l2mribd		2	2
lagd		2	2

sflow	2	2
pservd	2	2

## Logging to Remote Server

#configure terminal	Enter configure mode.
(config)#logging level bgp 7	This enable debug messages for BGP module.
(config)#logging remote server 10.16.2.1 vrf management	Redirects the log messages to the remote server configured.
(config)#debug bgp	This enables the debugging on BGP configurations.
(config)#router bgp 1	Enabling BGP process 1.
(config-router)#exit	Exit router mode.
(config)#exit	Exit configure mode.

## Validation Commands

```
#show logging server
  Remote Servers:
    10.16.2.1
    severity: (debugging)
    facility: local7
    VRF: management
```

```
#show logging level
```

Facility	Default	Severity	Current	Session	Severity
nsm		3		3	
ripd		3		3	
ospfd		3		3	
ospf6d		3		3	
isisd		3		3	
hostpd		3		3	
ldpd		2		2	
rsvpd		2		2	
mribd		2		2	
pimd		2		2	
authd		2		2	
mstpd		2		2	
imi		2		2	
onmd		2		2	
oamd		2		2	
vlogd		2		2	
vrrpd		2		2	
ribd		2		2	
bgpd		3		7	
l2mribd		2		2	
lagd		2		2	
sflow		2		2	
pservd		2		2	

## Configuration

Note: The configuration to support multiple logging servers is listed below. Maximum 4 remote syslog server is supported.

#configure terminal	Enter Configure mode.
(config)#hostname OcNOS	Configuring the hostname of the device
(config)#feature rsyslog vrf management	Enable feature on default or management VRF. By default this feature runs on the management VRF.
(config)#logging level all 7	Enables debug messages for all modules.
(config)# logging remote server 10.12.17.10 5 vrf management	Redirects the log messages to the server configured. (Configuring 1 logging server).Configuring with log severity level as 5.By default severity level 7 is considered if no specific levels configured.
(config)# logging remote server 10.12.17.16 5 vrf management	Redirects the log messages to the server configured. (Configuring 2 logging server). Configuring with log severity level as 5. By default severity level 7 is considered if no specific levels configured.
(config)# logging remote server 10.12.17.11 7 vrf management	Redirects the log messages to the server configured. (Configuring 3 logging server). Configuring with log severity level as 7. By default severity level 7 is considered if no specific levels configured.
(config)# logging remote server 10.12.28.22 7 vrf management	Redirects the log messages to the server configured. (Configuring 4 logging server). Configuring with log severity level as 7. By default severity level 7 is considered if no specific levels configured.
(config)#exit	Exit configure mode.

## Validation Commands

```
OcNOS # show running-config logging
<snippet of show running-config logging output ...>
feature rsyslog vrf management
logging remote server 10.12.17.10 5 vrf management
logging remote server 10.12.17.16 5 vrf management
logging remote server 10.12.17.11 7 vrf management
logging remote server 10.12.28.22 7 vrf management
```

```
OcNOS # show logging server
Remote Servers:
    10.12.17.10
    severity: Operator (informational)
    facility: local7
    VRF : management
    10.12.17.16
    severity: Operator (informational)
    facility: local7
    VRF : management
    10.12.17.11
    severity: Operator (debug-detailed)
```

```
facility: local7
VRF : management
10.12.28.22
severity: Operator (debug-detailed)
facility: local7
VRF : management
```

---

## Remote machine Syslog Configuration:

Provided below are the changes required for rsyslog configuration on a debian system. Please refer to respective operating system official sites for more information

```
cat /etc/rsyslog.conf
$ModLoad imuxsock.so      # provides support for local system logging (e.g. via
logger command)
$ModLoad imklog.so        # provides kernel logging support (previously done by
rklogd)
$ModLoad immark.so        # provides --MARK-- message capability
$ModLoad imudp.so
$UDPServerRun 514
$ModLoad imtcp.so
$InputTCPServerRun 514
# Logs will be placed in separate folders based on hostnames and process
modules in the provided path
$template RemoteLogs, "/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~

$template precise, "%msg%\n"
*.* /var/log/messages
auth,authpriv.*           /var/log/auth.log
```

Save the changes and restart the rsyslog services to bring the changes in effect.

---

## Monitoring Logging Server:

Provided below are the sample outputs collected from one of the remote logging server.

```
root@localhost:~# cd /var/log/
```

Different folders I get created based on hostnames in the defined location in rsyslog.conf

```
root@localhost:/var/log# ls -lt
drwx----- 2 root      root      4096 Nov 18 03:02 Leaf1
drwx----- 2 root      root      4096 Nov 15 07:24 10.12.56.112-leaf5
drwx----- 2 root      root      4096 Nov 15 05:40 10.12.56.109-leaf2
drwx----- 2 root      root      4096 Nov 15 01:26 Bingol
drwx----- 2 root      root      4096 Nov 14 06:07 Leaf2
drwx----- 2 root      root      4096 Nov 11 04:57 R1-LEAF1
drwx----- 2 root      root      4096 Nov  8 06:46 leaf2
drwx----- 2 root      root      4096 Nov  8 03:38 R7-LEAF4
drwx----- 2 root      root      4096 Nov  8 01:30 LEAF1
drwx----- 2 root      root      4096 Nov  8 01:18 leaf3
drwx----- 2 root      root      4096 Nov  7 07:56 OcNOS
drwx----- 2 root      root      4096 Nov  6 23:58 mgmt-sw-3k
drwx----- 2 root      root      4096 Nov  4 21:51 R5-LEAF3
```

Check under OcNOS folder

```
root@localhost:/var/log/OcNOS# ls -ltr
```

**Different log files get created based on process name under folder based on hostname.**

```
-rw-r--r-- 1 root root      444 Oct 25 02:20 PSERV.log
-rw-r--r-- 1 root root      328 Oct 30 05:05 ONMD.log
-rw-r--r-- 1 root root      174 Oct 30 05:37 usermod.log
-rw-r--r-- 1 root root      498 Oct 30 07:55 SFLOW.log
-rw-r--r-- 1 root root      486 Oct 30 07:55 RIP.log
-rw-r--r-- 1 root root      486 Oct 30 07:55 LAG.log
-rw-r--r-- 1 root root      492 Oct 30 07:55 VRRP.log
-rw-r--r-- 1 root root      486 Oct 30 07:55 PIM.log
-rw-r--r-- 1 root root      504 Oct 30 07:55 OSPFv3.log
-rw-r--r-- 1 root root      492 Oct 30 07:55 OSPF.log
-rw-r--r-- 1 root root      498 Oct 30 07:55 IS-IS.log
-rw-r--r-- 1 root root      504 Oct 30 07:55 802.1X.log
-rw-r--r-- 1 root root      492 Oct 30 07:56 MSTP.log
-rw-r--r-- 1 root root      483 Oct 30 07:56 HSL.log
-rw-r--r-- 1 root root      486 Oct 30 07:56 RIB.log
-rw-r--r-- 1 root root      492 Oct 30 07:56 MRIB.log
-rw-r--r-- 1 root root     8709 Nov  2 11:22 OAM.log
-rw-r--r-- 1 root root    17959 Nov  2 11:23 NSM.log
-rw-r--r-- 1 root root   12178 Nov  2 11:23 BGP.log
-rw-r--r-- 1 root root   74488 Nov  3 07:41 CMM.log
-rw-r--r-- 1 root root     4128 Nov  3 08:17 login.log
-rw-r--r-- 1 root root     5265 Nov  3 08:17 HOSTP.log
-rw-r--r-- 1 root root    21982 Nov  3 08:17 CML.log
-rw-r--r-- 1 root root 28094411 Nov  3 08:17 CMLSH.log
-rw-r--r-- 1 root root   278619 Nov  3 08:19 sshd.log
-rw-r--r-- 1 root root   695277 Nov  3 08:20 CRON.log
```





---

## CHAPTER 24 Custom Syslog Port Configuration

---

---

### Overview

OcNOS enables the establishment of a Syslog server by designating the logging server as XX.XX.XX.XXX. This configuration sends syslog messages via the default port, which is 514. However, utilizing the default port for the Syslog server is considered a security vulnerability.

---

### Support for In-band management over default VRF

OcNOS supports syslog over the default and management VRFs via in-band management interface and OOB management interface, respectively.

By default, syslog runs on the management VRF.

---

### Features

- CLI is supported for user to configure custom syslog port.
- Once configured syslog conf file is updated with the configured port value.
- At the rsyslog server side, stop the running rsyslogd daemon using the command `systemctl stop rsyslog.service`
- Update `/etc/rsyslog.conf` file with syslog client configured port.
- Start the rsyslog daemon –using `systemctl start rsyslog.service`.
- Logs will redirect to syslog server through configured port.
- After un-configuring, the port logs will be sent to syslog remote server through default port 514, to receive the logs at server side, it also needs to be set back to default.
- Delete the custom Syslog port.

---

### Custom Syslog Configuration with IPv4 Address

Logging is performed with IPv4 address and verified by logs on remote machine.

## Topology



Figure 24-38: Syslog sample topology

## Enabling rsyslog

#configure terminal	Enter configure mode.
(config)#feature rsyslog [vrf management]	Enable feature on default or management VRF. By default this feature runs on the management VRF.
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode
(config)# logging remote server 10.12.33.211 7 port 8514 vrf management	Redirect into the remote server configure the severity and custom port with vrf management (default custom port is 514).
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode

## Validation

```
#sh running-config logging
feature rsyslog vrf management
logging remote server 10.12.33.211 7 port 8514 vrf management

ocnos#show logging server
  Remote Servers:
    10.12.33.211
    port: 8514
    severity: Operator (debug-detailed)
    facility: local7
    VRF : management
```

Check the rsyslog messages in server at /var/log/OcNOS.log

---

```
2023-08-25T12:36:56+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:36:56.982 : OcNOS : PSERV :  
DEBUG : Keep-Alive message sent to systemd  
2023-08-25T12:37:03+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:03.610 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:13+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:13.610 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:23+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:23.610 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:33+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:33.610 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:43+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:43.611 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:49+05:30 OcNOS sshd[11651]: Accepted password for ocnos from  
192.168.230.131 port 57298 ssh2  
2023-08-25T12:37:49+05:30 OcNOS sshd[11651]: pam_unix(sshd:session): session opened for  
user ocnos by (uid=0)  
2023-08-25T12:37:50+05:30 OcNOS sshd[11660]: Accepted password for ocnos from  
192.168.230.131 port 57301 ssh2  
2023-08-25T12:37:50+05:30 OcNOS sshd[11660]: pam_unix(sshd:session): session opened for  
user ocnos by (uid=0)  
2023-08-25T12:37:50+05:30 OcNOS CML[4875]: 2023 Aug 25 12:37:50.359 : OcNOS : CML : INFO  
: [CML_5]: Client [cmlsh (/dev/pts/0)] established connection with CML server  
2023-08-25T12:37:51+05:30 OcNOS CMLSH[11672]: 2023 Aug 25 12:37:51.214 : OcNOS : CMLSH :  
CLI_HIST : User ocnos@/dev/pts/0 : CLI : terminal monitor  
2023-08-25T12:37:53+05:30 OcNOS CMLSH[11672]: 2023 Aug 25 12:37:53.330 : OcNOS : CMLSH :  
CLI_HIST : User ocnos@/dev/pts/0 : CLI : en *New User Login*  
2023-08-25T12:37:53+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:53.611 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:55+05:30 OcNOS CMLSH[11672]: 2023 Aug 25 12:37:55.570 : OcNOS : CMLSH :  
CLI_HIST : User ocnos@/dev/pts/0 : CLI : start-shell  
2023-08-25T12:37:56+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:37:56.983 : OcNOS : PSERV :  
DEBUG : Keep-Alive message sent to systemd  
2023-08-25T12:37:58+05:30 OcNOS su: (to root) ocnos on pts/0  
2023-08-25T12:37:58+05:30 OcNOS su: pam_unix(su-l:session): session opened for user  
root by ocnos(uid=1000)  
2023-08-25T12:38:03+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:38:03.611 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:38:13+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:38:13.611 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:38:17+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:17.201 : OcNOS : PSERV :  
CRITI : Module: ospfd has closed connection with PSERVD.  
2023-08-25T12:38:17+05:30 OcNOS CML[4875]: 2023 Aug 25 12:38:17.204 : OcNOS : CML :  
CRITI : Module ospf disconnected with CML  
2023-08-25T12:38:18+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:18.229 : OcNOS : PSERV :  
INFO : Protocol pservd published protocol-module-down notification.  
2023-08-25T12:38:18+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:18.241 : OcNOS : PSERV :  
DEBUG : pserv SIGUER2 signal for module :ospfd  
2023-08-25T12:38:18+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:18.242 : OcNOS : PSERV :  
DEBUG : Crash Dump Directory not present  
2023-08-25T12:38:20+05:30 OcNOS NSM[4639]: 2023 Aug 25 12:38:20.110 : OcNOS : NSM :  
DEBUG : G8031 : nsm_g8031_sync : Sync PG info to ONMD  
2023-08-25T12:38:20+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:20.116 : OcNOS : PSERV :  
NOTIF : [WATCHDOG_PM_RECOVERED_4]: The module ospfd recovered from a critical error  
2023-08-25T12:38:20+05:30 OcNOS PSERV[1595]: Signal SIGUSR2 received and restarted  
module: ospfd  
  
2019 Jan 05 20:10:52.212 : OcNOS : OSPF : INFO : Interface lacp aggregator update flag 0
```

---

# Custom Syslog Configuration with IPv6 Address

Logging is performed with IPv6 IP and verified by logs on remote PC (Logging server).

## Topology

Figure 24-39 shows the sample configuration of Syslog.



Figure 24-39: Syslog Configuration topology

## Enabling rsyslog

#configure terminal	Enter configure mode
(config)#feature rsyslog [vrf management]	Enable feature on default or management VRF. By default this feature runs on the management VRF.
(config)#commit	Commit the candidate configuration to the running configuration
(config)#logging remote server 200:201::100:10 7 port 8514 vrf management	Redirect into the remote server configure the severity and custom port with vrf management (default custom port is 514).
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode

## Validation

```
ocnos#sh running-config logging
feature rsyslog vrf management
logging remote server 200:201::100:10 7 port 8514 vrf management

#show logging server
Remote Servers:
    200:201::100:10
    port: 8514
    severity: Operator (debug-detailed)
    facility: local7
    VRF : management
```

Check the rsyslog messages in server at /var/log/OcNOS.log

```
2023-08-25T12:36:56+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:36:56.982 : OcNOS : PSERV :  
DEBUG : Keep-Alive message sent to systemd  
2023-08-25T12:37:03+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:03.610 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:13+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:13.610 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:23+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:23.610 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:33+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:33.610 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:43+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:43.611 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:49+05:30 OcNOS sshd[11651]: Accepted password for ocnos from  
192.168.230.131 port 57298 ssh2  
2023-08-25T12:37:49+05:30 OcNOS sshd[11651]: pam_unix(sshd:session): session opened for  
user ocnos by (uid=0)  
2023-08-25T12:37:50+05:30 OcNOS sshd[11660]: Accepted password for ocnos from  
192.168.230.131 port 57301 ssh2  
2023-08-25T12:37:50+05:30 OcNOS sshd[11660]: pam_unix(sshd:session): session opened for  
user ocnos by (uid=0)  
2023-08-25T12:37:50+05:30 OcNOS CML[4875]: 2023 Aug 25 12:37:50.359 : OcNOS : CML : INFO  
: [CML_5]: Client [cmlsh (/dev/pts/0)] established connection with CML server  
2023-08-25T12:37:51+05:30 OcNOS CMLSH[11672]: 2023 Aug 25 12:37:51.214 : OcNOS : CMLSH :  
CLI_HIST : User ocnos@/dev/pts/0 : CLI : terminal monitor  
2023-08-25T12:37:53+05:30 OcNOS CMLSH[11672]: 2023 Aug 25 12:37:53.330 : OcNOS : CMLSH :  
CLI_HIST : User ocnos@/dev/pts/0 : CLI : en *New User Login*  
2023-08-25T12:37:53+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:53.611 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:37:55+05:30 OcNOS CMLSH[11672]: 2023 Aug 25 12:37:55.570 : OcNOS : CMLSH :  
CLI_HIST : User ocnos@/dev/pts/0 : CLI : start-shell  
2023-08-25T12:37:56+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:37:56.983 : OcNOS : PSERV :  
DEBUG : Keep-Alive message sent to systemd  
2023-08-25T12:37:58+05:30 OcNOS su: (to root) ocnos on pts/0  
2023-08-25T12:37:58+05:30 OcNOS su: pam_unix(su-l:session): session opened for user  
root by ocnos(uid=1000)  
2023-08-25T12:38:03+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:38:03.611 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:38:13+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:38:13.611 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:38:17+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:17.201 : OcNOS : PSERV :  
CRITI : Module: ospfd has closed connection with PSERVD.  
2023-08-25T12:38:17+05:30 OcNOS CML[4875]: 2023 Aug 25 12:38:17.204 : OcNOS : CML :  
CRITI : Module ospf disconnected with CML  
2023-08-25T12:38:18+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:18.229 : OcNOS : PSERV :  
INFO : Protocol pservd published protocol-module-down notification.  
2023-08-25T12:38:18+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:18.241 : OcNOS : PSERV :  
DEBUG : pserv SIGUER2 signal for module :ospfd  
2023-08-25T12:38:18+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:18.242 : OcNOS : PSERV :  
DEBUG : Crash Dump Directory not present  
2023-08-25T12:38:20+05:30 OcNOS NSM[4639]: 2023 Aug 25 12:38:20.110 : OcNOS : NSM :  
DEBUG : G8031 : nsm_g8031_sync : Sync PG info to ONMD  
2023-08-25T12:38:20+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:20.116 : OcNOS : PSERV :  
NOTIF : [WATCHDOG_PM_RECOVERED_4]: The module ospfd recovered from a critical error
```

2023-08-25T12:38:20+05:30 OcNOS PSERV[1595]: Signal SIGUSR2 received and restarted module: ospfd  
2019 Jan 05 20:10:52.212 : OcNOS : OSPF : INFO : Interface lacp aggregator update flag 0

## Custom Syslog Configuration with HOSTNAME

Logging is performed with IPv6 IP and verified by logs on remote PC (Logging server).

### Topology

Figure 24-40 shows the sample configuration of Syslog.



Figure 24-40: Syslog Configuration topology

### Enabling rsyslog

#configure terminal	Enter configure mode
(config)#feature rsyslog [vrf management]	Enable feature on default or management VRF. By default this feature runs on the management VRF.
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode
(config)#hostname CUSTOM-SYSLOG	Change the hostname to custom-syslog
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode
(config)#logging remote server custom-syslog 7 port 8514 vrf management	Redirect into the remote server configure the severity and custom port with vrf management (default custom port is 514).
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode

### Validation

```
ocnos#sh running-config logging
CUSTOM-SYSLOG#sh ru logging
feature rsyslog vrf management
```

```
logging remote server custom-syslog 7 port 8514 vrf management
CUSTOM-SYSLOG#
```

```
#show logging server
```

```
Remote Servers:
    custom-syslog
    port: 8514
    severity: Operator (debug-detailed)
    facility: local7
    VRF : management
```

Check the rsyslog messages in server

Server Path:- /var/log/OcNOS.log

---

## Sample Output

```
2023-08-25T12:36:56+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:36:56.982 : OcNOS : PSERV :
DEBUG : Keep-Alive message sent to systemd
2023-08-25T12:37:03+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:03.610 : OcNOS : HSL :
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)
2023-08-25T12:37:13+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:13.610 : OcNOS : HSL :
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)
2023-08-25T12:37:23+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:23.610 : OcNOS : HSL :
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)
2023-08-25T12:37:33+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:33.610 : OcNOS : HSL :
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)
2023-08-25T12:37:43+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:43.611 : OcNOS : HSL :
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)
2023-08-25T12:37:49+05:30 OcNOS sshd[11651]: Accepted password for ocnos from
192.168.230.131 port 57298 ssh2
2023-08-25T12:37:49+05:30 OcNOS sshd[11651]: pam_unix(sshd:session): session opened for
user ocnos by (uid=0)
2023-08-25T12:37:50+05:30 OcNOS sshd[11660]: Accepted password for ocnos from
192.168.230.131 port 57301 ssh2
2023-08-25T12:37:50+05:30 OcNOS sshd[11660]: pam_unix(sshd:session): session opened for
user ocnos by (uid=0)
2023-08-25T12:37:50+05:30 OcNOS CML[4875]: 2023 Aug 25 12:37:50.359 : OcNOS : CML : INFO
: [CML_5]: Client [cmlsh (/dev/pts/0)] established connection with CML server
2023-08-25T12:37:51+05:30 OcNOS CMLSH[11672]: 2023 Aug 25 12:37:51.214 : OcNOS : CMLSH :
CLI_HIST : User ocnos@/dev/pts/0 : CLI : terminal monitor
2023-08-25T12:37:53+05:30 OcNOS CMLSH[11672]: 2023 Aug 25 12:37:53.330 : OcNOS : CMLSH :
CLI_HIST : User ocnos@/dev/pts/0 : CLI : en *New User Login*
2023-08-25T12:37:53+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:37:53.611 : OcNOS : HSL :
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)
2023-08-25T12:37:55+05:30 OcNOS CMLSH[11672]: 2023 Aug 25 12:37:55.570 : OcNOS : CMLSH :
CLI_HIST : User ocnos@/dev/pts/0 : CLI : start-shell
2023-08-25T12:37:56+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:37:56.983 : OcNOS : PSERV :
DEBUG : Keep-Alive message sent to systemd
2023-08-25T12:37:58+05:30 OcNOS su: (to root) ocnos on pts/0
2023-08-25T12:37:58+05:30 OcNOS su: pam_unix(su-l:session): session opened for user
root by ocnos(uid=1000)
```

```
2023-08-25T12:38:03+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:38:03.611 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:38:13+05:30 OcNOS HSL[4598]: 2023 Aug 25 12:38:13.611 : OcNOS : HSL :  
NOTIF : [IF_PKT_ERRORS_4]: Oversized packets received on ge14 (1 packets)  
2023-08-25T12:38:17+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:17.201 : OcNOS : PSERV :  
CRITI : Module: ospfd has closed connection with PSERVD.  
2023-08-25T12:38:17+05:30 OcNOS CML[4875]: 2023 Aug 25 12:38:17.204 : OcNOS : CML :  
CRITI : Module ospf disconnected with CML  
2023-08-25T12:38:18+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:18.229 : OcNOS : PSERV :  
INFO : Protocol pservd published protocol-module-down notification.  
2023-08-25T12:38:18+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:18.241 : OcNOS : PSERV :  
DEBUG : pserv SIGUER2 signal for module :ospfd  
2023-08-25T12:38:18+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:18.242 : OcNOS : PSERV :  
DEBUG : Crash Dump Directory not present  
2023-08-25T12:38:20+05:30 OcNOS NSM[4639]: 2023 Aug 25 12:38:20.110 : OcNOS : NSM :  
DEBUG : G8031 : nsm_g8031_sync : Sync PG info to ONMD  
2023-08-25T12:38:20+05:30 OcNOS PSERV[1595]: 2023 Aug 25 12:38:20.116 : OcNOS : PSERV :  
NOTIF : [WATCHDOG_PM_RECOVERED_4]: The module ospfd recovered from a critical error  
2023-08-25T12:38:20+05:30 OcNOS PSERV[1595]: Signal SIGUSR2 received and restarted  
module: ospfd  
2019 Jan 05 20:10:52.212 : OcNOS : OSPF : INFO : Interface lacp aggregator update flag 0
```



## CHAPTER 25 Telnet Configuration

### Overview

Telnet is a TCP/IP protocol used on the Internet and local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection. The Telnet program runs, connects it to a server on the network. A user can then enter commands through the Telnet program and they will be executed as if the user were entering them directly on the server console. Telnet enables users to control the server and communicate with other servers on the network. The default port number for Telnet protocol is 23. Telnet offers users the capability of running programs remotely and facilitates remote administration.

### Support for In-band Management Over Default VRF

OcNOS supports Telnet over the default and management VRFs via in-band management interface and OOB management interface, respectively.

By default, Telnet runs on the management VRF.

### Topology



Figure 25-41: Telnet topology

### Enable and Disable the Telnet Server

#configure terminal	Enter configure mode
(config)#no feature telnet vrf management	Disable Telnet feature
(config)#feature telnet vrf management	Enable Telnet feature
(config)#exit	Exit configure mode

### Configure the Telnet Server Port

#configure terminal	Enter configure mode
(config)#no feature telnet vrf management	Disable Telnet feature
(config)#telnet server port 6112 vrf management	Set Telnet port to 6112

## Telnet Configuration

---

<code>(config)#feature telnet vrf management</code>	Enable Telnet feature
<code>(config)#exit</code>	Exit configure mode

---

## Telnet Client Session

<code>#telnet 10.10.10.1 vrf management</code>	Log into remote machine using IPv4 address
--	--

---

## Validation Commands

```
#show telnet server
telnet server enabled port: 6112

#show running-config telnet server
feature telnet
```

# CHAPTER 26 TACACS Client Configuration

## Overview

Terminal Access Controller Access Control System (TACACS) is a remote authentication protocol that is used to communicate with an authentication server. With TACACS, a network device communicates to an authentication server to determine whether a particular user should be allowed access to the device. TACACS+ listens at port 49.

## TACACS Server Authentication

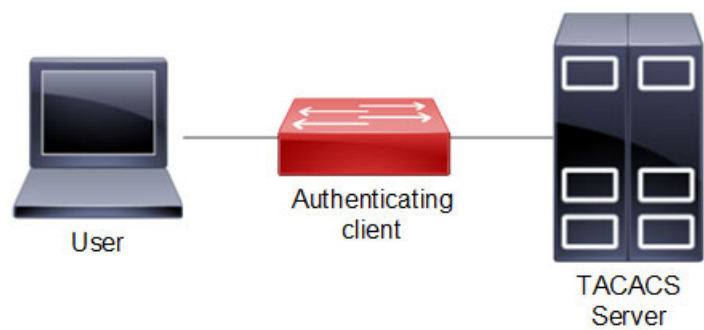


Figure 26-42: TACACS Server Host Configuration

TACACS+ Authentication determines whether a user should be granted access to the network or not. The primary purpose is to prevent intruders from entering into your networks. Authentication uses a database which comprises of user names and their passwords.

In OcNOS TACACS+ Client implementation, during authentication authorization-packet is sent prior to authentication-packet to ensure the requested user is present in the TACACS+ Server before actual authentication happens. In this case some TACACS+ Servers has to be explicitly configured to allow an unauthenticated user to perform authorization.

## Authenticating Device

#configure terminal	Enter configure mode.
(config)#feature tacacs+ vrf management	Enable the feature TACACS+ for management vrf
(config)#feature tacacs+	Enable the feature TACACS+. for default vrf
(config)#(config)#tacacs-server login key 0 testing101 vrf management	Specify the global key for tacacs servers that are not configured with their respective keys for management vrf This key should match the one present in the config file of tacacs server
(config)#tacacs-server login key 0 testing101	Specify the global key for tacacs servers that are not configured with their respective keys for default vrf This key should match the one present in the config file of tacacs server
(config)#tacacs-server login host 10.16.19.2 vrf management seq-num 1 key 0 testing123	Specify the tacacs server ipv4 address to be configured with shared key. The same key should be present on the server config file

## TACACS Client Configuration

(config)#tacacs-server login host 10.16.19.2 seq-num 2 key 0 testing123	Specify the tacacs server ipv4 address to be configured with shared local key for default vrf The same key should be present on the server config file.
(config)#tacacs-server login host 10.12.30.86 vrf management seq-num 4 port 1045	Specify the tacacs server ipv4 address to be configured with the sequence and port number.The tacacs server should be started with same port number
config)#tacacs-server login host 10.12.30.86 seq-num 2 port 1045	Specify the tacacs server ipv4 address to be configured with the sequence and port number for default vrf. The tacacs server should be started with same port number
(config)#tacacs-server login host 10.12.17.11 vrf management seq-num 8 key 7 65535 port 65535	Specify the tacacs server ipv4 address to be configured with the sequence, key and port number for management vrf. The tacacs server should be started with same port number.
(config)#tacacs-server login host 10.12.17.11 seq-num 8 key 7 65535 port 65535	Specify the tacacs server ipv4 address to be configured with the sequence, key and port number for default vrf. The tacacs server should be started with same port number.
(config)#tacacs-server login host Tacacs-Server-1 vrf management seq-num 7 key 7 65535 port 65535	Specify the tacacs server configured with host-name sequence number key and port number for management vrf. The tacacs server should be started with same port number
(config)#tacacs-server login host Tacacs-Server-1 seq-num 7 key 7 65535 port 65535	Specify the tacacs server configured with host-name sequence number key and port number for default vrf. The tacacs server should be started with same port number
(config)#aaa authentication login default vrf management group tacacs+	Enable authentication for TACACS+ server configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group tacacs+	Enable authentication for TACACS+ server configured for default vrf. Authorization is also enabled by default.
(config)#aaa authentication login default vrf management group tacacs+ local	Enable authentication for TACACS+ and fall-back to local configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group tacacs+ local none	Enable authentication for TACACS+ fall-back to local followed by fall-back to none configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group tacacs+ none	Enable authentication for TACACS+ fall-back to none configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group tacacs+ none	Enable authentication for TACACS+ fall-back to none , configured for default vrf. Authorization is also enabled by default
(config)#aaa group server tacacs+ G1 vrf management	Create aaa group G1 for management vrf
(config-tacacs)#server 10.12.30.86 vrf management	Make the tacacs-server 10.12.30.86 a part of this group G1 for default vrf
(config-tacacs)#server Tacacs-Server-1	Make the tacacs-server Tacacs-Server-1 a part of this group G1 for management vrf
(config-tacacs)#exit	Exit the tacacs-config
(config)#aaa group server tacacs+ G1	Create aaa group G1 for default vrf
(config-tacacs)server 10.12.30.86	Make the tacacs-server 10.12.30.86 a part of this group G1 for default vrf
(config-tacacs)#server Tacacs-Server-1	Make the tacacs-server Tacacs-Server-1 a part of this group G1 for management vrf
(config-tacacs)#exit	Exit the tacacs-config mode

(config)#aaa authentication login default vrf management group G1	Authenticate the tacacs+ group G1 with aaa authentication for management vrf
(config)#aaa authentication login default group G1	Authenticate the tacacs+ group G1 with aaa authentication for default vrf

Users are mapped as shown as shown in [Table 26-2](#):

**Table 26-2: Role/privilege level mapping**

Role	Privilege level
Network administrator	15
Network engineer	14
Network operator	1 to 13
Network user	0 or any other values (>15 or negative values or any character)

## Validation

```
Leaf1#show tacacs-server vrf management
VRF: management
total number of servers:4
```

```
Tacacs+ Server           : 10.16.19.2/49
  Sequence Number        : 1
  Failed Auth Attempts    : 0
  Success Auth Attempts   : 0
  Failed Connect Attempts : 0
  Last Successful authentication:
```

```
Tacacs+ Server           : 10.12.30.86/1045
  Sequence Number        : 2
  Failed Auth Attempts    : 0
  Success Auth Attempts   : 0
  Failed Connect Attempts : 0
  Last Successful authentication:
```

```
Tacacs+ Server           : Tacacs-Server-1/65535
  Sequence Number        : 7
  Failed Auth Attempts    : 0
  Success Auth Attempts   : 0
  Failed Connect Attempts : 0
  Last Successful authentication:
```

```
Tacacs+ Server           : 10.12.17.11/65535
  Sequence Number        : 8
  Failed Auth Attempts    : 0
  Success Auth Attempts   : 0
  Failed Connect Attempts : 0
  Last Successful authentication:
```

```
Leaf1#show tacacs-server
VRF: default
```

total number of servers:4

Tacacs+ Server : 10.16.19.2/49  
Sequence Number : 1  
Failed Auth Attempts : 0  
Success Auth Attempts : 0  
Failed Connect Attempts : 0  
Last Successful authentication:

Tacacs+ Server : 10.12.30.86/1045  
Sequence Number : 2  
Failed Auth Attempts : 0  
Success Auth Attempts : 0  
Failed Connect Attempts : 0  
Last Successful authentication:

Tacacs+ Server : Tacacs-Server-1/65535  
Sequence Number : 7  
Failed Auth Attempts : 0  
Success Auth Attempts : 0  
Failed Connect Attempts : 0  
Last Successful authentication:

Tacacs+ Server : 10.12.17.11/65535  
Sequence Number : 8  
Failed Auth Attempts : 0  
Success Auth Attempts : 0  
Failed Connect Attempts : 0  
Last Successful authentication:

(\*) indicates last active.

#show tacacs-server vrf all

VRF: management

total number of servers:2

Tacacs+ Server : Tacacs-Server-1/65535 (\*)  
Sequence Number : 7  
Failed Auth Attempts : 0  
Success Auth Attempts : 1  
Failed Connect Attempts : 0  
Last Successful authentication: 2018 October 30, 10:10:22

Tacacs+ Server : 10.12.17.11/65535  
Sequence Number : 8  
Failed Auth Attempts : 0  
Success Auth Attempts : 0  
Failed Connect Attempts : 0  
Last Successful authentication:

VRF: default

total number of servers:2

Tacacs+ Server : Tacacs-Server-1/2222  
Sequence Number : 7  
Failed Auth Attempts : 0  
Success Auth Attempts : 0

---

```
Failed Connect Attempts      : 0
Last Successful authentication:
```

```
Tacacs+ Server               : 100.0.0.1/2222
    Sequence Number          : 8
    Failed Auth Attempts     : 0
    Success Auth Attempts    : 0
    Failed Connect Attempts  : 0
Last Successful authentication:
```

```
(*) indicates last active.
```

```
#
```

```
#
```

```
#show tacacs-server
```

```
    VRF: default
total number of servers:2
```

```
Tacacs+ Server               : Tacacs-Server-1/2222
    Sequence Number          : 7
    Failed Auth Attempts     : 0
    Success Auth Attempts    : 0
    Failed Connect Attempts  : 0
Last Successful authentication:
```

```
Tacacs+ Server               : 100.0.0.1/2222
    Sequence Number          : 8
    Failed Auth Attempts     : 0
    Success Auth Attempts    : 0
    Failed Connect Attempts  : 0
Last Successful authentication:
```

```
(*) indicates last active.
```

```
#show tacacs-server vrf management groups G1
```

```
    VRF: management
```

```
group G1:
    server Tacacs-Server-1:
        seq-num 7
        port is 65535
        key is *****

    server 10.12.17.11:
        seq-num 8
        port is 65535
        key is *****
```

```
#show tacacs-server vrf all groups G1
```

```
    VRF: management
```

```
group G1:
    server Tacacs-Server-1:
        seq-num 7
```

```
port is 65535
key is *****
```

```
server 10.12.17.11:
seq-num 8
port is 65535
key is *****
```

```
VRF: default
```

```
group G1:
server Tacacs-Server-1:
seq-num 7
port is 2222
key is *****

server 100.0.0.1:
seq-num 8
port is 2222
key is *****
```

```
#
#show tacacs-server groups G1
VRF: default
group G1:
server Tacacs-Server-1:
seq-num 7
port is 2222
key is *****

server 100.0.0.1:
seq-num 8
port is 2222
key is *****
```

```
#show tacacs vrf management
VRF: management
total number of servers:2
```

```
Tacacs+ Server          : Tacacs-Server-1/65535 (*)
  Sequence Number       : 7
  Failed Auth Attempts   : 0
  Success Auth Attempts  : 1
  Failed Connect Attempts : 0
  Last Successful authentication: 2018 October 30, 10:10:22
```

```
Tacacs+ Server          : 10.12.17.11/65535
  Sequence Number       : 8
  Failed Auth Attempts   : 0
  Success Auth Attempts  : 0
  Failed Connect Attempts : 0
  Last Successful authentication:
```

(\*) indicates last active.



```
#show tacacs vrf all
    VRF: management
total number of servers:2

Tacacs+ Server      : Tacacs-Server-1/65535 (*)
    Sequence Number : 7
    Failed Auth Attempts : 0
    Success Auth Attempts : 1
    Failed Connect Attempts : 0
    Last Successful authentication: 2018 October 30, 10:10:22

Tacacs+ Server      : 10.12.17.11/65535
    Sequence Number : 8
    Failed Auth Attempts : 0
    Success Auth Attempts : 0
    Failed Connect Attempts : 0
    Last Successful authentication:

    VRF: default
total number of servers:2

Tacacs+ Server      : Tacacs-Server-1/2222 (*)
    Sequence Number : 7
    Failed Auth Attempts : 0
    Success Auth Attempts : 1
    Failed Connect Attempts : 0
    Last Successful authentication: 2018 October 30, 10:32:52

Tacacs+ Server      : 100.0.0.1/2222
    Sequence Number : 8
    Failed Auth Attempts : 0
    Success Auth Attempts : 0
    Failed Connect Attempts : 0
    Last Successful authentication:

(*) indicates last active.
#

#show tacacs
    VRF: default
total number of servers:2

Tacacs+ Server      : Tacacs-Server-1/2222 (*)
    Sequence Number : 7
    Failed Auth Attempts : 0
    Success Auth Attempts : 1
    Failed Connect Attempts : 0
    Last Successful authentication: 2018 October 30, 10:32:52

Tacacs+ Server      : 100.0.0.1/2222
    Sequence Number : 8
    Failed Auth Attempts : 0
```

```
    Success Auth Attempts      : 0
    Failed Connect Attempts    : 0
    Last Successful authentication:
```

(\*) indicates last active.

```
#show tacacs vrf management
    VRF: management
total number of servers:2
```

```
Tacacs+ Server                : Tacacs-Server-1/65535 (*)
    Sequence Number            : 7
    Failed Auth Attempts        : 0
    Success Auth Attempts       : 1
    Failed Connect Attempts     : 0
    Last Successful authentication: 2018 October 30, 10:10:22
```

```
Tacacs+ Server                : 10.12.17.11/65535
    Sequence Number            : 8
    Failed Auth Attempts        : 0
    Success Auth Attempts       : 0
    Failed Connect Attempts     : 0
    Last Successful authentication:
```

(\*) indicates last active.

```
#show tacacs vrf all
    VRF: management
total number of servers:2
```

```
Tacacs+ Server                : Tacacs-Server-1/65535 (*)
    Sequence Number            : 7
    Failed Auth Attempts        : 0
    Success Auth Attempts       : 1
    Failed Connect Attempts     : 0
    Last Successful authentication: 2018 October 30, 10:10:22
```

```
Tacacs+ Server                : 10.12.17.11/65535
    Sequence Number            : 8
    Failed Auth Attempts        : 0
    Success Auth Attempts       : 0
    Failed Connect Attempts     : 0
    Last Successful authentication:
```

```
    VRF: default
total number of servers:2
```

```
Tacacs+ Server                : Tacacs-Server-1/2222 (*)
    Sequence Number            : 7
    Failed Auth Attempts        : 0
    Success Auth Attempts       : 1
    Failed Connect Attempts     : 0
    Last Successful authentication: 2018 October 30, 10:32:52
```

```
Tacacs+ Server                : 100.0.0.1/2222
    Sequence Number            : 8
```

---

```
Failed Auth Attempts      : 0
Success Auth Attempts     : 0
Failed Connect Attempts   : 0
Last Successful authentication:
```

```
(*) indicates last active.
```

```
#
```

```
#show tacacs
```

```
    VRF: default
total number of servers:2
```

```
Tacacs+ Server           : Tacacs-Server-1/2222(*)
    Sequence Number      : 7
    Failed Auth Attempts  : 0
    Success Auth Attempts : 1
    Failed Connect Attempts : 0
    Last Successful authentication: 2018 October 30, 10:32:52
```

```
Tacacs+ Server           : 100.0.0.1/2222
    Sequence Number      : 8
    Failed Auth Attempts  : 0
    Success Auth Attempts : 0
    Failed Connect Attempts : 0
    Last Successful authentication:
```

```
(*) indicates last active.
```

```
#show aaa authentication vrf management
```

```
    VRF: management
default: group G1
console: local
```

```
#show aaa authentication vrf all
```

```
    VRF: management
default: group G1
console: local
```

```
    VRF: default
default: group tacacs+
console: local
```

```
#show aaa authentication
```

```
    VRF: default
default: group tacacs+
console: local
```

```
#
```

```
# show aaa groups vrf management
```

```
    VRF: management
radius
tacacs+
G1
```

```
#
# show aaa groups vrf all
#           VRF: management
radius
tacacs+
G1

#           VRF: default
radius
tacacs+
G1

#show aaa groups
#           VRF: default
radius
tacacs+
G1

#show running-config tacacs+
feature tacacs+ vrf management
tacacs-server login host Tacacs-Server-1 vrf management seq-num 7 key 7 65535
po
rt 65535
tacacs-server login host 10.12.17.11 vrf management seq-num 8 key 7 65535 port
6
5535

feature tacacs+
tacacs-server login host Tacacs-Server-1 seq-num 7 key 7 65535 port 2222
tacacs-server login host 100.0.0.1 seq-num 8 key 7 65535 port 2222

#show running-config aaa
aaa authentication login default vrf management group G1
aaa group server tacacs+ G1 vrf management
server Tacacs-Server-1 vrf management
server 10.12.17.11 vrf management

aaa authentication login default group tacacs+
aaa group server tacacs+ G1
server Tacacs-Server-1
server 100.0.0.1

#show running-config aaa all
aaa authentication login default vrf management group G1
aaa authentication login console local
aaa accounting default vrf management local
no aaa authentication login default fallback error local vrf management
no aaa authentication login console fallback error local
no aaa authentication login error-enable vrf management
aaa local authentication attempts max-fail 3
aaa local authentication unlock-timeout 1200
aaa group server tacacs+ G1 vrf management
server Tacacs-Server-1 vrf management
server 10.12.17.11 vrf management
```

```
aaa authentication login default group tacacs+
aaa authentication login console local
aaa accounting default local
no aaa authentication login default fallback error local
no aaa authentication login console fallback error local
no aaa authentication login error-enable
aaa local authentication attempts max-fail 3
aaa local authentication unlock-timeout 1200
aaa group server tacacs+ G1
    server Tacacs-Server-1
    server 100.0.0.1
```

## TACACS Server Accounting

After authentication, the user can configure accounting to measure the resources that the user consumes during access.

### Authenticating Device

#configure terminal	Enter configure mode.
(config)#feature tacacs+ vrf management	Enable the feature TACACS+ for vrf management
(config)#feature tacacs+	Enable the feature TACACS+ for default vrf
(config)#tacacs-server login host 10.16.19.2 vrf management seq-num 1 key 0 testing123	Specify the TACACS server IPv4 address to be configured with shared key for vrf management. The same key should be present in the server configuration file.
(config)#tacacs-server login host 10.16.19.2 key testing123	Specify the TACACS server IPv4 address to be configured with shared key default vrf. The same key should be present in the server configuration file.
(config)#aaa accounting default vrf management group tacacs+	Enable accounting for TACACS server configured for vrf management.
(config)#aaa accounting default group tacacs+	Enable accounting for TACACS server configured for default vrf
(config)#exit	Exit configure mode
#clear tacacs-server counters vrf management	Clear tacacs server counters for management vrf
#clear tacacs-server counters vrf all	Clear tacacs server counters for management and default vrf
#clear tacacs-server counters	Clear tacacs server counters for default vrf

To verify the TACACS accounting process, connect using SSH or Telnet from the host to the client with the user created and provided TACACS server password, and check whether the client validates the user with corresponding username and password.

### Validation Commands

show tacacs-server, show aaa accounting, show aaa accounting

```
#show aaa accounting vrf management
                        VRF: management
                        default: group tacacs+
```

```
#

#show aaa accounting vrf all
    VRF: management
default: group tacacs+

    VRF: default
default: group tacacs+

#show aaa accounting
    VRF: default
default: group tacacs+
#

#show running-config aaa
aaa authentication login default vrf management group G1
aaa accounting default vrf management group tacacs+
aaa group server tacacs+ G1 vrf management
    server Tacacs-Server-1 vrf management
    server 10.12.17.11 vrf management

aaa authentication login default group tacacs+
aaa accounting default group tacacs+
aaa group server tacacs+ G1
    server Tacacs-Server-1
    server 100.0.0.1
```

### Sample TACACS Config File Contents

```
#tacacs configuration file
#set the key

key = "testing123"
accounting file = /var/log/tac_acc.log

user = test1 {
    default service = permit
    login = cleartext "12345"
}

group = netadmin {
    service = ppp protocol = ip {
        priv-lvl = 1
    }
}

user = test2 {
    default service = permit
    login = cleartext "12345"
    member = netadmin
}

user = test3 {
    default service = permit
    login = cleartext "12345"
    service = ppp protocol = ip {
```

```

        priv-lvl = 15
    }
}

```

---

## TACACS Server Authorization

Authorization is realized by mapping the authenticated users to one of the existing predefined roles as shown in [Table 26-2](#).

The privilege information from the TACACS+ server is retrieved for the authenticated users and is mapped onto one of the roles as shown in [Table 26-2](#).

Each authenticated user is mapped to one of the pre-defined privilege level.

Users with priv-level  $\leq 0$  and priv-level  $> 15$  are treated as read-only user mapped onto the pre-defined network-user role.

There is no command to enable authorization. Authorization functionality is enabled by default when remote authentication is enabled with TACACS+.

Authorization is "auto-enabled". After successful authentication, a user can enter into privilege exec mode, irrespective of its privilege level and such user is not prompted with enable mode password, if configured. However based on their role, commands are rejected if not allowed to perform certain operations.

---

## Example

A network-user has read-only access and can only execute show commands. A network-user cannot enter configuration mode. An error message is displayed upon executing any command which is not allowed.

```

#write
% Access restricted for user %
#configure terminal
% Access restricted for user %

```

The following attribute value pair in TACACS+ server is used to fetch user privilege information.

```

service = ppp protocol = ip {
    priv-lvl = <0...15>
}

```

---

## Sample TACACS+ Configuration File

```

#tacacs configuration file from "tac_plus version F4.0.3.alpha "
#set the key

key = "testing123"
accounting file = /var/log/tac_acc.log

#Read only user "test1", without any priv-lvl, mapped to role "network-user"
user = test1 {
    default service = permit
    login = cleartext "12345"
}

#We can create a group of users mapped to a privilege
group = netadmin {

```

```
service = ppp protocol = ip {
priv-lvl = 15
}
}

#User "test2" with highest priv-lvl=15, mapped to role "network-admin"
user = test2 {
default service = permit
login = cleartext "12345"
member = netadmin
}

#User "test3" with priv-lvl= 1...13, mapped to role "network-operator"
user = test3 {
default service = permit
login = cleartext "12345"
service = ppp protocol = ip {
priv-lvl = 10
}
}
#User "test4" with priv-lvl=14, mapped to role "network-engineer" user = test4 {
default service = permit
login = cleartext "12345"
service = ppp protocol = ip {
priv-lvl = 14
}
}
```



---

## CHAPTER 27 Traffic Mirroring Configuration

---

This chapter 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.

Note: 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.

Also, the mirrored packet would be having default TPID of the mirror destination port i.e. 0x8100.

---

### 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

## Topology

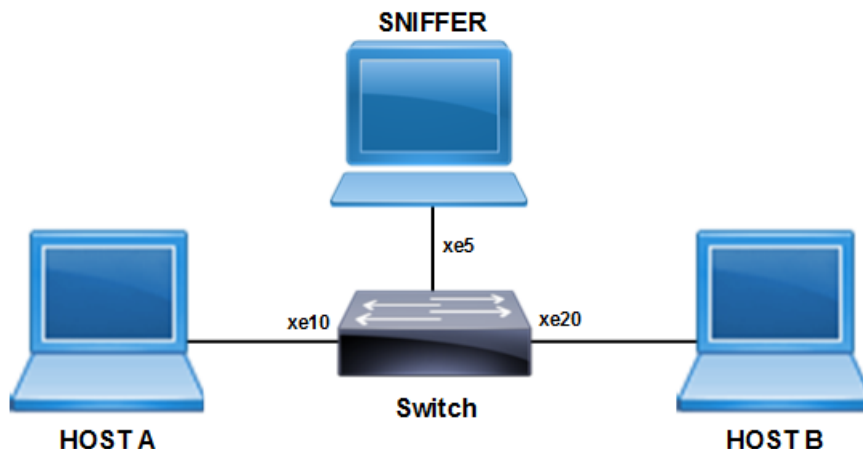


Figure 27-43: SPAN Topology

## 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.
(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.
(config)#interface xe20	Enter interface mode.

## Traffic Mirroring Configuration

(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

## 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.

## Topology

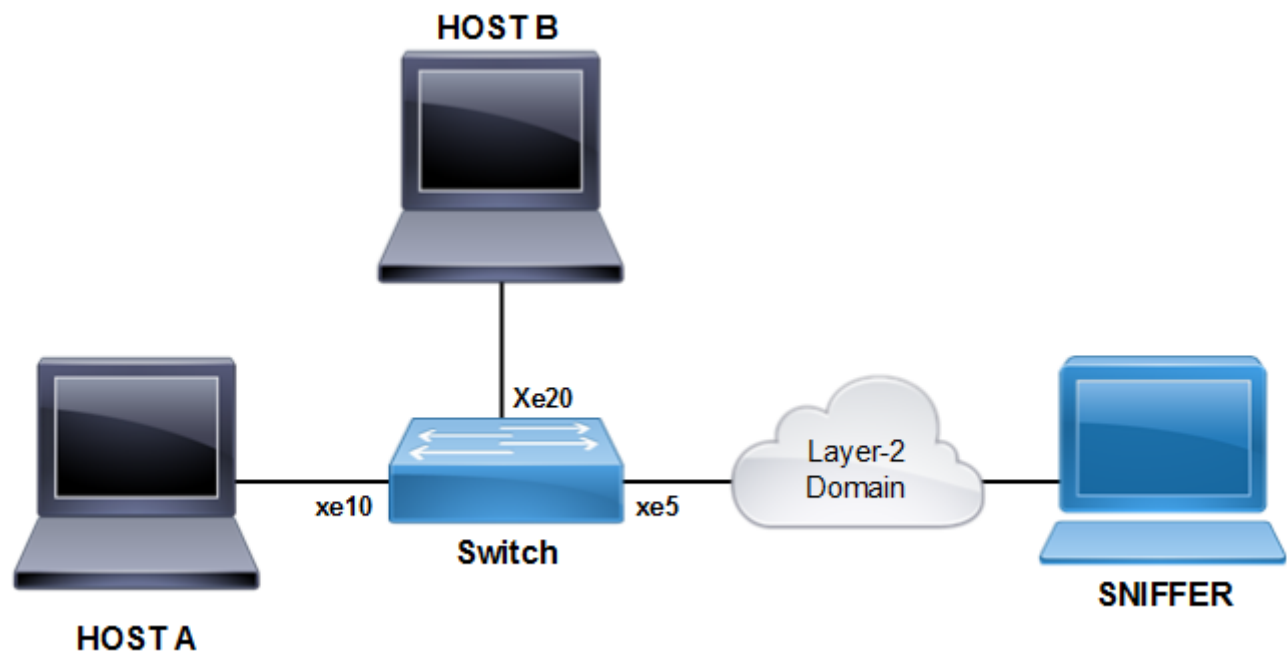


Figure 27-44: RSPAN Topology

## 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.
(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
```

## Traffic Mirroring Configuration

---

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
```

## Traffic Mirroring Configuration

---

```
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)
```

## CHAPTER 28 Trigger Failover Configuration

### Overview

This chapter contains Trigger Failover (TFO) configuration examples.

This example shows the complete configuration to enable TFO in a simple network topology. TFO complements NIC teaming functionality supported on blade servers. TFO allows a switch module to monitor specific uplink ports to detect link failures. When the switch module detects a link failure, it disables the corresponding downlink ports automatically.

TFO uses these components:

- A Fail Over Group (FOG) contains a Monitor Port Group (MPG) and a Control Port Group (CPG).
- An MPG contains only uplink ports.
- A CPG contains only downlink ports.

Note:

- TFO is supported in STP or RSTP bridge mode.
- TFO can be configured on a LAG interface.

### Basic Configuration

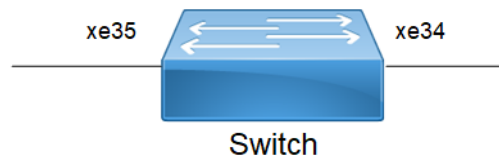


Figure 28-45: Basic topology

#### Switch

#configure terminal	Enter configure mode.
(config)#tfo enable	Enable TFO globally.
(config)#fog 1 enable	Create a Fail over group (FOG) and enable it.
(config)#interface xe35	Enter interface mode
(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#fog 1 type mpg	Specify the MPG member for FOG 1.
(config-if)#exit	Exit interface mode
(config)#interface xe34	Enter interface mode
(config-if)#link-type downlink	Specify the link-type as Downlink.
(config-if)#fog 1 type cpg	Specify the CPG member for FOG 1.
(config-if)#end	Exit interface and configure mode

Validation

```
#show tfo

TFO : Enable

Failover Group 1 : Enable
Failover Status : MPG Link Failure
No. of links to trigger failover : 0
MPG Port(s) :
xe35    Status : DOWN
CPG Port :
xe34    Status : DOWN
No. of times MPG link failure : 1
No. of times MPG link recovered : 0
No. of times CPG got auto disabled : 1
No. of times CPG got auto enable : 0
```

Port-Channel Configuration

Topology

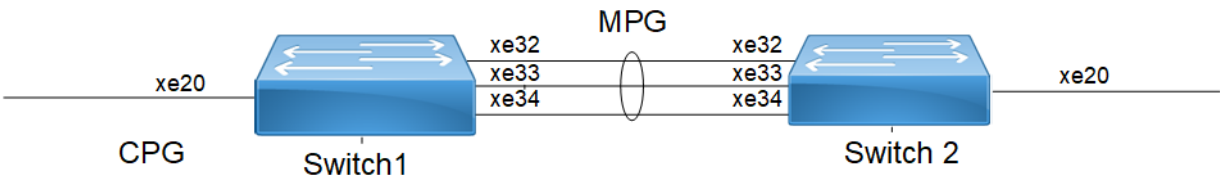


Figure 28-46: TFO with port-channel

Switch 1

#configure terminal	Enter configure mode.
(config)#tfo enable	Enable TFO globally.
(config)#fog 1 enable	Create a Fail over group (FOG) and enable it.
(config)#interface po1	Enter interface mode
(config-if)#switchport	Make the interface Layer2.
(config-if)#exit	Exit interface mode
(config)#interface xe32	Enter interface mode
(config-if)#switchport	Make the interface Layer2.
(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#interface xe33	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.

(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#interface xe34	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#interface xe20	Enter interface mode
(config-if)#link-type downlink	Specify the link-type as Downlink.
(config-if)#fog 1 type cpg	Specify the CPG member for FOG 1
(config-if)#exit	Exit interface mode
(config)#interface po1	Enter port-channel mode
(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#fog 1 type mpg	Specify the MPG member for FOG 1.
(config-if)#exit	Exit interface and configure mode

## Switch 2

(config)#interface po1	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#exit	Exit interface mode
(config)#interface xe32	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#interface xe33	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#interface xe34	Enter interface mode
(config-if)#switchport	Make the interface as Layer2
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode

## Validation

```
#show interface brief | include up
xe20      ETH    --    routed    up      none    1g     --      Br    Yes
xe32      ETH    --    routed    up      none    10g    --      Br    Yes
xe33      ETH    --    routed    up      none    10g    --      No    No
xe34      ETH    --    routed    up      none    10g    --      No    No
```

## Trigger Failover Configuration

---

```
eth0      METH                      up      --      1g
lo        up                        up      --
lo.management up                    up      --
```

```
#show tfo
```

```
TFO : Enable
```

```
Failover Group 1 : Enable
```

```
Failover Status : MPG Link Failure
```

```
No. of links to trigger failover : 0
```

```
MPG Port(s) :
```

```
po1      Status : DOWN
```

```
CPG Port :
```

```
xe20     Status : DOWN
```

```
No. of times MPG link failure : 0
```

```
No. of times MPG link recovered : 0
```

```
No. of times CPG got auto disabled : 0
```

```
No. of times CPG got auto enable : 0
```



## CHAPTER 29 User Configuration

### Overview

User management is an authentication feature that provides administrators with the ability to identify and control the users who log into the network.

OcNOS provides 4 different roles for users.

- Network Administrator: can make permanent changes to switch configuration. Changes are persistent across reset/reboot of switch.
- Network Engineer: can make permanent changes to switch configuration. Changes are persistent across reset/reboot of switch.
- Network Operator: can make permanent changes to switch configuration. Changes are not persistent across reset/reboot of switch.
- Network User: displays information; cannot modify configuration.

### User Configuration

#configure terminal	Enter configure mode.
(config)#username user1 password user12345	Create "user1" with password user12345 which will have default role as network-user.
(config)#username user1 role network-operator password user12345	Change the role for user1 to network-operator.
(config)#username user2 role network-operator password user12345	Create "user2" with role as network-operator.
(config)#username user3 role network-admin password user12345	Create "user3" with role as network-admin.
(config)#username user4 role network-engineer password user12345	Create "user4" with role as network-engineer.
(config)#exit	Exit configure mode.

### Validation Commands

```
show user-account, show user-account <username>, show role
#show user-account
User:user1
roles: network-operator
User:user2
roles: network-operator
User:user3
roles: network-admin
User:user4
roles: network-engineer
```

```
#show role
Role Name                               Info
-----
network-admin      Network Administrator - Have all permissions
network-engineer   Network Engineer - Can save configuration
network-operator   Network Operator - Can not save configuration
network-user       Network User - Can not change configuration
rbac-customized-role  RBAC User - Can change only permitted configuration

#show user-account user1
User:user1
           roles: network-operator
```

---

## CHAPTER 30 Using the Management Interface

---

---

### Overview

OcNOS provides support for different types of Management Interfaces. The management interface can be the standard out of band (OOB) port, or any in-band port.

To provide segregation between management traffic and data traffic, OcNOS provides a Management VRF. The Management VRF is created by default when OcNOS boots. This VRF cannot be deleted. All ports used as Management Interface needs to be in Management VRF. The management VRF is used for all types of Management applications listed below

- Remote access to router (SSH/Telnet)
- File transfer applications (SFTP/SCP)
- Login Authentication via Radius/Tacacs
- Network management protocols (SNMP, Netconf)

Apart from this, DHCP, DNS, NTP, Syslog, sFlow, and License/Software upgrade also uses ports mapped to management VRF for their operations. Also LLDP protocol can be run on any ports mapped to this Management VRF.

Note: If the management interface flaps, the device becomes unreachable.

---

### Management Port

The Out of Band (OOB) Management Port in OcNOS is identified as “eth0.” This port is automatically mapped to the Management VRF when OcNOS boots, and will remain in same VRF throughout. It cannot be moved out of this VRF.

The IP address of the management port can be configured statically or via DHCP.

---

### Static IP Configuration

A static IP can be configured on the management port during ONIE installation itself, or after installation using the OcNOS CLIs commands. To configure a static IP during ONIE installation, do the following

```
#onie-stop
#ifconfig eth0 <ip address> netmask <subnet mask> up
```

Please check the *Install Guide* for details.

The IP address configured during ONIE installation will be applied to the management port and the same will be retained when OcNOS boot up, and the port becomes part of Management VRF.

```
#show running-config interface eth0
!
interface eth0
 ip vrf forwarding management
 ip address 10.12.44.109/24
```

After getting the OcNOS prompt, this IP address can be changed from the CLI.

#configure terminal	Enter configure mode
(config)#interface eth0	Enter interface mode
(config-if)#ip address 10.12.44.120/24	Assign an IPv4 address to the interface
(config-if)#exit	Exit interface mode
(config)#exit	Exit configuration mode

If a static IP is not configured during ONIE installation the same can be configured via CLI by following the above steps. Using the OcNOS CLI, DHCP can also be enabled on the Management port.

#configure terminal	Enter configure mode
(config)#interface eth0	Enter interface mode
(config-if)#ip address dhcp	Enable DHCP on interface
(config-if)#exit	Exit interface mode
(config)#exit	Exit configuration mode

---

## Obtaining IP Address via DHCP

During onie installation, the management port attempts to acquire IP address via DHCP automatically unless stopped explicitly using "onie-stop". So, if management port is getting IP via DHCP, after OcNOS boots, the management port will continue to use DHCP, even when it is part of the Management VRF.

```
#show running-config interface eth0
!
interface eth0
 ip vrf forwarding management
 ip address dhcp
```

After OcNOS boots, the IP address can be changed to any static IP from the command line as shown earlier.

---

## In-Band Ports

Any front-end ports of the device (in-band ports) can be made part of the management VRF. Once they are part of the management VRF they can also support all management applications such as SSH/Telnet and others as listed in [Overview](#).

Once the ports are part of the management VRF, they should not be used for data traffic and routing or switching purposes. In-band ports can be added or removed from Management VRF as and when required.

#configure terminal	Enter configure mode
(config)#interface xel/1	Enter interface mode
(config-if)#ip vrf forwarding management	Add in-band port to Management VRF
(config-if)#exit	Exit interface mode
(config)#exit	Exit configuration mode

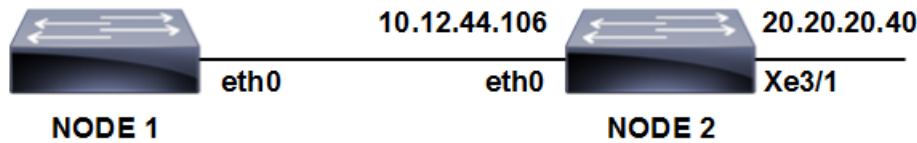
#configure terminal	Enter configure mode
(config)#interface xel/1	Enter interface mode

(config-if)# no ip vrf forwarding management	Remove in-band port from Management VRF
(config-if)#exit	Exit interface mode
(config)#exit	Exit configuration mode

## Using Ping in Management VRF

To check reachability to any node in the management network, you need to explicitly mention the VRF name as "management."

In the following example, Node-1 has management interface eth0 and Node-2 has management interfaces eth0 and xe3/1. In order to reach the network 20.20.20.40/24 from Node-1 a static route needs to be added.



#configure terminal	Enter configure mode
(config)# ip route vrf management 20.20.20.0/24 10.12.44.106 eth0	Add static route in management VRF to reach 20.20.20.0/24 network
(config)#exit	Exit configuration mode

```
Node-1#show ip route vrf management
```

Codes: K - kernel, C - connected, S - static, 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,

v - vrf leaked

\* - candidate default

```
IP Route Table for VRF "management"
```

```
C      10.12.44.0/24 is directly connected, eth0
```

```
S      20.20.20.0/24 [1/0] via 10.12.44.106, eth0
```

```
Gateway of last resort is not set
```

```
Node-1#ping 20.20.20.40 vrf management
```

```
PING 20.20.20.40 (20.20.20.40) 56(84) bytes of data.
```

```
64 bytes from 20.20.20.40: icmp_seq=1 ttl=64 time=0.494 ms
```

```
64 bytes from 20.20.20.40: icmp_seq=2 ttl=64 time=0.476 ms
```



## CHAPTER 31 Fault Management System Configuration

The Fault Management System (FMS) detects events, correlates them, and raises relevant alarms. The events are OPER\_LOGs relayed from the `vlogd` module. The alarms are a result of the correlation rules and provide a persistent indication of the faults. The alarms are maintained in a database and can be displayed via `show` commands.

Note:

- FMS relies on the loopback interface (`interface lo0`) for communication with VLOGd. Therefore, ensuring the operational status of the loopback interface is vital for the normal functioning of both the FMS and VLOGd modules.
- In OcNOS, FMS is disabled by default.
- After starting FMS, avoid editing the `alarm_def_config.yaml` file, as changes will only take effect after restarting FMS.
- Set the device's logging level to at least 4 (NOTIFY) to ensure timely delivery of notification events to FMS for appropriate actions. Adjusting the logging level below NOTIFY may cause FMS to miss clear events and fail to resolve active alarms.
- If FMS reboots due to a device reboot (upgrade/downgrade/reboot) or manual FMS reboots through disabling and enabling it, the device will close active alarms. Use the [show alarm closed](#) CLI command to view closed active alarms.

FMS applies the correlation procedures in [Table 31-3](#) based on the configurations specified.

**Table 31-3: FMS correlation procedures**

Correlation type	Description
Generalization	<ul style="list-style-type: none"><li>• Groups two or more events into a single alarm.</li><li>• A generalized alarm will further use one of the correlation types (none, time-bound, counting and compression) for applying correlation logic to the new alarm.</li></ul>
Time-bound	<ul style="list-style-type: none"><li>• Stipulates that when the event is received, a timer is started for that event.</li><li>• While the timer is running, subsequent events of the same type are suppressed.</li><li>• On the expiry of the timer, an alarm will be raised for that event stating the count for the number of times that event was received in this duration.</li></ul>
Counting	Considers a specified number of similar events as one. In this correlation type, the respective alarm will be raised after the event has occurred for count times.
Compression	Check multiple occurrences of the same event for duplicate/redundant event information, remove the redundancies, and report them as a single alarm.
Severity	Correlates events based on the severity of the events.

## Implementation

FMS was developed with NodeJS with scripts written in JavaScript with a \*.js extension and configuration files with a \*.yaml extension. These files are in the below paths in OcNOS.

Table 31-4: FMS script and configuration files

/usr/local/bin/js	JavaScript files (*.js files)
/usr/local/etc	Configuration files (*.yaml files)

## Enabling and Disabling the Fault Management System

Follow the below steps to enable or disable FMS:

### Enabling FMS

```
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#fault-management enable
(config)#
```

### Disabling FMS

```
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#fault-management disable
(config)#
```

## Alarm Configuration File

The alarm configuration file contains the configurations/rules for the alarms that will be referred by FMS to generate alarms upon receiving events. This file is in \*.yaml format (human readable) in /usr/local/etc.

This file can be edited before starting FMS to include correlation rules for specific events.

### Alarm Configuration File Template

```
#-----Template-----
#- Event_Group:
#   - ALARM_ID:                # Integer number identifying alarm
#   ALARM_TYPE_ID:            # Alarm Type-id(AIS, EQPT, LOS, OTS, OPWR, UNKNOWN)
#   EVENT:                    # Event name(oper_log)
#   GENERALIZED_EVENT_NAME:    # Event name for the Generalization Event Group
#   ALARM_DESC:                # Alarm string which will be generated
#   CORRELATION_TYPE:          # Correlation logic type(0:No-Correlation,
1:Generalization, 2:Timebound, 3:Counting, 4:Compression, 5:Drop-Event, 6:Severity)
#   GENERALIZED_CORRELATION_TYPE  # Correlation type, in which generalized event
will be sent
```



---

```

# CORRELATION_COUNTER:           # Counter value that will be considered during
counting logic to raise alarm
# CORRELATION_TIMER_DURATION:    # Timer duration to be considered for time bound
logic
# CORRELATION_SEVERITY:          # Alarm Severity(0:Critical, 1:Major, 2:Warning,
3:Minor, 4:Unknown)
# QUALIFIER_STRING_POSITION:     # List of positions where qualifier values present
# QUALIFIER_POSITION_1_EVENT_1: # First position of the qualifier value in the
first event
# RESOURCE_STRING_POSITION:      # List of positions where resource values present
# RESOURCE_POSITION_1_EVENT_1:  # First position of the resource value in the
first event
# SNMP_TRAP:                    # SNMP TRAP (true(1) or false(0))
# SNMP_OID:                     # OID for SNMP TRAP
# NETCONF_NOTIFICATION:         # Netconf Notification (true(1) or false(0))
# CLEAR_ALARM:                  # Clear Alarm (oper_log enum, Status for Alarm will
be made In-active if this event is received)
# CLEAR_EVENT_PATTERN_VALUES:    # Pattern values which will be searched in event's
description to identify clear event and to clear active alarm (required if both active
and clear event types are same)
# SNMP_TRAP_CLEAR:              # true(1) or false(0, if CLEAR_ALARM is null then
SNMP_TRAP_CLEAR will be null)
# SNMP_CLEAR_OID:               # OID for SNMP TRAP CLEAR
# NETCONF_CLEAR_NOTIFICATION:   # Clear Netconf Notification information

```

---

## Auto Generating the Alarm Configuration File

The `auto_yaml_generator.js` file is a NodeJS script that generates the alarm configuration file (`alarm_def_config.yaml`) for the oper logs which are listed in the `oper_logs_list.yaml` file with the default values as shown below.

```

# Integer number identifying alarm
ALARM_ID: 1000
# Event name (oper_log)
EVENT: oper_log string
# Event name for the Generalization Event Group
GENERALIZED_EVENT_NAME: null
# Alarm string which will be generated
ALARM_DESC: oper_log string
# Correlation logic type (0: No-Correlation, 1: Generalization, 2: Time Bound, 3:
Counting, 4: Compression, 5: Drop-Event)
CORRELATION_TYPE: 0
# Correlation type, in which generalized event will be sent
GENERALISED_CORRELATION_TYPE: null
# Counter value that will be considered during counting logic to raise alarm
CORRELATION_COUNTER: 3
# Timer duration to be considered for time bound logic
CORRELATION_TIMER_DURATION: 20000
# Alarm Severity(1:Emergency, 2:Alert, 3:Critical, 4:Error, 5:Warning, 6:Notification,
7:Informational, 8:Debugging, 9:Cli)
CORRELATION_SEVERITY: null
# QUALIFIER_STRING_POSITION
QUALIFIER_POSITION_1_EVENT_1: null

```

---

```
# RESOURCE_STRING_POSITION
  RESOURCE_POSITION_1_EVENT_1: null
SNMP_TRAP: 0
# OID for SNMP TRAP
SNMP_OID: null
# Netconf Notification (true (1) or false (0))
NETCONF_NOTIFICATION: 1
# Clear Alarm (oper_log enum, Status for Alarm will be made In-active if this event is
received)
CLEAR_ALARM: null
# Clear Event's pattern values which will be searched in event's description to identify
clear event
CLEAR_EVENT_PATTERN_VALUES: null
# True (1) or False (0, if CLEAR_ALARM is null then SNMP_TRAP_CLEAR will be null)
SNMP_TRAP_CLEAR: 0
# OID for SNMP TRAP CLEAR
SNMP_CLEAR_OID: null
# Clear Netconf Notification information
NETCONF_CLEAR_NOTIFICATION: 0
```

---

## Alarm Configuration File Generation Steps

1. List all the `oper_log` enums in the `oper_logs_list.yaml` file and keep the file in the same path with `auto_yaml_generator.js`.
2. Copy `auto_yaml_generator.js` and `oper_logs_list.yaml` files into `/usr/local/bin/js`.
3. Run the `auto_yaml_generator.js` script with the following command.  
`# node auto_yaml_generator.js`
4. After executing the above commands, you will see the `alarm-def-config.yaml` file in the same directory.

---

## Sample `oper_logs_list.yaml` File

```
EVENT_GROUP:
  IFMGR_IF_DOWN,
  IFMGR_IF_UP,
  STP_SET_PORT_STATE,
  STP_IPC_COMMUNICATION_FAIL,
  STP_ROOTGUARD_PORT_BLOCK,
  :
  :
```

## Alarm Descriptions

Table 31-5 describes the supported alarms.

**Table 31-5: FMS alarms**

Alarm	Description
CMM_DDM_MONITOR_CURRENT	Transceiver Bias Current crossed the threshold limit
CMM_DDM_MONITOR_FREQ	Transceiver Frequency crossed the threshold limit
CMM_DDM_MONITOR_RxPOWER	Transceiver Rx Power crossed the threshold limit
CMM_DDM_MONITOR_TEC	Transceiver Thermoelectric Cooler fault
CMM_DDM_MONITOR_TEMP	Transceiver Temperature crossed the threshold limit
CMM_DDM_MONITOR_TxPOWER	Transceiver Tx Power crossed the threshold limit
CMM_DDM_MONITOR_VOLT	Transceiver Voltage crossed the threshold limit
CMM_DDM_MONITOR_WAVE	Transceiver Wavelength crossed the threshold limit
CMM_FAN_CTRL	Fan insertion, removal, speed, or fault condition alarm
CMM_MONITOR_CPU	CPU load average crossed the threshold limit
CMM_MONITOR_CPU_CORE	CPU core usage crossed the threshold limit
CMM_MONITOR_CURRENT	Current crossed the threshold limit
CMM_MONITOR_DISK_READ_ACTIVITY	Disk read activity crossed the threshold limit
CMM_MONITOR_DISK_REMAIN_LIFE	Disk remaining life crossed the threshold limit
CMM_MONITOR_DISK_WRITE_ACTIVITY	Disk write activity crossed the threshold limit
CMM_MONITOR_FAN	FAN monitoring - crossed the threshold limit
CMM_MONITOR_PSU_POWER	Power supply unit insertion, removal, or fault condition
CMM_MONITOR_PSU_IIN	Power supply unit input current crossed the threshold limit

**Table 31-5: FMS alarms (Continued)**

Alarm	Description
CMM_MONITOR_PSU_IOUT	Power supply unit output current crossed the threshold limit
CMM_MONITOR_PSU_PIN	Power supply unit input power crossed the threshold limit
CMM_MONITOR_PSU_POUT	Power supply unit output power crossed the threshold limit
CMM_MONITOR_PSU_PRESENCE	Power supply unit is present
CMM_MONITOR_PSU_TEMP1	Power supply unit temperature 1 crossed the threshold limit
CMM_MONITOR_PSU_TEMP2	Power supply unit temperature 2 crossed the threshold limit
CMM_MONITOR_PSU_VIN	Power supply unit input voltage crossed the threshold limit
CMM_MONITOR_PSU_VOUT	Power supply unit output voltage crossed the threshold limit
CMM_MONITOR_RAM	RAM memory usage crossed the threshold limit
CMM_MONITOR_SDCARD	Hard-disk usage crossed the threshold limit or fault condition
CMM_MONITOR_TEMP	Temperature sensor crossed the threshold limit
CMM_MONITOR_VOLTAGE	Voltage crossed the threshold limit
CMM_TRANSCEIVER	Transceiver on fault condition
IFMGR_IF_DOWN	Interface state down
IFMGR_IF_UP	Interface state up

## CHAPTER 32 Erbium-Doped Fiber Amplifier (EDFA) Configuration

---

---

### Overview

Before the development of optical amplifiers, optical signals had to be converted into electrical signals, then amplified, and subsequently transformed back into optical signals. This was a very complicated and expensive process. To avoid this complexity, optical amplifiers are developed, enabling the direct amplification of optical signals without the need for conversion. This streamlined approach significantly reduced costs.

Various types of optical amplifiers include:

- Semiconductor Optical Amplifier (SOA)
- Raman Amplifiers
- Brillouin Amplifiers
- Erbium-Doped Fiber Amplifier (EDFA)

Erbium-Doped Fiber Amplifier (EDFA) uses erbium-doped fiber as an amplification medium and are extensively deployed in Wavelength Division Multiplexing (WDM) systems. It can amplify multiple optical signals simultaneously and is commonly used in the C-band and L-band.

---

### System Description

Basically, the system will be developed to combine the input signal with the pump light using a WDM coupler. This combined signal is then directed into the EDF. Within the EDF, the pump light initiates a process called population inversion, and the input signal undergoes amplification through stimulated emission.

To ensure stable signal amplification and prevent undesired back reflections from the output port, isolators are strategically placed at both the input and output ends. Additionally, the presence of isolators prevents the amplifier from functioning as a laser.

The wavelength of the pump LD is precisely controlled and maintained close to 980nm.

These optical and communication systems operate in two different modes.

---

#### APC (Automatic Power Control)

In APC mode, the microprocessor controls the output power by adjusting the pump laser to maintain a predefined reference output power level. This control mechanism ensures the output power remains constant, even when the input power fluctuates within the dynamic range.

---

#### AGC (Automatic Gain Control)

In AGC mode, the microprocessor controls the output power to maintain the specified gain relative to the input power. The expected output power cannot be guaranteed, if the input power falls below the minimum assured input power range.

## Objectives

The objective of this document is to provide the application of EDFA as a booster amplifier, Inline amplifier, and pre-amplifier.

- **Booster Amplifier:** The booster amplifier is placed just after the transmitter to increase the optical power launched to the transmission line. It's not always required in single-channel links but is an essential part of the DWDM link where the multiplexer attenuates the signal channels. It has high input power, high output power, and medium optical gain.
- **Inline Amplifier:** The inline amplifiers are placed in the transmission line, compensating for the attenuation induced by the optical fiber. The in-line EDFA is designed for optical amplification between two network nodes on the main optical link. In-line EDFAs are placed every 80-100 km to ensure that the optical signal level remains above the noise floor. It features medium to low input power, high output power, high optical gain, and a low noise figure.
- **Pre-Amplifier:** The pre-amplifier is placed just before the receiver, such that sufficient optical power is launched to the receiver. It has relatively low input power, medium output power, and medium gain.

Support added for the DDM parameters specific to the EDFA available in the QSFP28 form factor. This application supports the reading of In-power, Out-power, pump BIAS, and gain. Additionally, it will enable the configuration of the target out-power and the continuous monitoring of these attributes in accordance with the specified thresholds.

## Topology

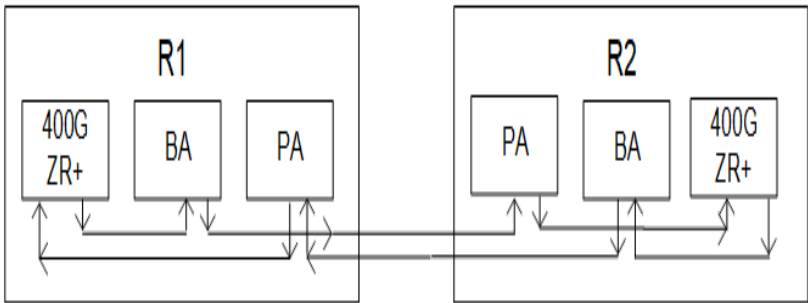


Figure 32-47: EDFA Sample Topology

## Configuration

### R1

#configure terminal	Enter into configure mode.
(config)#interface ce15	Enter into interface mode.
(config-if)#edfa operating-mode agc	Enable the EDFA operating mode AGC.
(config-if)#edfa target-gain 5	Specify the desired EDFA gain value.
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the router mode.
(config)#interface ce15	Enter into interface mode.

(config-if)#edfa operating-mode apc	Enable the EDFA operating mode APC.
(config-if)# edfa target-outpwr 10	Specify the desired EDFA output power value.
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the router mode.

## Validation

### R1 - validation for AGC mode

```
#show running-config interface cel5
```

```
!
```

```
interface cel5
```

```
    edfa operating-mode agc
```

```
    edfa target-gain 5.000
```

verify is the gain value is applied after configuring.

```
ROUTER-1#show interface cel5 transceiver detail
```

Codes: \* Not Qualified By IP Infusion, \*\* Not Supported By Module, -- No Power, - Not Applicable

Intf	DDM	InPwr (dBm)	AlertMax (dBm)	CritMax (dBm)	CritMin (dBm)	AlertMin (dBm)
cel5	Active*	-9.81	+5.00	+4.00	-20.97	-21.94
Intf	DDM	OutPwr (dBm)	AlertMax (dBm)	CritMax (dBm)	CritMin (dBm)	AlertMin (dBm)
cel5	Active*	-4.46	+20.00	+18.00	-10.00	-11.94
Intf	DDM	PumpBias (Amp)	AlertMax (Amp)	CritMax (Amp)	CritMin (Amp)	AlertMin (Amp)
cel5	Active*	+0.05	+0.59	+0.53	+0.00	+0.00
Intf	DDM	Gain (dB)	AlertMax (dB)	CritMax (dB)	CritMin (dB)	AlertMin (dB)
cel5	Active*	+3.67	+26.00	+25.00	+8.00	+7.00

### R1 - validation for APC mode

```
#show running-config interface cel5
```

```
!
```

```
interface cel5
```

```
    edfa operating-mode apc
```

```
    edfa target-outpwr 10.000
```

```
R-1#show interface cel5 transceiver detail
```

## Erbium-Doped Fiber Amplifier (EDFA) Configuration

Codes: \* Not Qualified By IP Infusion, \*\* Not Supported By Module, -- No Power, - Not Applicable

Intf	DDM	InPwr (dBm)	AlertMax (dBm)	CritMax (dBm)	CritMin (dBm)	AlertMin (dBm)
------	-----	----------------	-------------------	------------------	------------------	-------------------

ce15	Active*	-9.77	+5.00	+4.00	-20.97	-21.94
------	---------	-------	-------	-------	--------	--------

Intf	DDM	OutPwr (dBm)	AlertMax (dBm)	CritMax (dBm)	CritMin (dBm)	AlertMin (dBm)
------	-----	-----------------	-------------------	------------------	------------------	-------------------

ce15	Active*	+10.08	+20.00	+18.00	-10.00	-11.94
------	---------	--------	--------	--------	--------	--------

Intf	DDM	PumpBias (Amp)	AlertMax (Amp)	CritMax (Amp)	CritMin (Amp)	AlertMin (Amp)
------	-----	-------------------	-------------------	------------------	------------------	-------------------

ce15	Active*	+0.13	+0.59	+0.53	+0.00	+0.00
------	---------	-------	-------	-------	-------	-------

Intf	DDM	Gain (dB)	AlertMax (dB)	CritMax (dB)	CritMin (dB)	AlertMin (dB)
------	-----	--------------	------------------	-----------------	-----------------	------------------

ce15	Active*	+19.85	+26.00	+25.00	+8.00	+7.00
------	---------	--------	--------	--------	-------	-------

\*NOTE : after unconfiguring the edfa the value of output power and gain should be in default value.

Provide the following:

- o Include a Topology diagram.
- o Document configuration steps. Ensure the topology and configuration steps match.
- o Request a show running-config for the new feature.
- o Provide verification steps to demonstrate that the configuration has taken effect.
- o Add a reference to any relevant information in the existing Configuration Guide.

Note:Request a "test report" before importing QA scenarios into your doc. Ensure you only include configurations samples that "Pass".



# CHAPTER 33 NetConf Call Home Configuration

By default, in the NetConf protocol (RFC 6241), a NetConf client application initiates the connection towards the NetConf server in the network element (OcNOS device). However, for certain use cases such as in the presence of firewalls or NAT, it is useful to have “call home” functionality where the connection process is reversed and the NetConf server initiates the connection to the NetConf client. This process, as shown in [Figure 33-48](#), is standardized by IETF in RFC 8071.

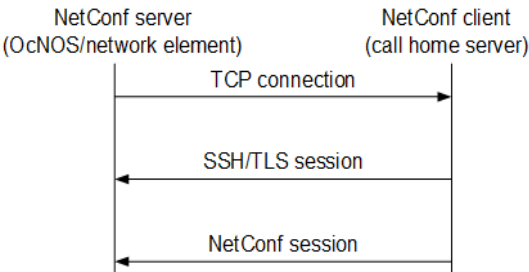


Figure 33-48: RFC 8071 NetConf call home functionality

OcNOS supports call home feature (only for SSH) at the NetConf server side. You can use any standard NetConf client application which supports call home functionality. (Call home support in the NetConf client application [Yangcli] is not supported.)

Call home is generally useful for both the initial deployment and ongoing management of networking elements.

## Configuration

(config)#netconf callhome	Enter call home mode
(netconf-callhome)#feature netconf callhome enable	Enable the call home feature
(netconf-callhome)#reconnect enable	Enable the reconnect feature
(netconf-callhome)#retry-max-attempts 10	Set the number of connect retries
(netconf-callhome)#retry-interval 20	Set the retry interval
(netconf-callhome)#callhome server test-ch-server 192.168.56.1	Configure the call home server
(netconf-callhome)#management-port enp0s3	Set the call home management port
(netconf-callhome)#commit	Commit the candidate configuration to the running configuration
(netconf-callhome)#exit	Exit call home mode

## Validation

```
(config)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
  management-port enp0s3
  reconnect enable
  retry-max-attempts 10
```

```
retry-interval 20
callhome server test-ch-server 192.168.56.1
!
(config)#
(config)#do show users
Current user          : (*).  Lock acquired by user : (#).
CLI user             : [C].  Netconf users          : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.
```

Role	Line	User	Idle	Location/Session	PID	TYPE
(#) (*)	130 vty 0	[C]root	0d00h00m	pts/0	2730	Local
network-admin						

(config)#

---

## Start the Call Home Server

After you start the call home server, the `show users` command displays a NetConf user.

2022 May 18 15:32:55.989 : OcNOS : CML : INFO : [CML\_5]: Client [netconf (192.168.56.1)] established connection with CML server

```
(config)#do show users
Current user          : (*).  Lock acquired by user : (#).
CLI user             : [C].  Netconf users          : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.
```

Role	Line	User	Idle	Location/Session	PID	TYPE
(#) (*)	130 vty 0	[C]root	0d00h00m	pts/0	2730	Local
network-admin						
	NA	[N]root	0d00h00m	1	2118	Local
network-admin						

(config)#

---

## NetConf sget Output

While the NetConf client is running, the `sget` command returns the session-specific data:

```
sget /netconf-state/sessions
```

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <netconf-state xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring">
      <sessions>
        <session>
          <session-id>1</session-id>
```

```

    <transport
      xmlns:ncm="urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring">ncm:netconf-
ssh</transport>
    <username>root</username>
    <source-host>192.168.56.1</source-host>
    <login-time>2022-05-18T15:32:55Z</login-time>
    <in-rpcs>0</in-rpcs>
    <in-bad-rpcs>0</in-bad-rpcs>
    <out-rpc-errors>0</out-rpc-errors>
    <out-notifications>0</out-notifications>
  </session>
</sessions>
</netconf-state>
</data>
</rpc-reply>

```

---

## Stop the Call Home Server

After you stop the call home server, the `show users` command no longer displays a NetConf user.

```
2022 May 18 15:33:20.028 : OcNOS : CML : NOTIF : [CML_4]: Client [netconf
(192.168.56.1)] has closed connection with CML server
```

```

(config)#
(config)#do show users
Current user      : (*).  Lock acquired by user : (#).
CLI user         : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

```

Role	Line	User	Idle	Location/Session	PID	TYPE
(#) (*) 130 vty 0 network-admin		[C]root	0d00h00m	pts/0	2730	Local

```
(config)#
```



# System Management Command Reference



## CHAPTER 1 Access Control List Commands (Standard)

---

This chapter is a reference for the standard Access Control List (ACL) commands. Standard access-lists are not allowed to be attached to interfaces and are used for protocol-level filtering.

- [ip access-list standard](#)
- [ip access-list standard filter](#)
- [ipv6 access-list standard](#)
- [ipv6 access-list standard filter](#)

---

## ip access-list standard

Use this command to define a standard IP access control list (ACL) in which multiple specifications can be configured. A specification determines whether to accept or drop an incoming IP packet based on the source IP address, either an exact match or a range of prefixes.

A standard ACL can be used by Layer 3 and SNMP protocols to permit or deny IP packets from a host or a range of prefixes.

Use the `no` form of this command to remove an ACL.

**Note:** Standard access-lists are not allowed to be attached to interfaces and are used for protocol-level filtering purposes.

### Command Syntax

```
ip access-list standard NAME
no ip access-list standard NAME
```

### Parameters

NAME	Standard IP access-list name.
------	-------------------------------

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Examples

```
#configure terminal
(config)#ip access-list standard ip-acl-01
(config-ip-acl-std)#exit
(config)#no ip access-list standard ip-acl-01
```



---

## ip access-list standard filter

Use this command to configure an access control entry in an access control list (ACL). This command determines whether to accept or drop a packet based on the configured source IP address.

Use the `no` form of this command to remove an ACL specification.

### Command Syntax

```
(deny|permit) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
no (deny|permit) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
```

### Parameters

<code>deny</code>	Drop the packet.
<code>permit</code>	Accept the packet.
<code>A.B.C.D/M</code>	Source IP prefix and length.
<code>A.B.C.D A.B.C.D</code>	Source IP address and mask.
<code>host A.B.C.D</code>	A single source host IP address.
<code>any</code>	Match any source IP address.

### Default

No default value is specified

### Command Mode

Standard IP access-list mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl-std)#permit 30.30.30.0/24
(config-ip-acl-std)#no permit 30.30.30.0/24
```

---

## Ipv6 access-list standard

Use this command to define a standard IPv6 access control list (ACL) in which multiple specifications can be configured. A specification determines whether to accept or drop an incoming IPv6 packet based on the source IPv6 address, either an exact match or a range of prefixes.

a standard IPv6 ACL can be used by Layer 3 protocols to permit or deny IPv6 packets from a host or a range of prefixes.

Use the `no` form of this command to remove an ACL.

Note: Standard access-lists are not allowed to be attached to interfaces and are used for protocol-level filtering purposes.

### Command Syntax

```
ipv6 access-list standard NAME
no ipv6 access-list standard NAME
```

### Parameters

NAME	Standard IPv6 access-list name.
------	---------------------------------

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Examples

```
#configure terminal
(config)#ipv6 access-list standard ipv6-acl-01
(config-ipv6-acl-std)#exit
(config)#no ipv6 access-list standard ipv6-acl-01
```

---

## ipv6 access-list standard filter

Use this command to configure an access control entry in an access control list (ACL). This command determines whether to accept or drop a packet based on the configured IPv6 prefix.

Use the `no` form of this command to remove an ACL specification.

### Command Syntax

```
(deny|permit) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
no (deny|permit) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
```

### Parameters

<code>deny</code>	Drop the packet.
<code>permit</code>	Accept the packet.
<code>X:X::X:X/M</code>	Source address with network mask length.
<code>X:X::X:X X:X::X:X</code>	Source address with wild card mask.
<code>any</code>	Any source address.

### Default

No default value is specified

### Command Mode

Standard IPv6 access-list mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Examples

```
#configure terminal
(config)#ipv6 access-list standard ipv6-acl-01
(config-ipv6-acl-std)#permit 2000::0/64
(config-ipv6-acl-std)#no permit 2000::0/64
```



---

## CHAPTER 2 Access Control List Commands (XGS)

---

This chapter is a reference for the Access Control List (ACL) commands for XGS devices (Trident II, Trident II+, and Tomahawk):

- [access-list logging cache-size](#)
- [access-list logging rate-limit](#)
- [arp access-group](#)
- [arp access-list](#)
- [arp access-list filter](#)
- [arp access-list remark](#)
- [arp access-list resequence](#)
- [arp access-list response](#)
- [clear access-list](#)
- [clear access-list log-cache](#)
- [clear arp access-list](#)
- [clear ip access-list](#)
- [clear ipv6 access-list](#)
- [clear mac access-list](#)
- [ip access-group](#)
- [ip access-list](#)
- [ip access-list default](#)
- [ip access-list filter](#)
- [ip access-list fragments](#)
- [ip access-list icmp](#)
- [ip access-list remark](#)
- [ip access-list resequence](#)
- [ip access-list tcp|udp](#)
- [ipv6 access-group](#)
- [ipv6 access-list](#)
- [ipv6 access-list default](#)
- [ipv6 access-list filter](#)
- [ipv6 access-list fragments](#)
- [ipv6 access-list icmpv6](#)
- [ipv6 access-list remark](#)
- [ipv6 access-list resequence](#)
- [ipv6 access-list sctp](#)
- [ipv6 access-list tcp|udp](#)
- [line vty](#)
- [mac access-group](#)

- [mac access-list](#)
- [mac access-list default](#)
- [mac access-list filter](#)
- [mac access-list remark](#)
- [mac access-list resequence](#)
- [show access-lists](#)
- [show access-list log-cache](#)
- [show arp access-lists](#)
- [show ip access-lists](#)
- [show ipv6 access-lists](#)
- [show mac access-lists](#)
- [show running-config aclmgr](#)
- [show running-config access-list](#)
- [show running-config ipv6 access-list](#)

---

## access-list logging cache-size

Use this command to set the ACL logging table size.

Use the `no` form of this command to set the table size to its default (1000).

### Command Syntax

```
access-list logging cache-size <1000-10000>
no access-list logging cache-size
```

### Parameters

<1000-10000>      Maximum number of cache entries

### Default

By default, the logging table size is 1000.

### Command Mode

Configuration mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#access-list logging cache-size 2000
(config)#end
```

---

## access-list logging rate-limit

Use this command to set the rate limit for logging ACL denied packets.

Use the `no` form of this command to reset the rate to its default (200).

### Command Syntax

```
access-list logging rate-limit <0-1000>
no access-list logging rate-limit
```

### Parameters

<0-1000>	Packets per second
----------	--------------------

### Default

By default, the rate is 200 packets per second.

### Command Mode

Configuration mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#access-list logging rate-limit 500
(config)#end
```



---

## arp access-group

Use this command to attach ARP access list to an interface to filter incoming ARP packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

Use the `no` form of this command to detach an ARP access group.

Note: To attach an ARP access-group to an interface, the `ingress-arp TCAM` group should be enabled. See the [hardware-profile filter \(XGS\)](#) command for more details.

### Command Syntax

```
arp access-group NAME in
no arp access-group NAME in
```

### Parameters

NAME	ARP Access list name
------	----------------------

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#exit
(config)#interface xe1
(config-if)#arp access-group ARP_ACL1 in
(config-if)#no arp access-group ARP_ACL1 in
```

---

## arp access-list

Use this command to define a named ARP access control list (ACL) that determines whether to accept or drop an incoming ARP packet based on the sender or target IP address, sender or target MAC address, ARP type.

An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are sequenced. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. The implied specification can be updated to permit if the use-case is to deny a certain set of ARP traffic.

Use the no form of this command to remove an ACL specification

### Command Syntax

```
arp access-list NAME
no arp access-list NAME
```

### Parameters

NAME	ARP Access list name
------	----------------------

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#exit
(config)#no arp access-list ARP_ACL1
```

## arp access-list filter

Use this command to configure access control entry in ARP access control list (ACL).

This determines whether to accept or drop an ARP packet based on the configured match criteria. Use the no form of this command to remove an ACL specification.

**Note:** Configuring the same filter again with a change of sequence number or change of action results in an update of sequence number or filter action.

### Command Syntax

```
(<1-268435453>|) (deny|permit) (request |) ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
A.B.C.D|any) mac (any | (XX-XX-XX-XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-
XX-XX-XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (vlan <1-4094>|) (inner-vlan <1-4094>|)
(log|) (sample|)

no (<1-268435453>|) (deny|permit) (request |) ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
A.B.C.D|any) mac (any | (XX-XX-XX-XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-
XX-XX-XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (vlan <1-4094>|) (inner-vlan <1-4094>|)
(log|) (sample|)
```

### Parameters

deny	Drop the packet.
permit	Accept the packet.
<1-268435453>	ARP ACL sequence number.
request	RP request type
A.B.C.D/M	Source IP prefix and length.
A.B.C.D A.B.C.D	Source IP address and mask.
host A.B.C.D	Single source host IP address.
any	Match any source IP address.
any	Any source/destination.
XX-XX-XX-XX-XX-XX	Source MAC address (Option 1).
XX:XX:XX:XX:XX:XX	Source MAC address (Option 2).
XXXX.XXXX.XXXX	Source MAC address (Option 3).
XX-XX-XX-XX-XX-XX	Source wildcard (Option 1).

`XX:XX:XX:XX:XX:XX`

Source wildcard (Option 2).

`xxxx.xxxx.xxxx` Source wildcard (Option 3).

`vlan <1-4094>` VLAN identifier.

`inner-vlan<1-4094>`

Inner VLAN identifier.

`log` Log the packets matching the filter (in-direction only).

`sample` Sample the packets matching the filter (in-direction only).

### Command Mode

ARP access-list mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#15 permit ip host 2.2.2.1 mac any inner-vlan 3
(config-arp-acl)#no 15
```

---

## arp access-list remark

Use this command to add a description to a named ARP access control list (ACL).

Use the no form of this command to remove an ACL description.

### Command Syntax

```
remark LINE
no remark
```

### Parameters

LINE                      ACL description up to 100 characters.

### Command Mode

ARP access-list mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Example

```
#configure terminal
(config)#arp access-list arplist
(config-arp-acl)#remark permit the selected arp entries
(config-arp-acl)#exit
(config)#arp access-list arplist
(config-arp-acl)#no remark
(config-arp-acl)#exit
```

---

## arp access-list resequence

Use this command to modify the sequence numbers of an ARP access list.

Note: IP Infusion Inc. recommends to use a non-overlapping sequence space for a new sequence number set to avoid unexpected rule matches during transition.

### Command Syntax

```
resequence <1-268435453> INCREMENT
```

### Parameters

<1-268435453>	Starting sequence number.
INCREMENT	Sequence number increment steps.

### Command Mode

ARP access-list mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Example

```
#configure terminal
(config)#ip access-list arplist
(config-arp-acl)#resequence 5 5
(config-arp-acl)#end
```

## arp access-list response

Use this command to configure an ARP access control entry in an ARP access control list (ACL). This determines whether to accept or drop an ARP response packet based on the configured match criteria.

Use the **no** form of this command to remove an ACL specification.

### Command Syntax

```
(<1-268435453>|) (deny|permit) response ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) mac (any | (XX-XX-XX-
XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) ) (any | (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) ) (any | (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) ) (any | (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) ) (vlan <1-4094>|) (inner-vlan <1-4094>|)
(log|) (sample|)

no (<1-268435453>|) (deny|permit) response ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) mac (any | (XX-XX-XX-
XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) ) (any | (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) ) (any | (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) ) (any | (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) ) (vlan <1-4094>|) (inner-vlan <1-4094>|)
(log|) (sample|)
```

### Parameters

deny	Drop the packet.
permit	Accept the packet.
<1-268435453>	ARP ACL sequence number.
response	ARP reply type
A.B.C.D/M	Source/Destination IP prefix and length.
A.B.C.D A.B.C.D	Source/Destination IP address and mask.
host A.B.C.D	A single source/destination host IP address.
any	Match any source/destination IP address.

any	Source/Destination any.
XX-XX-XX-XX-XX-XX	Source/Destination MAC address (Option 1).
XX:XX:XX:XX:XX:XX	Source/Destination MAC address (Option 2).
XXXX.XXXX.XXXX	Source/Destination MAC address (Option 3).
XX-XX-XX-XX-XX-XX	Source/Destination wildcard (Option 1).
XX:XX:XX:XX:XX:XX	Source/Destination wildcard (Option 2).
XXXX.XXXX.XXXX	Source/Destination wildcard (Option 3).
vlan <1-4094>	VLAN identifier.
inner-vlan <1-4094>	Inner VLAN identifier.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).

### Command Mode

ARP access-list mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#50 permit response ip host 2.2.2.1 any mac any any vlan 2
(config-arp-acl)#no 50 permit response ip host 2.2.2.1 any mac any any vlan 2
```



---

## clear access-list

Use this command to clear the access-list counters.

### Command Syntax

```
clear access-list (NAME|) counters
```

### Parameters

NAME	Access-list name.
------	-------------------

### Command Mode

Exec mode and Privilege exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#clear access-list counters
```

---

## clear access-list log-cache

Use this command to clear the access-list logging table.

### Command Syntax

```
clear access-list log-cache
```

### Parameters

None

### Command Mode

Exec mode and Privilege exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#clear access-list log-cache
```

---

## clear arp access-list

Use this command to clear the ARP access-list counters.

### Command Syntax

```
clear arp access-list (NAME|) counters
```

### Parameters

NAME	ARP access list name
------	----------------------

### Command Mode

Exec mode and privileged exec mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Example

```
#clear arp access-list counters
```

---

## clear ip access-list

Use this command to clear the IP access-list counters.

### Command Syntax

```
clear ip access-list (NAME|) counters
```

### Parameters

NAME                      Access-list name.

### Command Mode

Exec mode and Privilege exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#clear ip access-list counters
```

---

## clear ipv6 access-list

Use this command to clear the IPv6 access-list counters.

### Command Syntax

```
clear ipv6 access-list (NAME|) counters
```

### Parameters

NAME	Access-list name.
------	-------------------

### Command Mode

Exec mode Privilege exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#clear ipv6 access-list counters
```

---

## clear mac access-list

Use this command to clear the MAC access-list counters.

### Command Syntax

```
clear mac access-list (NAME|) counters
```

### Parameters

NAME	Access-list name.
------	-------------------

### Command Mode

Exec mode Privilege exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#clear mac access-list counters
```

---

## ip access-group

Use this command to attach an IP access list to an interface or terminal line to filter incoming or outgoing IP packets.

The `time-range` parameter is optional. If used, the access-group is tied to the timer specified.

After the access-group has been configured with the time-range, to detach the access-group from the time-range, use the `no` form of this command with a time-range parameter as shown in the syntax and examples below.

To delete the access-group, use the `no` form of this command without a time-range.

**Note:** An egress IP ACL is supported on physical and lag interfaces only. An egress IP ACL will match only routed traffic and not switched traffic. VLAN and inner-VLAN options in ACL rules will match incoming packet VLANs even when ACL attached at egress.

### Command Syntax

```
ip access-group NAME (in|out) (time-range TR_NAME|)
no ip access-group NAME (in|out) (time-range TR_NAME|)
```

### Parameters

NAME	Access list name.
in	Filter incoming packets
out	Filter outgoing packets.
TR_NAME	Time range name set with the <a href="#">time-range</a> command.

### Command Mode

Line mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3. The `time-range` parameter was added in OcNOS-SP version 5.0.

### Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#permit ip any any
(config-ip-acl)#exit

(config)#hardware-profile filter ingress-ipv4-ext enable

(config)#interface xe3
(config-if)#ip access-group mylist in
(config-if)#exit

(config)#interface xe3
(config-if)#no ip access-group mylist in time-range TIMER1
(config-if)#exit
```

```
(config)#line vty
(config-all-line)#no ip access-group mylist in
```

### Usage: VLANs and LAGs

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

### Usage: TCAM Groups

An access-group in the egress direction uses the TCAM group used by the QoS output service policy. Therefore, actions are unpredictable when conflicting matches are configured on same interface. IP Infusion Inc. recommends to avoid such a configuration. Otherwise, you need to configure the priority (in QoS) or the sequence number (in ACL) carefully to handle such cases.

To attach an IP ACL in the ingress direction, ensure the `ingress-ipv4` TCAM group is enabled. See the [hardware-profile filter \(XGS\)](#) commands for details.

### Usage: Loopback and VTY Interfaces

You can create ACLs for loopback (inband) and VTY interfaces to protect management applications such as SSH, Telnet, NTP, SNMP, and SNMP traps. Filtering TCP, UDP, and ICMP are supported.

**Note:** Loopback and VTY ACLs are mutually exclusive. If you set up one, you cannot set up the other.

For an ACL for a loopback interface, you create the ACL, configure it with rules, and associate the ACL with a loopback interface:

```
...
(config)#interface lo
(config-if)#ip access-group loopback in
```

For an ACL for VTY, you create the ACL, configure it with rules, and associate the ACL to the terminal line in line mode:

```
...
(config)#line vty
(config-all-line)#ip access-group vty in
```

Loopback and VTY ACLs do not support the following:

- The default rule `deny all`. You must explicitly set up a `deny all` rule based on your requirements.
- VLAN-specific rules.
- Rules with TCP flags.
- Rules with `dscp`, `fragments`, `log`, `precedence`, and `sample` parameters.

### Usage: Timed ACL on interfaces

You create a timer range that is identified by a name and configured with a start time, end time, and frequency. Once you create the time range, you can tie the ACL configuration to the time-range object. This allows you to create an



access group that is enabled when the timer has started and disabled when the timer ends. You can also disassociate an access group from the timer if needed.

---

## ip access-list

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming IP packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Use the `no` form of this command to remove an ACL

### Command Syntax

```
ip access-list NAME
no ip access-list NAME
```

### Parameters

NAME	Access-list name.
------	-------------------

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
```

---

## ip access-list default

Use this command to modify the default rule action of access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the IP packets not matching any of the user defined rules match default rule.

### Command Syntax

```
default (deny-all|permit-all) (log|) (sample|)
```

### Parameters

deny-all	Drop all packets.
permit-all	Accept all packets.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).

### Command Mode

IP access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl)#default permit-all sample
```

---

## ip access-list filter

Use this command to configure access control entry in an access control list (ACL).

This determines whether to accept or drop an IP packet based on the configured match criteria.

Use the `no` form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

**Note:** Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

### Command Syntax

```
(<1-268435453>|) (deny|permit) (<0-255>|ahp|any|eigrp|esp|gre|ipip|ipcomp|ipv6ip
|ospf|pim|rsvp|vrrp) (A.B.C.D/ M|A.B.C.D A.B.C.D|host A.B.C.D|any) (A.B.C.D/
M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63>|af11| af12| af13| af21| af22|
af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
default| ef )) (fragments|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|)
(sample|)((redirect-to-port IFNAME)|)

no (<1-268435453>|) (deny|permit) (<0-255> |ahp | any | eigrp | esp | gre | ipip |
ipcomp | ipv6ip | ospf | pim | rsvp| vrrp) (A.B.C.D/ M|A.B.C.D A.B.C.D | host
A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63> |af11|
af12| af13| af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3|
cs4| cs5|cs6| cs7| default| ef )) (fragments|) (vlan <1-4094>|) (inner-vlan <1-
4094>|) (log|) (sample|)|)((redirect-to-port IFNAME)|)

no (<1-268435453>)
```

### Parameters

<1-268435453>	IPv4 ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
<0-255>	IANA assigned protocol number.
any	Any protocol packet.
ahp	Authentication Header packet.
eigrp	Enhanced Interior Gateway Routing Protocol packet.
esp	Encapsulating Security Payload packet.
gre	Generic Routing Encapsulation packet.
ipip	IPv4 over IPv4 encapsulation packet.
ipcomp	IP Payload Compression Protocol packet.
ipv6ip	IPv6 over IPv4 encapsulation packet.
ospf	Open Shortest Path First packet.
pim	Protocol Independent Multicast packet
rsvp	Resource Reservation Protocol packet.
vrrp	Virtual Router Redundancy Protocol packet.
A.B.C.D/M	Source IP prefix and length.

---

A.B.C.D A.B.C.D	Source IP address and mask.
host A.B.C.D	A single source host IP address.
any	Match any source IP address.
A.B.C.D/M	Destination IP prefix and length.
A.B.C.D A.B.C.D	Destination IP address and mask.
host A.B.C.D	A single destination host IP address.
any	Any destination address
any	Match any destination IP address.
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).

---

immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).
priority	Match packets with priority precedence (1).
routine	Match packets with routine precedence (0).
fragments	Check non-initial fragments.
vlan	Match packets with given VLAN identifier.
<1-4094>	Enter VLAN identifier.
inner-vlan	Match packets with given inner VLAN identifier.
<1-4094>	Enter inner-VLAN identifier.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).
redirect-to-port	Redirect the packet (in-direction only)
IFNAME	Interface name to which packet to be redirected (switchport only)

### Command Mode

IP access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl)#11 permit any 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
(config-ip-acl)#no 11
```

---

## ip access-list fragments

Use this command to configure access list to deny or permit all the IP fragmented packets.

Use the `no` form of this command to remove an ACL specification.

**Note:** Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

### Command Syntax

```
(<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|)
no (<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|)
```

### Parameters

<code>deny-all</code>	Drop the packet.
<code>permit-all</code>	Accept the packet.
<code>&lt;1-268435453&gt;</code>	IPv4 ACL sequence number.
<code>fragments</code>	Check non-initial.
<code>log</code>	Log the packets matching the filter (in-direction only).
<code>sample</code>	Sample the packets matching the filter (in-direction only).

### Command Mode

IP access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#fragments deny-all
(config-ip-acl)#end
```

## ip access-list icmp

Use this command to permit or deny ICMP packets based on the given source and destination IP address. Even DSCP, precedence, VLAN identifier, inner VLAN identifier, and fragment number can be configured to permit or deny with the given values.

Use the **no** form of this command to remove an ACL specification.

**Note:** Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

### Command Syntax

```
(<1-268435453>|) (deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
(A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (administratively-prohibited|
alternate-address| conversion-error|dod-host-prohibited| dod-net-prohibited|
echo| echo-reply|general-parameter-problem| host-isolated| host-precedence-
unreachable|host-redirect| host-tos-redirect| host-tos-unreachable| host-
unknown|host-unreachable| information-reply| information-request| mask-
reply|mask-request| mobile-redirect| net-redirect| net-tos-redirect|net-tos-
unreachable| net-unreachable| network-unknown| no-room-for-option|option-missing|
packet-too-big| parameter-problem| port-unreachable|precedence-unreachable|
protocol-unreachable| reassembly-timeout| redirect|router-advertisement| router-
solicitation| source-quench|source-route-failed|time-exceeded| timestamp-reply|
timestamp-request| traceroute|ttl-exceeded|unreachable|(<0-255> (<0-255>|))|)
(("dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32| af33| af41| af42|
af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef ))| (precedence (<0-7>|
critical| flash | flashoverride|immediate| internet| network| priority|
routine))|) (fragments|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|) (sample|)
((redirect-to-port IFNAME)|)

no (<1-268435453>|) (deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|host
A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (administratively-
prohibited| alternate-address| conversion-error|dod-host-prohibited| dod-net-
prohibited| echo| echo-reply|general-parameter-problem| host-isolated| host-
precedence-unreachable|host-redirect| host-tos-redirect| host-tos-unreachable|
host-unknown|host-unreachable| information-reply| information-request| mask-
reply|mask-request| mobile-redirect| net-redirect| net-tos-redirect|net-tos-
unreachable| net-unreachable| network-unknown| no-room-for-option|option-missing|
packet-too-big| parameter-problem| port-unreachable|precedence-unreachable|
protocol-unreachable| reassembly-timeout| redirect|router-advertisement| router-
solicitation| source-quench|source-route-failed|time-exceeded| timestamp-reply|
timestamp-request| traceroute|ttl-exceeded|unreachable|(<0-255> (<0-255>|))|)
(("dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32| af33| af41| af42|
af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef ))| (precedence (<0-7>|
critical| flash | flashoverride|immediate| internet| network| priority|
routine))|) (fragments|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|) (sample|)
((redirect-to-port IFNAME)|)
```

### Parameters

<1-268435453>	IPv4 ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.



---

icmp	Internet Control Message Protocol packet.
A.B.C.D/M	Source IP prefix and length.
A.B.C.D A.B.C.D	Source IP address and mask.
host A.B.C.D	A single source host IP address.
any	Match any source IP address.
A.B.C.D/M	Destination IP prefix and length.
A.B.C.D A.B.C.D	Destination IP address and mask.
host A.B.C.D	A single destination host IP address.
any	Match any destination IP address.
administratively-prohibited	Administratively prohibited.
alternate-address	Alternate address.
conversion-error	Datagram conversion.
dod-host-prohibited	Host prohibited.
dod-net-prohibited	Net prohibited.
echo	Echo (ping).
echo-reply	Echo reply.
general-parameter-problem	Parameter problem.
host-isolated	Host isolated.
host-precedence-unreachable	Host unreachable for precedence.
host-redirect	Host redirect.
host-tos-redirect	Host redirect for ToS.
host-tos-unreachable	Host unreachable for ToS.
host-unknown	Host unknown.
host-unreachable	Host unreachable.
information-reply	Information replies.
information-request	

---

	Information requests.
mask-reply	Mask replies.
mask-request	Mask requests.
mobile-redirect	
	Mobile host redirect.
net-redirect	Network redirect.
net-tos-redirect	
	Net redirect for ToS.
net-tos-unreachable	
	Network unreachable for ToS.
net-unreachable	
	Net unreachable.
network-unknown	
	Network unknown.
no-room-for-option	
	Parameter required but no room.
option-missing	Parameter required but not present.
packet-too-big	Fragmentation needed and DF set.
parameter-problem	
	All parameter problems.
port-unreachable	
	Port unreachable.
precedence-unreachable	
	Precedence cutoff.
protocol-unreachable	
	Protocol unreachable.
reassembly-timeout	
	Reassembly timeout.
redirect	All redirects.
router-advertisement	
	Router discovery advertisements.
router-solicitation	
	Router discovery solicitations.
source-quench	Source quenches.
source-route-failed	
	Source route failed.
time-exceeded	All time-exceeded messages.
timestamp-reply	
	Time-stamp replies.

---

timestamp-request	Time-stamp requests.
traceroute	Traceroute.
ttl-exceeded	TTL exceeded.
unreachable	All unreachables.
<0-255>	ICMP type.
<0-255>	ICMP code.
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34.
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).

---

<code>priority</code>	Match packets with priority precedence (1).
<code>routine</code>	Match packets with routine precedence (0).
<code>fragments</code>	Check non-initial fragments.
<code>vlan</code>	Match packets with given VLAN identifier.
<code>&lt;1-4094&gt;</code>	Enter VLAN identifier.
<code>inner-vlan</code>	Match packets with given inner VLAN identifier.
<code>&lt;1-4094&gt;</code>	Enter inner-VLAN identifier.
<code>log</code>	Log the packets matching the filter (in-direction only).
<code>sample</code>	Sample the packets matching the filter (in-direction only).
<code>redirect-to-port</code>	Redirect the packet (in-direction only)
<code>IFNAME</code>	Interface name to which packet to be redirected (switchport only)

### Command Mode

IP access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip access-list ip-icmp
(config-ip-acl)#200 permit icmp any any
```

---

## ip access-list remark

Use this command to add a description to a named IPv4 access control list (ACL).

Use the `no` form of this command to remove an ACL description.

### Command Syntax

```
remark LINE
no remark
```

### Parameters

LINE                      ACL description up to 100 characters.

### Command Mode

IP access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#remark permit the inside admin address
(config-ip-acl)#exit

(config)#ip access-list mylist
(config-ip-acl)#no remark
(config-ip-acl)#exit
```

---

## ip access-list resequence

Use this command to modify the sequence numbers of an IP access list specification.

**Note:** Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

**Note:** Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

### Command Syntax

```
resequence <1-268435453> INCREMENT
```

### Parameters

<1-268435453> Starting sequence number.

INCREMENT Sequence number increment steps.

### Command Mode

IP access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#resequence 5 5
(config-ip-acl)#end
```

## ip access-list tcp|udp

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming packet based on the criteria specified match criteria.

This form of this command filters packets based on source and destination IP address along with protocol (TCP or UDP) and port.

Use the `no` form of this command to remove an ACL specification.

**Note:** Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

**Note:** TCP flags options and range options like `neq`, `gt`, `lt` and `range` are not supported by hardware in egress direction.

**Note:** Both `Ack` and `established` flag in `tcp` have same functionality in hardware.

### Command Syntax

```
(<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|drip|echo
|exec|finger|ftp|ftp-data|gopher|hostname|ident|irc|klogin|kshell|login
|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|
uucp|whois|www)| range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host
A.B.C.D|any) ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|
drip|echo|exec|finger|ftp|ftp-data|gopher|hostname|ident|irc|klogin|kshell|login
|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
|time|uucp|whois|www)| range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12|
af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4|
cs5| cs6| cs7| default| ef)) |(precedence (<0-7>| critical| flash |
flashoverride| immediate| internet| network| priority| routine)) |)
({ack|established|fin|psh|rst|syn|urg}|) (fragments|) (vlan <1-4094>|) (inner-vlan
<1-4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|)

(<1-268435453>|) (deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
((eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard|dnsmx|domain|
echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-
isakmp|ntp|pim-auto-rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp
|time|who|xmcpc)| range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host
A.B.C.D|any) ((eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard|dnsmx|
domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
ss|non500-isakmp|ntp|pim-auto-rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|
tftp|time|who|xmcpc)| range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12|
af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4|
cs5| cs6| cs7| default| ef)) |(precedence (<0-7>| critical| flash |
flashoverride| immediate| internet| network| priority| routine)) |)
(fragments|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|) (sample|)

no (<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D A.B.C.D|host
A.B.C.D|any) ((eq|gt|lt|neq) (<0-65535>| bgp| chargen| cmd| daytime| discard|
domain| drip| echo|exec|finger|ftp|ftp-data|gopher|hostname| ident| irc|
klogin| kshell|login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs
|talk|telnet|time|uucp|whois|www)| range <0-65535> <0-65535>|) (A.B.C.D/
M|A.B.C.D A.B.C.D|host A.B.C.D|any) ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd
|daytime|discard|domain|drip|echo|exec|finger|ftp|ftp-data|gopher|hostname|
ident|irc|klogin|kshell|login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh
```

```

|sunrpc|tacacs|talk|telnet|time|uucp|whois|www) | range <0-65535> <0-65535>|)
((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42|
af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>|
critical| flash | flashoverride| immediate| internet| network| priority|
routine)) |) ({ack|established|fin|psh|rst|syn|urg}|) (fragments|)(vlan <1-
4094>|)(inner-vlan <1-4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|)

no (<1-268435453>|)(deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix| domain| echo|
isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|
ntp|pim-auto- rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xdmcp) |
range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D| any)
((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix| domain|echo|
isakmp|mobile- ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|
ntp|pim-auto- rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xdmcp) |
range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12| af13| af21| af22| af23|
af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default|
ef)) | (precedence (<0-7>| critical| flash | flashoverride| immediate| internet|
network| priority| routine)) |) (fragments|)(vlan <1-4094>|)(inner-vlan <1-
4094>|) (log|) (sample|)((redirect-to-port IFNAME)|)

```

## Parameters

<1-268435453>	IPv4 ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
tcp	Transmission Control Protocol.
udp	User Datagram Protocol.
A.B.C.D/M	Source or destination IP prefix and length.
A.B.C.D A.B.C.D	Source or destination IP address and mask.
host A.B.C.D	Source or destination host IP address.
any	Any source or destination IP address.
eq	Source or destination port equal to.
gt	Source or destination port greater than.
lt	Source or destination port less than.
neq	Source or destination port not equal to.
<0-65535>	Source or destination port number.
range	Range of source or destination port numbers:
<0-65535>	Lowest value in the range.
<0-65535>	Highest value in the range.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd	Remote commands.
daytime	Daytime.
discard	Discard.



---

domain	Domain Name Service.
drip	Dynamic Routing Information Protocol.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections.
gopher	Gopher.
hostname	NIC hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login.
lpd	Printer service.
nnntp	Network News Transport Protocol.
pim-auto-rp	PIM Auto-RP.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
smtp	Simple Mail Transport Protocol.
ssh	Secure Shell.
sunrpc	Sun Remote Procedure Call.
tacacs	TAC Access Control System.
talk	Talk.
telnet	Telnet.
time	Time.
uucp	UNIX-to-UNIX Copy Program.
whois	WHOIS/NICNAME
www	World Wide Web.
nnntp	Range of source or destination port numbers:
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.

---

af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).
priority	Match packets with priority precedence (1).
routine	Match packets with routine precedence (0).
ack	Match on the Acknowledgment (ack) bit.
established	Matches only packets that belong to an established TCP connection.
fin	Match on the Finish (fin) bit.
psh	Match on the Push (psh) bit.
rst	Match on the Reset (rst) bit.
syn	Match on the Synchronize (syn) bit.
urg	Match on the Urgent (urg) bit.
biff	Biff.
bootpc	Bootstrap Protocol (BOOTP) client.
bootps	Bootstrap Protocol (BOOTP) server.
discard	Discard.
dnsix	DNSIX security protocol auditing.
domain	Domain Name Service.
echo	Echo.
isakmp	Internet Security Association and Key Management Protocol.

---

mobile-ip	Mobile IP registration.
nameserver	IEN116 name service.
netbios-dgm	Net BIOS datagram service.
netbios-ns	Net BIOS name service.
netbios-ss	Net BIOS session service.
non500-isakmp	Non500-Internet Security Association and Key Management Protocol.
ntp	Network Time Protocol.
pim-auto-rp	PIM Auto-RP.
snmp	Simple Network Management Protocol.
snmptrap	SNMP Traps.
sunrpc	Sun Remote Procedure Call.
syslog	System Logger.
tacacs	TAC Access Control System.
talk	Talk.
tftp	Trivial File Transfer Protocol.
time	Time.
who	Who service.
xdmcp	X Display Manager Control Protocol.
fragments	Check non-initial fragments.
vlan	Match packets with given VLAN identifier.
<1-4094>	Enter VLAN identifier.
inner-vlan	Match packets with given inner VLAN identifier.
<1-4094>	Enter inner-VLAN identifier.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).
IFNAME	Interface name to which packet to be redirected (switchport only)
redirect-to-port	Redirect the packet (in-direction only)

## Command Mode

IP access-list mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#configure terminal
(config)#ip access-list ip-acl-02
(config-ip-acl)#deny udp any any eq tftp
(config-ip-acl)#deny tcp any any eq ssh
(config-ip-acl)#end
```

---

## ipv6 access-group

Use this command to attach an IPv6 access list to an interface to filter incoming or outgoing packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

**Note:** To attach an IPv6 access-group on interface, the IPv6 TCAM group should be enabled. To enable ingress-IPv6 / egress-IPv6, see the [hardware-profile filter \(XGS\)](#) command.

The `time-range` parameter is optional. If used, the access-group is tied to the timer specified.

After the access-group has been configured with the time-range, to detach the access-group from the time-range, use the `no` form of this command with a time-range parameter as shown in the syntax and examples below.

To delete the access-group, use the `no` form of this command without a time-range.

**Note:** To attach IPv6 ACL in the ingress direction ingress-ipv6 TCAM group needs to be enabled. See the [hardware-profile filter \(Qumran\)](#) command for details.

### Command Syntax

```
ipv6 access-group NAME in (time-range TR_NAME|)
no ipv6 access-group NAME in (time-range TR_NAME|)
```

### Parameters

NAME	Access list name.
TR_NAME	Time range name set with the <a href="#">time-range</a> command.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3. The `time-range` parameter was added in OcNOS-SP version 5.0.

### Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#permit ipv6 any any
(config-ipv6-acl)#exit
(config)#hardware-profile filter ingress-ipv6 enable

(config)#interface xe3
(config-if)#ipv6 access-group mylist in
```

```
(config)#interface xe3
(config-if)#no ipv6 access-group mylist in

(config)#interface xe3
(config-if)#ipv6 access-group mylist in time-range TIMER1

(config)#interface xe3
(config-if)#no ipv6 access-group mylist in time-range TIMER1
```

---

## ipv6 access-list

Use this command to define a IPv6 access control list (ACL) that determines whether to accept or drop an incoming IPv6 packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Use the `no` form of this command to remove an ACL.

**Note:** For IPv6 routing protocols need neighbor discovery for the session to establish. Applying `ipv6 acls` implicitly drops all the `icmpv6` packets, thereby affecting the protocol sessions. To overcome this problem, implicit `icmpv6 permit` rule is added in the IPv6 acls.

If required behavior is to deny the `icmpv6`, implicit rule can be deleted.

For example,

To create an `ipv6 acl`, execute the following:

```
(config)#ipv6 access-list ipv6-acl
#show ipv6 access-lists
IPv6 access list ip1
268435453 permit icmpv6 any any
```

To delete this rule, execute the following:

```
(config)#ipv6 access-list ipv6-acl
(config-ipv6-acl)# no 268435453 permit icmpv6 any any

#show ipv6 access-lists
IPv6 access list ip1
```

### Command Syntax

```
ipv6 access-list NAME
no ipv6 access-list NAME
```

### Parameters

NAME	Access-list name.
------	-------------------

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

Implicit rule is introduced in OcNOS version 2.0.

**Examples**

```
#configure terminal
(config)#ipv6 access-list ipv6-acl-01
(config-ipv6-acl)#exit
```

---

## ipv6 access-list default

Use this command to modify the default rule action of access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the IPv6 packets not matching any of the user defined rules match default rule.

### Command Syntax

```
default (deny-all|permit-all) (log|) (sample|)
```

### Parameters

deny-all	Drop all packets.
permit-all	Accept all packets.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).

### Command Mode

IPv6 access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip access-list ipv6-acl-01
(config-ipv6-acl)#default permit-all sample
```



## ipv6 access-list filter

Use this command to define an access-control entry in an access control list (ACL) that determines whether to accept or drop an IPv6 packet based on the criteria specified. This form of this command filters packets based on:

- Protocol
- Source IP address
- Destination IP address

Use the `no` form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

**Note:** Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

**Note:** For IPv6 source and destination address filters, only the network part from the address (upper 64 bits) is supported due to hardware restriction. If the address length is more than 64 bits, it cannot be applied on the interfaces but it can be used with distributed list in control plane protocols.

### Command Syntax

```
(<1-268435453>|) (deny|permit) (<0-255>|ahp|any|eigrp|esp|gre|ipip6|ipcomp
|ipv6|ospf|pim|rsdp|vrrp) (X:X::X:X/ M|X:X::X:X X:X::X:X|host X:X::X:X|any)
(X:X::X:X/M|X:X::X:X X:X::X:X|any) (dscp (<0-63>|af11| af12| af13| af21| af22|
af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
default| ef )) (flow-label<0-1048575>|) (fragments|) (vlan <1-4094>|) (inner-vlan
<1-4094>|) (log|) (sample|)((redirect-to-port IFNAME)|)

no (<1-268435453>|) (deny|permit) (<0-255>|ahp|any|eigrp|esp|gre|ipip6|ipcomp
|ipv6|ospf|pim|rsdp|vrrp) (X:X::X:X/ M|X:X::X:X X:X::X:X|host X:X::X:X|any)
(X:X::X:X/M|X:X::X:X X:X::X:X|any) (dscp (<0-63>|af11| af12| af13| af21| af22|
af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
default| ef )) (flow-label<0-1048575>|) (fragments|) (vlan <1-4094>|) (inner-vlan
<1-4094>|) (log|) (sample|)((redirect-to-port IFNAME)|)

no (<1-268435453>|)
```

### Parameters

<1-268435453>	IPv4 ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
<0-255>	IANA assigned protocol number.
any	Any protocol packet.
ahp	Authentication Header packet.
eigrp	Enhanced Interior Gateway Routing Protocol packet.
esp	Encapsulating Security Payload packet.
gre	Generic Routing Encapsulation packet.
ipip6	IPv4 over IPv6 Encapsulation packet.
ipcomp	IP Payload Compression Protocol packet.
ipv6ip6	IPv6 over IPv6 Encapsulation packet.

ospf	Open Shortest Path First packet.
pim	Protocol Independent Multicast packet
rsvp	Resource Reservation Protocol packet. v
rrp	Virtual Router Redundancy Protocol packet.
X:X::X:X/M	Source Address with network mask length.
X:X::X:X X:X::X:X	Source Address with wild card mask.
any	Any source address.
X:X::X:X/M	Destination address with network mask length.
X:X::X:X X:X::X:X	Destination address with wild card mask.
any	Match any destination IP address.
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
vlan	Match packets with given VLAN identifier.
<1-4094>	VLAN identifier.
inner-vlan	Match packets with given inner VLAN identifier.
<1-4094>	Inner-VLAN identifier.

<code>redirect-to-port</code>	Redirect the packet (in-direction only)
<code>IFNAME</code>	Interface name to which packet to be redirected

## Command Mode

IPv6 access-list mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#configure terminal
(config)#ipv6 access-list ipv6-acl-01
(config-ip-acl)#permit ipipv6 any any
(config-ip-acl)#end
```

---

## ipv6 access-list fragments

Use this command to permit or deny all the IPv6 fragments.

Use the no form of this command to remove an ACL specification.

**Note:** Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

### Command Syntax

```
(<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|)  
no (<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|)
```

### Parameters

<1-268435453>	IPv6 ACL sequence number.
fragments	Check non-initial fragments.
deny-all	Specify packets to reject.
permit-all	Specify packets to forward.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).

### Command Mode

IPv6 access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal  
(config)#ipv6 access-list mylist  
(config-ipv6-acl)#fragments deny-all
```

## ipv6 access-list icmpv6

Use this command to permit or deny IPv6 ICMP packets with the given source and destination IPv6 address, DSCP value, VLAN identifier, inner VLAN identifier, fragments, and flow label.

Use the no form of this command to remove an ACL specification.

**Note:** Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

### Command Syntax

```
(<1-268435453>|) (deny|permit) (icmpv6) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
(X:X::X:X/ M|X:X::X:X X:X::X:X|any) (beyond-scope| destination-unreachable| echo-reply|
echo-request| header| hop-limit| mld-query| mld-reduction| mld-report| nd-na| nd-ns| next-
header| no-admin| no-route| packet-too-big| parameter-option| parameter-problem| port-
unreachable| reassembly-timeout| redirect| renum-command| renum-result| renum-seq-number|
router-advertisement| router-renumbering| router-solicitation| time-exceeded| unreachable |
(<0-255> (<0-255>|)|)) (dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32|
af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef)|) (flow-
label <0-1048575>|) (fragments|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|)
(sample|)((redirect-to-port IFNAME)|)

no (<1-268435453>|) (deny|permit) (icmpv6) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
(X:X::X:X/M|X:X::X:X X:X::X:X|any) (beyond-scope| destination-unreachable| echo-reply|
echo-request| header| hop-limit| mld-query| mld-reduction| mld-report| nd-na| nd-ns| next-
header| no-admin| no-route| packet-too-big| parameter-option| parameter-problem| port-
unreachable| reassembly-timeout| redirect| renum-command| renum-result| renum-seq-number|
router-advertisement| router-renumbering| router-solicitation| time-exceeded| unreachable |
(<0-255> (<0-255>|)|)) (dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32|
af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef)|) (flow-
label <0-1048575>|) (fragments|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|)
(sample|)((redirect-to-port IFNAME)|)
```

### Parameters

<1-268435453>	IPv6 ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
icmpv6	Internet Control Message Protocol packet.
X:X::X:X/M	Source Address with network mask length.
X:X::X:X X:X::X:X	Source Address with wild card mask.
any	Any source address.
X:X::X:X/M	Destination address with network mask length.
X:X::X:X X:X::X:X	Destination address with wild card mask.
any	Any destination address
beyond-scope	Destination beyond scope
destination-unreachable	

	Destination address is unreachable
echo-reply	Echo reply
echo-request	Echo request (ping)
header	Parameter header problems
hop-limit	Hop limit exceeded in transit
mld-query	Multicast Listener Discovery Query
mld-reduction	Multicast Listener Discovery Reduction
mld-report	Multicast Listener Discovery Report
nd-na	Neighbor discovery neighbor advertisements
nd-ns	Neighbor discovery neighbor solicitations
next-header	Parameter next header problems
no-admin	Administration prohibited destination
no-route	No route to destination
packet-too-big	Packet too big
parameter-option	Parameter option problems
parameter-problem	All parameter problems
port-unreachable	Port unreachable
reassembly-timeout	Reassembly timeout
redirect	Neighbor redirect
renum-command	Router renumbering command
renum-result	Router renumbering result
renum-seq-number	Router renumbering sequence number reset
router-advertisement	Neighbor discovery router advertisements
router-renumbering	All router renumbering
router-solicitation	Neighbor discovery router solicitations
time-exceeded	All time exceeded messages
unreachable	All unreachable
<0-255>	ICMPv6 message type
<0-255>	ICMPv6 message code
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.

---

af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34.
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
flow-label	IPv6 Flow-label.
<0-1048575>	IPv6 Flow-label value.
fragments	Check non-initial fragments.
vlan	Match packets with given VLAN identifier.
<1-4094>	Enter VLAN identifier.
inner-vlan	Match packets with given inner VLAN identifier.
<1-4094>	Enter inner-VLAN identifier.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).
redirect-to-port	Redirect the packet (in-direction only)
IFNAME	Interface name to which packet to be redirected (switchport only)

**Command Mode**

IPv6 access-list mode

**Applicability**

This command was introduced before OcNOS version 1.3.

## Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#200 permit icmpv6 any any fragments
```



---

## ipv6 access-list remark

Use this command to add a description to an IPv6 access control list (ACL).

Use the `no` form of this command to remove an access control list description.

### Command Syntax

```
remark LINE
no remark
```

### Parameters

LINE                      ACL description up to 100 characters.

### Command Mode

IPv6 access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)# remark Permit the inside admin address
```

---

## ipv6 access-list resequence

Use this command to modify the sequence numbers of an IPv6 access list specification.

**Note:** Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

**Note:** Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

### Command Syntax

```
resequence <1-268435453> INCREMENT
```

### Parameters

<1-268435453> Starting Sequence number.

INCREMENT Sequence number increment steps.

### Command Mode

IPv6 access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#resequence 15 15
```

## ipv6 access-list sctp

Use this command to allow ACL to permit or deny SCTP packets based on the given source and destination IPV6 address. Even DSCP, VLAN identifier, inner VLAN identifier, flow label, and fragment can be configured to permit or deny with the given values.

Use the **no** form of this command to remove an ACL specification.

**Note:** Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

### Command Syntax

```
(<1-268435453>|) (deny|permit) (sctp) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>) | (range <0-65535> <0-65535>)| (fragments)| } (dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)|) ((flow-label <0-1048575>)|) (fragments|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|) (sample|)((redirect-to-port IFNAME)|)

no (<1-268435453>|) (deny|permit) (sctp) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>) | (range <0-65535> <0-65535>)| (fragments)| } (dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)|) ((flow-label <0-1048575>)|) (fragments|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|) (sample|)((redirect-to-port IFNAME)|)
```

### Parameters

<1-268435453>	IPv6 ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
sctp	Stream Control Transmission Protocol packet.
X:X::X:X/M	Source address with network mask length.
X:X::X:X	Source address with wild card mask.
X:X::X:X	Source address's wild card mask (ignored bits).
any	Any source address.
X:X::X:X/M	Destination address with network mask length.
X:X::X:X	Destination address with wild card mask.
X:X::X:X	Destination address's wild card mask (ignored bits).
any	Any destination address.
eq	Source or destination port equal to.
gt	Source or destination port greater than.
lt	Source or destination port less than.
neq	Source or destination port not equal to.
<0-65535>	Source or destination port number.
range	Range of source or destination port numbers:
<0-65535>	Lowest value in the range.

<0-65535>	Highest value in the range.
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34.
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
flow-label	IPv6 Flow-label.
<0-1048575>	IPv6 Flow-label value.
fragments	Check non-initial fragments.
vlan	Match packets with given VLAN identifier.
<1-4094>	Enter VLAN identifier.
inner-vlan	Match packets with given inner VLAN identifier.
<1-4094>	Enter inner-VLAN identifier.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).
redirect-to-port	Redirect the packet (in-direction only)
IFNAME	Interface name to which packet to be redirected (switchport only)

**Command Mode**

IPv6 access-list mode

**Applicability**

This command was introduced before OcNOS version 1.3.

**Examples**

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#200 permit sctp any any fragments
```

## ipv6 access-list tcp|udp

Use this command to define a IPv6 access control list (ACL) specification that determines whether to accept or drop an incoming IPv6 packet based on the criteria that you specify. This form of this command filters packets based on source and destination IPv6 address along with protocol (TCP or UDP) and port.

Use the **no** form of this command to remove an ACL specification.

**Note:** Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

### Command Syntax

```
(<1-268435453>|) (deny|permit) (tcp) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (X:X::X:X/
M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|
discard|domain|drip|echo|exec|finger|ftp |ftp-
data|gopher|hostname|ident|irc|klogin|kshell|login|lpd|nntp|pim-auto-
rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|uucp|whois|www)| (range <0-
65535> <0-65535>)| (fragments) |} ((dscp (<0-63>| af11| af12| af13| af21| af22|
af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7|
default|ef ))|) (flow-label <0-1048575>|)
({ack|established|fin|psh|rst|syn|urg}|)) (vlan <1-4094>|) (inner-vlan <1-
4094>|) (log|) (sample|)

(<1-268435453>|) (deny|permit) (tcp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
{(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|drip|
echo|exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|kshell
|login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
|time|uucp|whois|www)| (range <0-65535> <0-65535>)} (X:X::X:X/M|X:X::X:X
X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|
drip|echo|exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|kshell|
login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|
talk|telnet|time|uucp|whois|www)| (range <0-65535> <0-65535>)|} ((dscp (<0-
63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1|
cs2| cs3| cs4| cs5| cs6| cs7| default|ef ))|) (flow-label <0-1048575>|)
({ack|established|fin|psh|rst|syn|urg}|)) (vlan <1-4094>|) (inner-vlan <1-
4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|)

(<1-268435453>|) (deny|permit) (udp) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (X:X::X:X/
M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard
|dnsix|domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
ss|non500-isakmp|ntp|pim-auto-rp|snmp|snmptrap|sunrpc|syslog|
tacacs|talk|tftp|time|who|xnmcp)| (range <0-65535> <0-65535>)| (fragments) |}
((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42|
af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default|ef ))|) (flow-label <0-
1048575>|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|) (sample|) ((redirect-
to-port IFNAME)|)

(<1-268435453>|) (deny|permit) (udp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
{(eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard|dnsix
|domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
ss|non500-isakmp|ntp|pim-auto-rp|snmp|snmptrap|sunrpc|syslog|
tacacs|talk|tftp|time|who|xnmcp)| (range <0-65535> <0-65535>)} (X:X::X:X/
M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard|
dnsix|domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
ss|non500-isakmp|ntp|pim-auto-rp|snmp|snmptrap|sunrpc|
```

```

syslog|tacacs|talk|tftp|time|who|xmcpc) | (range <0-65535> <0-65535>) } ((dscp
<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43|
cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ))|) (flow-label <0-1048575>|)
(vlan <1-4094>|) (inner-vlan <1-4094>|) (log|) (sample|) ((redirect-to-port
IFNAME)|)

no (<1-268435453>|) (deny|permit) (tcp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
(X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|
daytime|discard|domain|drip|echo|exec|finger|ftp |ftp-data|gopher|hostname
|ident|irc|klogin|kshell|login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc
|tacacs|talk|telnet|time|uucp|whois|www) | (range <0-65535> <0-65535>)|
(fragments) |} (((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32|
af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ))|)
(flow-label <0-1048575>|) ({ack|established|fin|psh|rst|syn|urg|})) (vlan <1-
4094>|) (inner-vlan <1-4094>|) (log|) (sample|)

no (<1-268435453>|) (deny|permit) (tcp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
{(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|drip
|echo|exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|kshell
|login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
|time|uucp|whois|www) | (range <0-65535> <0-65535>)} (X:X::X:X/M|X:X::X:X
X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|
domain|drip|echo|exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|
kshell|login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk
|telnet|time|uucp|whois|www) | (range <0-65535> <0-65535>)|} (((dscp (<0-63>|
af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2|
cs3| cs4| cs5| cs6| cs7| default| ef ))|) (flow-label <0-1048575>|)
({ack|established|fin|psh|rst|syn|urg|})) (vlan <1-4094>|) (inner-vlan <1-
4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|)

no (<1-268435453>|) (deny|permit) (udp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
(X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-
65535>|biff|bootpc|bootps|discard|dnsix|domain|echo|isakmp|mobile-
ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|ntp|pim-auto-
rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xmcpc) | (range <0-
65535> <0-65535>) | (fragments) |} ((dscp (<0-63>| af11| af12| af13| af21| af22|
af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7|
default| ef ))|) (flow-label <0-1048575>|) (vlan <1-4094>|) (inner-vlan <1-
4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|)

no (<1-268435453>|) (deny|permit) (udp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
{(eq|gt|lt|neq) (<0-
65535>|biff|bootpc|bootps|discard|dnsix|domain|echo|isakmp|mobile-
ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|ntp|pim-auto-
rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xmcpc) | (range <0-
65535> <0-65535>) } (X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-
65535>|biff|bootpc|bootps|discard|dnsix|domain|echo|isakmp|mobile-
ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|ntp|pim-auto-
rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xmcpc) | (range <0-
65535> <0-65535>) } ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31|
af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ))|)
(flow-label <0-1048575>|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|)
(sample|) ((redirect-to-port IFNAME)|)

```

## Parameters

<1-268435453> IPv6 ACL sequence number.

deny	Drop the packet.
permit	Accept the packet.
tcp	Transmission Control Protocol.
udp	User Datagram Protocol.
X:X::X:X/M	Source or destination IPv6 prefix and length.
X:X::X:X X:X::X:X	Source or destination IPv6 address and mask.
host X:X::X:X	A single source or destination host IPv6 address.
any	Any source or destination IPv6 address.
eq	Source or destination port equal to.
gt	Source or destination port greater than.
lt	Source or destination port less than.
neq	Source or destination port not equal to.
<0-65535>	Source or destination port number.
range	Range of source or destination port numbers:
<0-65535>	Lowest value in the range.
<0-65535>	Highest value in the range.
ftp	File Transfer Protocol (21).
ssh	Secure Shell (22).
telnet	Telnet (23).
www	World Wide Web (HTTP 80).
tftp	Trivial File Transfer Protocol (69).
bootp	Bootstrap Protocol (BOOTP) client (67).
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Name Service.
drip	Dynamic Routing Information Protocol.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections.
gopher	Gopher.
hostname	NIC hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat.



---

klogin	Kerberos login.
kshell	Kerberos shell.
login	Login.
lpd	Printer service.
nnt	Network News Transport Protocol.
pim-auto-rp	PIM Auto-RP.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
smtp	Simple Mail Transport Protocol.
ssh	Secure Shell.
sunrpc	Sun Remote Procedure Call.
tacacs	TAC Access Control System.
talk	Talk.
telnet	Telnet.
time	Time.
uucp	UNIX-to-UNIX Copy Program.
whois	WHOIS/NICNAME
www	World Wide Web.
nntp	Range of source or destination port numbers:
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.

---

cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).
priority	Match packets with priority precedence (1).
routine	Match packets with routine precedence (0).
ack	Match on the Acknowledgment (ack) bit.
established	Matches only packets that belong to an established TCP connection.
fin	Match on the Finish (fin) bit.
psh	Match on the Push (psh) bit.
rst	Match on the Reset (rst) bit.
syn	Match on the Synchronize (syn) bit.
urg	Match on the Urgent (urg) bit.
biff	Biff.
bootpc	Bootstrap Protocol (BOOTP) client.
bootps	Bootstrap Protocol (BOOTP) server.
discard	Discard.
dnsix	DNSIX security protocol auditing.
domain	Domain Name Service.
echo	Echo.
isakmp	Internet Security Association and Key Management Protocol.
mobile-ip	Mobile IP registration.
nameserver	IEN116 name service.
netbios-dgm	Net BIOS datagram service.
netbios-ns	Net BIOS name service.
netbios-ss	Net BIOS session service.
non500-isakmp	Non500-Internet Security Association and Key Management Protocol.
ntp	Network Time Protocol.
pim-auto-rp	PIM Auto-RP.
snmp	Simple Network Management Protocol.
snmptrap	SNMP Traps.
sunrpc	Sun Remote Procedure Call.

---

syslog	System Logger.
tacacs	TAC Access Control System.
talk	Talk.
tftp	Trivial File Transfer Protocol.
time	Time.
who	Who service.
xmcp	X Display Manager Control Protocol.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).
flow-label	IPv6 Flow-label.
<0-1048575>	IPv6 Flow-label value.
fragments	Check non-initial fragments.
vlan	Match packets with given VLAN identifier.
<1-4094>	Enter VLAN identifier.
inner-vlan	Match packets with given inner VLAN identifier.
<1-4094>	Enter inner-VLAN identifier.
redirect-to-port	Redirect the packet (in-direction only)
IFNAME	Interface name to which packet to be redirected (switchport only)

## Command Mode

IPv6 access-list mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#deny udp any eq tftp
(config-ipv6-acl)#deny tcp fd22:bf66:78a4:10a2::/64 fd2:860a:746a:e49c::/64
eq ssh
```

---

## line vty

Use this command to move or change to ALL LINE VTY mode.

### Command Syntax

```
line vty
```

### Parameters

NA

### Command Mode

Configure mode

### Applicability

This command was introduced from OcNOS version 1.3.8

### Examples

The following example shows entering all line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty
(config-all-line)#exit
```

## mac access-group

Use this command to attach a MAC access list to an interface to filter incoming packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

The `time-range` parameter is optional. If used, the access-group is tied to the timer specified.

After the access-group has been configured with the time-range, to detach the access-group from the time-range, use the `no` form of this command with a time-range parameter as shown in the syntax and examples below.

To delete the access-group, use the `no` form of this command without a time-range.

**Note:** An access-group on egress access-group on egress direction uses the TCAM group used by the QoS output service policy. Therefore, actions are unpredictable when conflicting matches are configured on same interface. IP Infusion Inc. recommends avoiding such a configuration. Otherwise, you need to configure the priority (in QoS) or the sequence number (in ACL) carefully to handle such cases.

### Command Syntax

```
mac access-group NAME (in|out) (in|out) (time-range TR_NAME|)
no mac access-group NAME (in|out) (time-range TR_NAME|)
```

### Parameters

NAME	Access list name.
in	Filter incoming packets.
out	Filter outgoing packets
TR_NAME	Time range name set with the <a href="#">time-range</a> command

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3. The `time-range` parameter was added in OcNOS-SP version 5.0.

### Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)#permit any any
(config-mac-acl)#exit

(config)#hardware-profile filter ingress-l2-ext enable
```

```
(config)#interface xe3
(config-if)#mac access-group mylist in
(config-if)#exit
```

```
(config)#interface xe3
(config-if)#mac access-group mylist in time-range TIMER1
(config-if)#exit
```

```
(config)#interface xe3
(config-if)#no mac access-group mylist in time-range TIMER1
(config-if)#exit
```

```
(config)#interface xe3
(config-if)#no mac access-group mylist in
(config-if)#exit
```

---

## mac access-list

Use this command to define a MAC access control list (ACL) that determines whether to accept or drop an incoming packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Use the `no` form of this command to remove the ACL.

### Command Syntax

```
mac access-list NAME
no mac access-list NAME
```

### Parameters

NAME	Access-list name.
------	-------------------

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#exit
```

---

## mac access-list default

Use this command to modify the default rule action of access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the packets not matching any of the user defined rules match default rule.

### Command Syntax

```
default (deny-all|permit-all) (log|) (sample|)
```

### Parameters

deny-all	Drop all packets.
permit-all	Accept all packets.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).

### Command Mode

MAC access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#default permit-all sample
```



## mac access-list filter

Use this command to define an access control entry (ACE) in a MAC access control list (ACL) that determines whether to permit or deny packets with the given source and destination MAC, ethertype, CoS, and VLAN identifiers.

Use the `no` form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

**Note:** Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

### Command Syntax

```
(<1-268435453>|) (deny|permit) (any | (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (arp|appletalk|decnet-
iv|diagnostic|etype-6000|etype-8042 |ip4|ip6|mpls|lat|lavc-sca|mop-console|mop-
dump|vines-echo|WORD|) (cos <0-7>|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|)
(sample|)

no (<1-268435453>|) (deny|permit) (any | (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (arp|appletalk|decnet-
iv|diagnostic|etype-6000|etype-8042 |ip4|ip6|mpls|lat|lavc-sca|mop-console|mop-
dump|vines-echo|WORD|) (cos <0-7>|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|)
(sample|)

no (<1-268435453>)
```

### Parameters

<code>deny</code>	Drop the packet.
<code>permit</code>	Accept the packet.
<code>&lt;1-268435453&gt;</code>	IPv4 ACL sequence number.
<code>any</code>	Source/Destination any.
<code>XX-XX-XX-XX-XX-XX</code>	Source/Destination MAC address (Option 1).
<code>XX:XX:XX:XX:XX:XX</code>	Source/Destination MAC address (Option 2).
<code>XXXX.XXXX.XXXX</code>	Source/Destination MAC address (Option 3).
<code>XX-XX-XX-XX-XX-XX</code>	Source/Destination wildcard (Option1).

XX:XX:XX:XX:XX:XX	Source/Destination wildcard (Option2).
XXXX.XXXX.XXXX	Source/Destination wildcard (Option3).
host	A single source/destination host.
aarp	Ethertype - 0x80f3.
appletalk	Ethertype - 0x809b.
decnet-iv	Ethertype - 0x6003.
diagnostic	Ethertype - 0x6005.
etype-6000	Ethertype - 0x6000.
etype-8042	Ethertype - 0x8042.
ip4	Ethertype - 0x0800.
ip6	Ethertype - 0x86dd.
mpls	Ethertype - 0x8847.
lat	Ethertype - 0x6004.
lavc-sca	Ethertype - 0x6007.
mop-console	Ethertype - 0x6002.
mop-dump	Ethertype - 0x6001.
vines-echo	Ethertype - 0x0baf.
WORD	Any Ethertype value.
cos <0-7>	Cos value.
vlan <1-4094>	VLAN identifier.
inner-vlan <1-4094>	Inner-VLAN identifier.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).

### Command Mode

MAC access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#permit 0000.1234.1234 0000.0000.0000 any sample
```

---

## mac access-list remark

Use this command to add a description to an MAC access control list (ACL).

Use the `no` form of this command to remove an ACL description.

### Command Syntax

```
remark LINE
no remark
```

### Parameters

LINE                      ACL description up to 100 characters.

### Command Mode

MAC access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)# remark Permit the inside admin address
```

---

## mac access-list resequence

Use this command to modify the sequence numbers of MAC access list specifications.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

### Command Syntax

```
resequence <1-268435453> INCREMENT
```

### Parameters

<1-268435453>	Starting sequence number.
INCREMENT	Sequence number increment steps.

### Command Mode

MAC access-list mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)#resequence 15 15
```

---

## show access-lists

Use this command to display access lists.

### Command Syntax

```
show access-lists (NAME|) (expanded|summary|)
```

### Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show access-lists expanded
IP access list Iprule1
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
default deny-all
MAC access list Macrule1
10 permit host 0000.1234.1234 any
default deny-all
IPv6 access list ipv6-acl-01
10 deny ahp 3ffe::/64 4ffe::/64
default deny-all

#show access-lists summary
IPV4 ACL Iprule1
statistics enabled
Total ACEs Configured: 1
Configured on interfaces:
xe3/1 - egress (Router ACL)
Active on interfaces:
xe1/3 - ingress (Router ACL)
MAC ACL Macrule1
statistics enabled
Total ACEs Configured: 0
Configured on interfaces:
Active on interfaces:
IPV6 ACL ipv6-acl-01
statistics enabled
Total ACEs Configured: 2
Configured on interfaces:
xe7/1 - ingress (Router ACL)
Active on interfaces:
```

---

## show access-list log-cache

Use this command to show the ACL logging table entries

### Command Syntax

```
show access-lists log-cache
```

### Parameters

None

### Command Mode

Privileged Exec mode and Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show access-lists log-cache
2016 Oct 26 12:08:37:xe1/1: 0000.0100.0a00 -> 0000.0100.0b00, ethertype IP
(0x800), proto tcp, vlan 2, 0.0.0.0:0 -> 0.0.0.0:0 ...suppressed 11 times

2016 Oct 26 12:07:51:xe1/1: 0000.0100.0a00 -> 0000.0100.0b00, ethertype IP
(0x800), proto 255, vlan 2, 0.0.0.0 -> 0.0.0.0 ...suppressed 10 times
```

---

## show arp access-lists

Use this command to display ARP access lists.

### Command Syntax

```
show arp access-lists (NAME|) (expanded|summary|)
```

### Parameters

NAME	ARP access-list name.
expanded	Expanded access-list.
summary	Access-list summary.

### Command Mode

Privileged Exec mode and Exec mode

### Applicability

This command was introduced in OcNOS version 1.3.6.

### Example

```
#show arp access-lists
ARP access list arp1
    remark "arp access-list created"
    10 permit ip any mac any
```

---

## show ip access-lists

Use this command to display IP access list

### Command Syntax

```
show ip access-lists (NAME|) (expanded|summary|)
```

### Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show ip access-lists
IP access list Iprule2
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
12 deny ip 30.0.0.2 0.0.0.255 182.124.0.3/24
default deny-all
```

```
#show ip access-lists summary
IPV4 ACL Iprule3
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa1 - ingress (Port ACL)
sa3 - ingress (Router ACL)
sa8 - ingress (Port ACL)
vlan1.3 - ingress (Router ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
xe3/1 - egress (Router ACL)
Active on interfaces:
sa1 - ingress (Port ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```



---

## show ipv6 access-lists

Use this command to display IPv6 access lists.

### Command Syntax

```
show ipv6 access-lists (NAME|) (expanded|summary|)
```

### Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

### Command Mode

Privileged Exec mode and Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show ipv6 access-lists
IPv6 access list ipv6-acl-01
10 deny ahp 3ffe::/64 4ffe::/64
20 permit ahp 78fe::1/48 68fe::1/48
30 permit ahp 3333::1/64 4444::1/48 fragments
40 permit ahp 5555::1/64 4444::1/48 dscp af23
default deny-all
```

```
#show ipv6 access-lists summary
IPV6 ACL ipv6-acl-01
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa3 - ingress (Router ACL)
vlan1.3 - ingress (Router ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
Active on interfaces:
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```

---

## show mac access-lists

Use this command to display MAC access lists.

### Command Syntax

```
show mac access-lists (NAME|) (expanded|summary|)
```

### Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

### Command Mode

Privileged exec mode and exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show mac access-lists
MAC access list Macrule2
default deny-all
MAC access list Macrule3
10 permit host 0000.1234.1234 any
20 deny host 1111.1111.AAAA any 65535
30 permit host 2222.2222.AAAA any 65535
40 permit 0000.3333.3333 0000.0000.FFFF 4444.4444.4444 0000.0000.FFFF
default deny-all [match=1126931077]

# show mac access-lists summary
MAC ACL Macrule3
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa3 - ingress (Router ACL)
sa8 - ingress (Port ACL)
vlan1.3 - ingress (Router ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
Active on interfaces:
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```

---

## show running-config aclmgr

Use this command to display the entire access list configurations along with the attachment to interfaces.

### Command Syntax

```
show running-config aclmgr (all|)
```

### Parameters

all                      Show running configuration with defaults.

### Command Mode

Exec mode and privileged exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show running-config aclmgr
ip access-list ip-acl-01
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
12 deny ip 30.0.0.2 0.0.0.255 182.124.0.3/24
mac access-list mac-acl-01
10 permit host 0000.1234.1234 any
20 permit host 0000.1111.AAAA any ipv4 cos 3 vlan 3
!
ipv6 access-list ipv6-acl-01
10 deny ipv6 3ffe::/64 4ffe::/64 dscp af43
20 permit ipv6 78fe::/64 68fe::/64 dscp cs3
!
interface xel/1
ip access-group ip-acl-01 in
!
```

---

## show running-config access-list

Use this command to show the running system status and configuration details for MAC and IP access lists.

### Command Syntax

```
show running-config access-list
```

### Parameters

None

### Command Mode

Privileged exec mode, configure mode, and route-map mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show running-config access-list
ip access-list abd
10 deny any any any
!
mac access-list abc
remark test
10 deny any any
!
```

---

## show running-config ipv6 access-list

Use this command to show the running system status and configuration details for IPv6 access lists.

### Command Syntax

```
show running-config ipv6 access-list
```

### Parameters

None

### Command Mode

Privileged exec mode, configure mode, and route-map mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show running-config ipv6 access-list
ipv6 access-list test
10 permit any any any
!
```



---

## CHAPTER 3 Authentication, Authorization and Accounting

---

This chapter is a reference for the authentication:

- Authentication identifies users by challenging them to provide a user name and password. This information can be encrypted if required, depending on the underlying protocol.
- Authorization provides a method of authorizing commands and services on a per user profile basis.

Note: Authorization will be auto-enabled if user enables the Authentication.

- Accounting collects detailed system and command information and stores it on a central server where it can be used for security and quality assurance purposes.

The authentication feature allows you to verify the identity and, grant access to managing devices. The authentication feature works with the access control protocols as described in these chapters:

- [Chapter 19, RADIUS](#)
- [Chapter 26, TACACS+](#)

Note: Only network administrators can execute these commands. For more, see the [username](#) command.

Note: The commands below are supported only on the “management” VRF.

Note: Per-command authorization needs to be enabled explicitly by the user whereas Session based authorization will be implicitly enabled when user enables authentication.

This chapter describes these commands:

- [aaa authentication login](#)
- [aaa accounting default](#)
- [aaa authentication login console](#)
- [aaa authentication login default](#)
- [aaa authorization default](#)
- [aaa authentication login console fallback error](#)
- [aaa authentication login default fallback error](#)
- [aaa group server](#)
- [aaa local authentication attempts max-fail](#)
- [aaa local authentication unlock-timeout](#)
- [debug aaa](#)
- [server](#)
- [show aaa authentication](#)
- [show aaa authentication login](#)
- [show aaa authorization](#)
- [show aaa groups](#)
- [show aaa accounting](#)
- [show running-config aaa](#)

---

## aaa authentication login

Use this command to set login authentication behavior.

Use the `no` form of this command to disable either authentication behavior.

### Command Syntax

```
aaa authentication login error-enable (vrf management|)
no aaa authentication login error-enable (vrf management|)
```

### Parameters

<code>error-enable</code>	Display login failure messages
<code>management</code>	Management VRF

### Default

By default, aaa authentication login is local

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#aaa authentication login error-enable vrf management
```



---

## aaa accounting default

Use this command to set a list of server groups to which to redirect accounting logs.

Use the `no` form of this command to only log locally.

### Command Syntax

```
aaa accounting default (vrf management|) ((group LINE)|local)
no aaa accounting default (vrf management|) ((group)|local)
```

### Parameters

<code>group</code>	Server group list for authentication
<code>LINE</code>	A space-separated list of up to 8 configured RADIUS or TACACS+ server group names
<code>local</code>	Use local authentication
<code>management</code>	Management VRF

### Default

Default AAA method is local

Default groups: RADIUS or TACACS+

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#aaa accounting default vrf management group radius
```

---

## aaa authentication login console

Use this command to set the AAA authentication methods for console log ins.

Use the `no` form of this command to set the default AAA authentication method (`local`).

### Command Syntax

```
aaa authentication login console ((group LINE) | (local (|none)) | (none))
no aaa authentication login console ((group LINE) | (local (|none)) | (none))
```

### Parameters

<code>group</code>	Use a server group list for authentication
<code>LINE</code>	Specify a space-separated list of up to 8 configured RADIUS or TACACS+ server group names followed by <code>local</code> or <code>none</code> or both <code>local</code> and <code>none</code> . The list can also include:
<code>radius</code>	All configured RADIUS servers
<code>tacacs+</code>	All configured TACACS+ servers
<code>local</code>	Use local authentication
<code>none</code>	No authentication

### Default

Default AAA authentication method is `local`

Default groups: RADIUS or TACACS+

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#aaa authentication login console group radius
```

---

## aaa authentication login default

Use this command to set the AAA authentication methods.

Use the `no` form of this command to set the default AAA authentication method (`local`).

### Command Syntax

```
aaa authentication login default (vrf management|) ((group LINE) | (local (|none))
| (none))
no aaa authentication login default (vrf management|) ((group) | (local (|none)) |
(none))
```

### Parameters

<code>group</code>	Use a server group list for authentication
<code>LINE</code>	A space-separated list of up to 8 configured RADIUS or TACACS+, server group names followed by <code>local</code> or <code>none</code> or both <code>local</code> and <code>none</code> . The list can also include:
<code>radius</code>	All configured RADIUS servers
<code>tacacs+</code>	All configured TACACS+ servers
<code>local</code>	Use local authentication
<code>none</code>	No authentication
<code>management</code>	Management VRF

### Default

By default, AAA authentication method is `local`

By default, groups: RADIUS or TACACS+

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#aaa authentication login default vrf management group radius
```

---

## aaa authorization default

Use this command to enable per-command authorization. By enabling this user should be able to authorize every command executed via configured server.

This authorization will work only when authentication is successful.

Use the no form of this command to disable authorization.

### Command Syntax

```
aaa authorization default (vrf management|) ((group LINE)|local)
no aaa authorization default (vrf management|) ((group LINE)|local)
```

### Parameters

group	Server group list for authentication
LINE	Space-separated list of up to 8 configured TACACS+ server group names
local	Use local authentication
management	Management VRF

### Default

Default AAA method is local

Default groups: TACACS+

### Command Mode

Configure mode

### Applicability

This command is introduced in OcNOS version 6.1.0

### Examples

```
#configure terminal
(config)#aaa authorization default vrf management group tacacs+
```

---

## aaa authentication login console fallback error

Use this command to enable fallback to local authentication for the console login if remote authentication is configured and all AAA servers are unreachable.

Use the `no` form of this command to disable fallback to local authentication.

### Command Syntax

```
aaa authentication login console fallback error local
no aaa authentication login console fallback error local
```

### Parameters

None

### Default

By default, AAA authentication is local

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#aaa authentication login console fallback error local
```

---

## aaa authentication login default fallback error

Use this command to enable fallback to local authentication for the default login if remote authentication is configured and all AAA servers are unreachable.

Use the `no` form of this command to disable fallback to local authentication.

Note: If you have specified `local` (use local authentication) in the [aaa authentication login default](#) command, you do not need to use this command to ensure that “fall back to local” occurs.

### Command Syntax

```
aaa authentication login default fallback error local (vrf management|)
no aaa authentication login default fallback error local (vrf management|)
```

### Parameters

<code>management</code>	Management VRF
-------------------------	----------------

### Default

By default, AAA authentication is local.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#aaa authentication login default fallback error local vrf management
```

---

## aaa group server

Use this command to create a server group and enter server group configuration mode.

Use the `no` form of this command to remove a server group.

### Command Syntax

```
aaa group server (radius|tacacs+) WORD (vrf management|)
no aaa group server (radius|tacacs+) WORD (vrf management|)
```

### Parameters

radius	RADIUS server group
tacacs+	TACACS+ server group
WORD	Server group name; maximum 127 characters
management	Management VRF

### Default

By default, the AAA group server option is disabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#aaa group server radius maxsmart
(config-radius)#
```

---

## aaa local authentication attempts max-fail

Use this command to set the number of unsuccessful authentication attempts before a user is locked out.

Use the `no` form of this command to disable the lockout feature.

### Command Syntax

```
aaa local authentication attempts max-fail <1-25>
no aaa local authentication attempts max-fail
```

### Parameters

<1-25>	Number of unsuccessful authentication attempts
--------	--

### Default

By default, the maximum number of unsuccessful authentication attempts before a user is locked out is 3.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#aaa local authentication attempts max-fail 2
```



---

## aaa local authentication unlock-timeout

Use this command to set timeout value in seconds to unlock local user-account.

Use the no form of this command to set default timeout value in seconds.

Note: This command is applicable only to local user but not for user/s present at the server end to authenticate using TACACS+ or RADIUS.

### Command Syntax

```
aaa local authentication unlock-timeout <1-3600>
no aaa local authentication unlock-timeout
```

### Parameters

<1-3600>                      Timeout in seconds to unlock local user-account. Default value is 1200.

### Default

By default, the unlock timeout is 1200 seconds

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#aaa local authentication unlock-timeout 1800
```

---

## debug aaa

Use this command to display AAA debugging information.

Use the `no` form of this command to stop displaying AAA debugging information.

### Command Syntax

```
debug aaa
```

```
no debug aaa
```

### Parameters

None

### Command Mode

Executive mode and configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#debug aaa
```

---

## server

Use this command to add a server to a server group.

Use the `no` form of this command to remove from a server group.

### Command Syntax

```
server (A.B.C.D | X:X::X:X | HOSTNAME)
no server (A.B.C.D | X:X::X:X | HOSTNAME)
```

### Parameters

A.B.C.D	IPv4 address
X:X::X:X	IPv6 address

### Default

None

### Command Modes

RADIUS server group configure mode

TACACS+ server group configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#feature tacacs+
(config)#aaa group server tacacs+ TacacsGroup4
(config-tacacs)#server 203.0.113.127
```

# show aaa authentication

Use this command to display AAA authentication configuration.

## Command Syntax

```
show aaa authentication (|vrf(management|all))
```

## Parameters

None

## Command Modes

Executive mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show aaa authentication
VRF: default
default: local
console: local
```

[Table 3-6](#) explains the output fields.

Table 3-6: show aaa authentication fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Default	Displays the aaa authentication method list.
Console	Authentication setting for the console access.

---

## show aaa authentication login

Use this command to display AAA authentication configuration for login default and login console.

### Command Syntax

```
show aaa authentication login error-enable (|vrf management|all))
```

### Parameters

error-enable	Display setting for login failure messages
vrf	Management VRF or all VRFs

### Command Modes

Executive mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show aaa authentication login error-enable  
  
VRF: default  
  
disabled
```

[Table 3-7](#) explains the output fields.

**Table 3-7: show aaa authentication login error-enable fields**

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.

---

## show aaa authorization

Use this command to display AAA authorization configuration.

### Command Syntax

```
show aaa authorization (|vrf(management|all))
```

### Parameters

vrf management	Authorization configs present in Management VRF
vrf all	Authorization configs present in all VRFs

### Command Modes

Executive mode

### Applicability

This command is introduced in OcNOS version 6.1.0.

### Examples

```
#show aaa authorization
VRF: default
default: group tacacs+
```

---

## show aaa groups

Use this command to display AAA group configuration.

### Command Syntax

```
show aaa groups (vrf (management|all)|)
```

### Parameters

vrf                      Management VRF or all VRFs

### Command Modes

Executive mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show aaa groups
VRF: default
radius
```

[Table 3-8](#) explains the output fields.

**Table 3-8: show aaa groups fields**

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.

# show aaa accounting

Use this command to display AAA accounting configuration.

## Command Syntax

```
show aaa accounting (vrf (management|all)|)
```

## Parameters

vrf                      Management VRF or all VRFs

## Command Modes

Executive mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show aaa accounting
VRF: default
default: group tacacs+
```

[Table 3-9](#) explains the output fields.

Table 3-9: show aaa accounting fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.



---

## show running-config aaa

Use this command to display AAA settings in the running configuration.

### Command Syntax

```
show running-config aaa (vrf(management|all)|)
```

### Parameters

vrf                      Management VRF or all VRFs

### Command Modes

Executive mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show aaa accounting
```

```
    VRF: default
```

```
default: local
```

[Table 3-10](#) explains the output fields.

**Table 3-10: show aaa accounting fields**

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Default	Displays the aaa authentication method list.



---

## CHAPTER 4 Basic Commands

---

This chapter describes basic commands.

- `banner motd`
- `clock timezone`
- `clock set`
- `configure terminal`
- `configure terminal force`
- `copy running-config startup-config`
- `crypto pki generate rsa common-name ipv4`
- `debug nsm`
- `disable`
- `do`
- `enable`
- `enable password`
- `end`
- `exec-timeout`
- `exit`
- `help`
- `history`
- `hostname`
- `line console`
- `line vty (all line mode)`
- `line vty (line mode)`
- `logging cli`
- `logout`
- `max-session`
- `ping`
- `ping (interactive)`
- `quit`
- `reload`
- `service advanced-vty`
- `service password-encryption`
- `service terminal-length`
- `show clock`
- `show cli`
- `show cli history`
- `show crypto csr`

- `show debugging nsm`
- `show list`
- `show logging cli`
- `show nsm client`
- `show nsm forwarding-timer`
- `show process`
- `show running-config`
- `show startup-config`
- `show timezone`
- `show users`
- `show version`
- `sys-reload`
- `sys-shutdown`
- `terminal length`
- `terminal monitor`
- `traceroute`
- `write`
- `write terminal`

---

## banner motd

Use this command to set the message of the day (motd) at login.

After giving this command, you must write to memory using the [write](#) command. If you do not write to memory, the new message of the day is not available after the device reboots.

Use the `no` parameter to not display a banner message at login.

### Command Syntax

```
banner motd LINE
banner motd default
no banner motd
```

### Parameters

LINE	Custom message of the day.
default	Default message of the day.

### Default

By default, the following banner is displayed after logging in:

```
OcNOS version 1.3.4.268-DC-MPLS-ZEBM 09/27/2018 13:44:22
```

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#banner motd default

#configure terminal
(config)#no banner motd
```

---

## clock timezone

Use this command to set the system time zone.

Use `no` form of this command to set the default system time zone (UTC).

### Command Syntax

```
clock timezone (WORD)
no clock timezone
```

### Parameters

`WORD` Timezone name. Use [show timezone](#) to get the list of city names.

### Default

By default, system time zone is UTC

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
(config)#clock timezone Los_Angeles
```

---

## clock set

Use this command to set the system time manually.

### Command Syntax

```
clock set <time> <day> <month> <year>
```

### Parameters

TIME	Time of the day.
DAYS	Specify the day
MONTH	Month of the year
YEAR	Specify the Year

### Examples

```
OcNOS#clock set 18:30:00 13 january 2021
18:30:00 UTC Wed Jan 13 2021
```

---

## configure terminal

Use this command to enter configure mode.

### Command Syntax

```
configure terminal
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

The following example shows entering configure mode (note the change in the command prompt).

```
#configure terminal
(config) #
```



---

## configure terminal force

Use the configure terminal force command to kick out the configure command mode to privileged EXEC mode, iff there is any session already in configure command mode.

Note: Configure terminal force with option 0 or without any option indicates immediate kick out the session which is locked to configure command mode. similarly, configure terminal force with option of any value indicates session locked to configure command mode will be exited to privileged Exec mode after the specified number of seconds completed.

### Command Syntax

```
configure terminal force <0-600|>
```

### Parameters

<0-600>                      Timeout value in seconds for the session in config mode to exit to Privileged

### Default

No default value is specified

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal force 0
(config)#
```

---

## copy running-config startup-config

Use this command to write the configuration to the file used at startup. This is the same as the [write](#) command.

### Command Syntax

```
copy running-config startup-config
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#copy running-config startup-config
Building configuration...
[OK]
#
```

## crypto pki generate rsa common-name ipv4

Use this command to generate a private key and Certificate Signing Request (CSR) which are required for OcNOS to establish a Transport Layer Security (TLS) connection with a NetConf client.

### Command Syntax

```
crypto pki generate rsa common-name ipv4 IPv4ADDR
```

### Parameters

IPv4ADDR	IPv4 address for the Common Name field of the CSR
----------	---

### Default

N/A

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#crypto pki generate rsa common-name ipv4 7.7.7.7
#show crypto csr
-----BEGIN CERTIFICATE REQUEST-----
MIICVzCCAT8CAQAwEjEQMA4GA1UEAwHNy43LjcuNzCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMkzIZaxNYPd8PW0hexecUFKq9pJn5IJzJkOQDtoVFOT
zeLPRxBaOt1NVd+1EF+wy3AgnGMw004g4AP7qaE+S5X1vKGAjagt fh/gfDAPDUtM
CpYLMCACM7n76OmyP9eUpkMbOSPkZDIBZfjUMxDTFwkzCBH+BF6SkSxtA24NUA9z
5heCIb1ArXYjdlIeB+9FfiVdOZ5yxQsLY8604ONL7Upl766SArGQo6oZ1dJ+bc91
sQVCEpF40SdCNn+Uw3R0cPfQF81BJD4H0EHf1VnHtYJwQ1yax6qc5ghT9R/rABDa
BFB3R09QpjV4Ihd/MyrdQmEIoxHeNNvSGDj9+eiEpksCAwEAAaAAMA0GCSqGSIb3
DQEBCwUAA4IBAQAwwXkQmNf3yiL+pmpwvE+gU8KVp3i4cvD13Vjh7IQMkCT47WPam
DUiYgwk+dPVAI+iWZq4qTvUNn6xahOyN5rnkTz9eipsQ1YHPpZB7hj5fimWwzJws
m4Tun0GZieEBCROqUpbuW+6QDvtR3XSzHhdGGSIteZv9cYyKhNu007okwr67c2Ea
11b7PcultOb4wj3xjqaO/ENDG+nmdUPaIKZrAwf2fEOarOaHgKwcl1AHHbusbJWL
qH0fAlOyVgfvG/WuCPP6Peg/Cpla7bDWqeGYt9vFTtekKoomQLzJwl6oINbtBCcw
DZJpeaQpUhFm+ZOjwibZ5NGPBRSTuYncp5xJ
-----END CERTIFICATE REQUEST-----
#
```

---

## debug nsm

Use this command to enable NSM debugging.

Use the `no` form of this command or the `undebug` command to disable NSM debugging.

### Command Syntax

```
debug nsm (all|)
```

```
no debug nsm (all|)
```

```
undebug nsm (all|)
```

```
debug nsm bfd
```

```
no debug nsm bfd
```

```
undebug nsm bfd
```

```
debug nsm events
```

```
no debug nsm events
```

```
undebug nsm events
```

```
debug nsm hal (all|) debug
```

```
debug nsm hal events
```

```
no debug nsm hal (all|)
```

```
no debug nsm hal events
```

```
undebug nsm hal events
```

```
debug nsm packet (recv|send|) (detail|)
```

```
no debug nsm packet (recv|send|) (detail|)
```

```
undebug nsm packet (recv|send|) (detail|)
```

### Parameters

<code>all</code>	Enable all debugging.
<code>bfd</code>	Debug BFD events.
<code>events</code>	Debug NSM events.
<code>hal</code>	Debug HAL.
<code>events</code>	Debug HAL events.
<code>packet</code>	Debug packet events.
<code>recv</code>	Debug received packets.
<code>send</code>	Debug sent packets.
<code>detail</code>	Show detailed packet information.

**Default**

By default, debugging is disabled.

**Command Mode**

Exec mode, privileged exec mode, and configure mode

**Applicability**

This command was introduced before OcNOS version 1.3.

**Examples**

```
#debug nsm all
#
#debug nsm bfd
#
#debug nsm events
#
#debug nsm hal all
#
#debug nsm packet
#
#debug nsm packet recv detail
```

---

## disable

Use this command from to exit privileged exec mode and return to exec mode. This is the only command that allows you to go back to exec mode. The [exit](#) or [quit](#) commands in privileged exec mode end the session without returning to exec mode.

### Command Syntax

```
disable
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#disable  
>
```

## do

Use this command to run several exec mode or privileged exec mode commands from configure mode. The commands that can be run from configure mode using **do** are: **show**, **clear**, **debug**, **ping**, **traceroute**, **write**, and **no debug**.

**Note:** The **do** command supports only the following CLI commands only

### Command Syntax

```
do LINE
```

### Parameters

LINE                      Command and its parameters.

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
#(config)#do show interface
Interface lo
  Hardware is Loopback index 1 metric 1 mtu 16436 duplex-half arp ageing
  timeout 25
  <UP, LOOPBACK, RUNNING>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet 4.4.4.40/32 secondary
  inet 127.0.0.1/8
  inet6 ::1/128
  Interface Gifindex: 3
  Number of Data Links: 0
  GMPLS Switching Capability Type:
    Packet-Switch Capable-1 (PSC-1)
  GMPLS Encoding Type: Packet
  Minimum LSP Bandwidth 0
    input packets 10026, bytes 730660, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 10026, bytes 730660, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
#
```

---

## enable

Use this command to enter privileged exec command mode.

### Command Syntax

```
enable
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

The following example shows entering the Privileged Exec mode (note the change in the command prompt).

```
>enable  
#
```



---

## enable password

Use this command to change or create a password to use when entering enable mode.

Note: Only network administrators can execute this command. For more, see the [username](#) command.

There are two methods to enable a password:

- Plain Password: a clear text string that appears in the configuration file.
- Encrypted Password: An encrypted password does not display in the configuration file; instead, it displays as an encrypted string. First, use this command to create a password. Then, use the [service password-encryption](#) command to encrypt the password.

Use the `no` parameter to disable the password.

### Command Syntax

```
enable password LINE
no enable password
no enable password LINE
```

### Parameters

<code>line</code>	Password string, up to 8 alpha-numeric characters, including spaces. The string cannot begin with a number.
-------------------	---

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#enable password mypasswd
```

---

## end

Use this command to return to privileged exec command mode from any other advanced command mode.

### Command Syntax

```
end
```

### Parameters

None

### Default

No default value is specified

### Command Mode

All command modes

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

The following example shows returning to privileged exec mode directly from interface mode.

```
#configure terminal
(config)#interface eth0
(config-if)#exit
#
```

---

## exec-timeout

Use this command to set the interval the command interpreter waits for user input detected. That is, this sets the time a telnet session waits for an idle VTY session before it times out. A value of zero minutes and zero seconds (0 and 0) causes the session to wait indefinitely.

Use the `no` parameter to disable the wait interval.

### Command Syntax

```
exec-timeout <0-35791> (<0-2147483>|)  
no exec-timeout
```

### Parameters

<0-35791>	Timeout value in minutes.
<0-2147483>	Timeout value in seconds.

### Default

No default value is specified

### Command Mode

Line mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

In the following example, the telnet session will timeout after 2 minutes, 30 seconds if there is no response from the user.

```
Router#configure terminal  
Router(config)#line vty 23 66  
Router(config-line)#exec-timeout 2 30
```

---

## exit

Use this command to exit the current mode and return to the previous mode. When used in exec mode or privileged exec mode, this command terminates the session.

### Command Syntax

```
exit
```

### Parameters

None

### Default

No default value is specified

### Command Mode

All command modes

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

The following example shows exiting interface mode and returning to configure mode.

```
#configure terminal
(config)#interface eth0
(config-if)#exit
(config)#
```

---

## help

Use this command to display help for the OcNOS command line interface.

### Command Syntax

```
help
```

### Parameters

None

### Default

No default value is specified

### Command Mode

All command modes

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.
```

If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show ve?'.)

---

## history

Use this command to set the maximum number of commands stored in the command history.

Use the `no` parameter to remove the configuration.

### Command Syntax

```
history max <0-2147483647>
no history max
```

### Parameters

<0-2147483647> Number of commands.

### Default

No default value is specified

### Command Mode

Line mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#line vty 12 77
(config-line)#history max 123

(config-line)#no history max
```

---

## hostname

Use this command to set the network name for the device. OcNOS uses this name in system prompts and default configuration filenames.

Setting a host name using this command also sets the host name in the kernel.

**Note:** After giving the `hostname` command, you must write to memory using the [write](#) command. If you do not write to memory, the change made by this command (the new host name) is not set after the device reboots.

Use the `no` parameter to disable this function.

### Command Syntax

```
hostname WORD
no hostname (WORD|)
```

### Parameter

WORD	Network name for a system. Per RFC 952 and RFC 1123, a host name string can contain only the special characters period (".") and hyphen ("-"). These special characters cannot be at the start or end of a host name.
------	---

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#hostname ABC
(config)#

(config)#no hostname
(config)#exit
```

---

## line console

Use the this command to move or change to the line console mode.

### Command Syntax

```
line console <0-0>
```

### Parameters

<0-0>                      First line number.

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

This example enters line mode (note the change in the prompt).

```
#configure terminal
(config)#line console 0
(config-line)#
```



---

## line vty (all line mode)

Use this command to move or change to “all lin”e VTY mode.

### Command Syntax

```
line vty
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 1.3.8.

### Example

The following example shows entering all line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty
(config-all-line)#exit
(config)#
```

---

## line vty (line mode)

Use this command to move or change to VTY mode. This command is used to connect to a protocol daemon. This configuration is necessary for any session. This configuration should be in the daemon's config file before starting the daemon.

Use the `no` parameter to disable this command.

### Command Syntax

```
line vty <0-871> <0-871>
no line vty <0-871> (<0-871>|)
```

### Parameters

<0-871>	Specify the first line number.
<0-871>	Specify the last line number.

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

The following example shows entering line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty 9
(config-line)#exit
(config)no line vty 9
```

---

## logging cli

Use this command to enable logging commands entered by all users.

Use the `no` parameter to disable logging commands entered by all users.

### Command Syntax

```
logging cli
no logging cli
```

### Parameter

None

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#logging cli
(config)#no logging cli
```

---

## logout

Use this command to exit the OcNOS shell.

### Command Syntax

```
logout
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Exec mode and privileged exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

```
>logout
OcNOS login:

>enable
en#logout
>
```

---

## max-session

Use this command to set maximum VTY session limit.

Use `no` form of this command to unset session-limit.

User can configure session-limit for Telnet and SSH sessions separately but this max-session parameter value takes the precedence to restrict the maximum number of sessions. If user configured this max-session to be 4, then the device would allow only maximum of 4 SSH and Telnet sessions collectively irrespective of the individual SSH and Telnet max-session configuration. Active sessions won't be disturbed even if the configured max-session limit is lesser than the current active sessions.

### Command syntax

```
max-session <1-40>
```

### Parameters

<1-40>	Number of sessions
--------	--------------------

### Default

By default, 40 sessions are allowed.

### Command Mode

Line mode

### Applicability

This command is introduced in OcNOS-DC version 5.0

### Example

In the following example max-session is configured as 4, thus the device would allow only 4 management sessions of SSH and Telnet collectively.

```
Router#configure terminal
Router(config)#line vty 23 66
Router(config-line)#max-session 4
```

---

## ping

Use this command to send echo messages to another host.

### Command Syntax

```
ping WORD (vrf (NAME|management))
ping ip WORD (vrf (NAME|management))
ping ipv6 WORD (|IFNAME)
ping ipv6 WORD (|IFNAME) (vrf (NAME|management))
```

### Parameters

WORD	Destination address (in A.B.C.D format for IPv4 or X:X::X:X for IPv6) or host name.
vrf	Virtual Routing and Forwarding instance.
NAME	Virtual Routing and Forwarding name.
management	Virtual Routing and Forwarding name.
ip	IPv4 echo.
WORD	Destination address in A.B.C.D format or host name.
ipv6	IPv6 echo.
WORD	Destination address in X:X::X:X format or host name.
IFNAME	Name of the interface.

### Default

No default value is specified

### Command Mode

Privileged exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
>enable
#ping 20.20.20.1 vrf management
Press CTRL+C to exit
PING 20.20.20.1 (20.20.20.1) 56(84) bytes of data.
64 bytes from 20.20.20.1: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 20.20.20.1: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 20.20.20.1: icmp_seq=3 ttl=64 time=0.033 ms
64 bytes from 20.20.20.1: icmp_seq=4 ttl=64 time=0.034 ms
64 bytes from 20.20.20.1: icmp_seq=5 ttl=64 time=0.034 ms
64 bytes from 20.20.20.1: icmp_seq=6 ttl=64 time=0.036 ms
64 bytes from 20.20.20.1: icmp_seq=7 ttl=64 time=0.036 ms
64 bytes from 20.20.20.1: icmp_seq=8 ttl=64 time=0.036 ms

--- 20.20.20.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6999ms
```

```
rtt min/avg/max/mdev = 0.032/0.034/0.036/0.006 ms
```

```
#ping ipv6 3001:db8:0:1::129 vrf management
```

```
Press CTRL+C to exit
```

```
PING 3001:db8:0:1::129(3001:db8:0:1::129) 56 data bytes
```

```
64 bytes from 3001:db8:0:1::129: icmp_seq=1 ttl=64 time=0.038 ms
```

```
64 bytes from 3001:db8:0:1::129: icmp_seq=2 ttl=64 time=0.047 ms
```

```
64 bytes from 3001:db8:0:1::129: icmp_seq=3 ttl=64 time=0.047 ms
```

```
64 bytes from 3001:db8:0:1::129: icmp_seq=4 ttl=64 time=0.049 ms
```

```
64 bytes from 3001:db8:0:1::129: icmp_seq=5 ttl=64 time=0.044 ms
```

```
64 bytes from 3001:db8:0:1::129: icmp_seq=6 ttl=64 time=0.048 ms
```

```
64 bytes from 3001:db8:0:1::129: icmp_seq=7 ttl=64 time=0.046 ms
```

```
64 bytes from 3001:db8:0:1::129: icmp_seq=8 ttl=64 time=0.048 ms
```

```
--- 3001:db8:0:1::129 ping statistics ---
```

```
8 packets transmitted, 8 received, 0% packet loss, time 6999ms
```

---

## ping (interactive)

Use this command to send echo messages to another host interactively. You are prompted with options supported by the command.

### Command Syntax

```
ping
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
>enable
#ping
Protocol [ip]:
Target IP address: 20.20.20.1
Name of the VRF : management
Repeat count [5]: 6
Time Interval in Sec [1]: 2.2
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Ping Broadcast? Then -b [n]:
PING 20.20.20.1 (20.20.20.1) 100(128) bytes of data.
108 bytes from 20.20.20.1: icmp_seq=1 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=2 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=3 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=4 ttl=64 time=0.036 ms
108 bytes from 20.20.20.1: icmp_seq=5 ttl=64 time=0.037 ms
108 bytes from 20.20.20.1: icmp_seq=6 ttl=64 time=0.034 ms

--- 20.20.20.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 11000ms
rtt min/avg/max/mdev = 0.034/0.036/0.038/0.007 ms

#ping
Protocol [ip]: ipv6
Target IP address: 3001:db8:0:1::129
Name of the VRF : management
Repeat count [5]:
Time Interval in Sec [1]:
Datagram size [100]:
```



```

Timeout in seconds [2]:
Extended commands [n]:
PING 3001:db8:0:1::129(3001:db8:0:1::129) 100 data bytes
108 bytes from 3001:db8:0:1::129: icmp_seq=1 ttl=64 time=0.050 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=2 ttl=64 time=0.047 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=3 ttl=64 time=0.042 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=4 ttl=64 time=0.048 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=5 ttl=64 time=0.051 ms

--- 3001:db8:0:1::129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.042/0.047/0.051/0.008 ms

```

The input prompts are described in [Table 4-11](#):

**Table 4-11: ping output fields**

Protocol [ip]	IPv4 or IPv6. The default is IPv4 if not specified.
Target IP address	IPv4 or IPv6 address or host name.
Name of the VRF	Name of the Virtual Routing and Forwarding instance.
Repeat count [5]	Number of ping packets to send. The default is 5 if not specified.
Time Interval in Sec [1]	Time interval between two ping packets. The default is 1 second if not specified.
Datagram size [100]	Ping packet size. The default is 100 bytes if not specified.
Timeout in seconds [2]	Time to wait for ping reply. The default is 2 seconds if not specified.
Extended commands [n]	Options for extended ping. The default is “no”.
Source address or interface	Source address or interface.
Type of service [0]	Types of service. The default is 0 if not specified.
Set DF bit in IP header? [no]	Do not fragment bit. The default value is “no” if not specified.
Data pattern [0xABCD]	Specify a pattern.
Ping Broadcast? Then -b [n]	Broadcast ping. The default is “no”. For a broadcast address, the value should be “y”.

---

## quit

Use this command to exit the current mode and return to the previous mode. When this command is executed in one of the exec modes, it closes the shell and logs you out.

### Command Syntax

```
quit
```

### Parameters

None

### Default

No default value is specified

### Command Mode

All modes

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#interface eth1
(config-if)#quit
(config)#
```

```
>enable
#quit
[root@TSUP-123 sbin]#
```

---

## reload

Use this command to shut down the device and perform a cold restart. You call this command when:

- You detect a configuration issue such as `show running-config` displaying a configuration but when you try to remove that configuration, you get a message that it is not configured.
- You have replaced the start-up configuration file (in this case you specify the `flush-db` parameter).

### Command Syntax

```
reload (flush-db|)
```

### Parameters

<code>flush-db</code>	Delete the database file and recreate it from the start-up configuration file.
-----------------------	--

### Default

No default value is specified

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

This example shows replacing a start-up configuration file and then synchronizing it to the configuration database:

```
#copy file /home/TEST.conf startup-config
Copy Success
#
#reload flush-db
The system has unsaved changes.
Would you like to save them now? (y/n): n

Configuration Not Saved!
Are you sure you would like to reset the system? (y/n): y
```

For both of these prompts, you must specify whether to save or discard the changes. Abnormal termination of the session without these inputs can impact the system behavior.

For the `unsaved changes` prompt:

Would you like to save them now?

You should always say “no” to this prompt because otherwise the command takes the current *running configuration* and applies it to the current start-up configuration.

---

## service advanced-vty

Use this command to set multiple options to list when the tab key is pressed while entering a command. This feature applies to commands with more than one option.

Use the `no` parameter to not list options when the tab key is pressed while entering a command.

### Command Syntax

```
service advanced-vty
no service advanced-vty
```

### 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)#service advanced-vty
(config)#no service advanced-vty
```

---

## service password-encryption

Use this command to encrypt passwords created with the [enable password](#) command. Encryption helps prevent observers from reading passwords.

Use the `no` parameter to disable this feature.

Only network administrators can execute these commands. For more, see the [username](#) command.

### Command Syntax

```
service password-encryption
no service password-encryption
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#enable password mypasswd
(config)#service password-encryption
```

---

## service terminal-length

Use this command to set the number of lines that display at one time on the screen for the current terminal session.

Use the `no` parameter to disable this feature.

### Command Syntax

```
service terminal-length <0-512>
no service terminal-length (<0-512>|)
```

### Parameters

<0-512>	Number of lines to display. A value of 0 prevents pauses between screens of output.
---------	---

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#service terminal-length 60
```

---

## show clock

Use this command to display the current system time.

### Command Syntax

```
show clock
```

### Parameters

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show clock
12:54:02 IST Fri Apr 29 2016
```

---

## show cli

Use this command to display the command tree of the current mode.

### Command Syntax

```
show cli
```

### Parameters

None

### Default

None

### Command Mode

All command modes

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show cli
Exec mode:
+-clear
  +-arp-cache [clear arp-cache]
  +-ethernet
    +-cfm
      +-errors
      +-domain
        +-DOMAIN_NAME [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
          +-bridge
            +-<1-32> [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
              +-level
                +-LEVEL_ID [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
                  +-bridge
                    +-<1-32> [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
                      +-maintenance-points
                      +-remote
                      +-domain
                        +-DOMAIN_NAME [clear ethernet cfm maintenance-points remote(domain
D
--More--
```



---

## show cli history

Use this command to list the commands entered in the current session. The history buffer is cleared automatically upon reboot.

### Command Syntax

```
show cli history
```

### Parameters

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show cli history
1 en
2 show ru
3 con t
4 show spanning-tree
5 exit
```

---

## show crypto csr

Use this command to display the Certificate Signing Request (CSR) created with the [crypto pki generate rsa common-name ipv4](#) command.

### Command Syntax

```
show crypto csr
```

### Parameters

None

### Default

None

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
#crypto pki generate rsa common-name ipv4 7.7.7.7
#show crypto csr
-----BEGIN CERTIFICATE REQUEST-----
MIICVzCCAT8CAQAwEjEQMA4GA1UEAwwHNy43LjcuNzCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMkzIZaxNYPd8PW0hexecUFKq9pJn5IJzJkOQDtoVFOT
zeLPRxBaOt1NVd+lEF+wy3AgnGMw004g4AP7qaE+S5X1vKGAjagt fh/gfDAPDUtM
CpYLMCACM7n76OmyP9eUpkMbOSPkZDIBZfjUMxDTFwkzCBH+BF6SkSxtA24NUA9z
5heCIb1ArXYjdlIeB+9FfiVd0Z5yxQsLY8604ONL7Up1766SArGQo6oZ1dJ+bc91
sQVCEpF40SdCnn+Uw3R0cPfQF81BJD4H0EHf1VnHtYJwQ1yax6qc5ghT9R/rABDa
BFB3R09QpjV4Ihd/MyrdQmEIoxHeNNvSGDj9+eiEpksCAwEAAaAAMA0GCSqGSIb3
DQEBCwUAA4IBAQAwxkQmNf3yiL+pmpwvE+gU8KVp3i4cvD13Vjh7IQMkCT47WPam
DUiYgwk+dPVAI+iWZq4qTvUNn6xahOyN5rnkTz9eipsQ1YHPpZB7hj5fimWwzJws
m4Tun0GZieEBCROqUpbuW+6QDvtR3XSzHhdGGSItZv9cYyKhNu007okwr67c2Ea
11B7PcultOb4wj3xjqao/ENDG+nmdUPaIKZrAwf2fEOarOaHgKwcl1AHHbusbJWL
qH0fAlOyVgfvG/WuCPP6Peg/Cpla7bDWqeGYt9vFTtekKoOMQLzJwl6oINbtBCcw
DZJpeaQpUhFm+ZOjwibZ5NGPBRSTuYncp5xJ
-----END CERTIFICATE REQUEST-----
```

---

## show debugging nsm

Use this command to display debugging information.

### Command Syntax

```
show debugging nsm
```

### Parameters

None

### Default

None

### Command Mode

Exec mode and privileged exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show debugging nsm
NSM debugging status:
  NSM event debugging is on
  NSM packet debugging is on
  NSM kernel debugging is on
#
```

---

## show list

Use this command to display the commands relevant to the current mode.

### Command Syntax

```
show list
```

### Parameters

None

### Default

None

### Command Mode

All command modes except IPv4 access-list and IPv6 access-list mode.

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
>show list
clear arp-cache
clear bgp *
clear bgp * in
clear bgp * in prefix-filter
clear bgp * out
clear bgp * soft
clear bgp * soft in
clear bgp * soft out
clear bgp <1-4294967295>
clear bgp <1-4294967295> in
clear bgp <1-4294967295> in prefix-filter
clear bgp <1-4294967295> out
clear bgp <1-4294967295> soft
clear bgp <1-4294967295> soft in
clear bgp <1-4294967295> soft out
clear bgp (A.B.C.D|X:X::X:X)
clear bgp (A.B.C.D|X:X::X:X) in
clear bgp (A.B.C.D|X:X::X:X) in prefix-filter
clear bgp (A.B.C.D|X:X::X:X) out
clear bgp (A.B.C.D|X:X::X:X) soft
clear bgp (A.B.C.D|X:X::X:X) soft in
clear bgp X:X::X:X soft out

--more--
```

## show logging cli

Use this command to display command history for all users.

### Command Syntax

```
show logging cli ((logfile LOGFILENAME)) (match-pattern WORD |)
show logging cli last <1-9999>
show logging logfile list
```

### Parameters

LOGFILENAME	Name of a saved command history log file. The default path is /var/log/messages, but you can specify a full path to override the default.
WORD	Display only lines with this search pattern.
<1-9999>	Number of lines to display from the end of the command history.
logfile list	Display a list of command history files.

### Default

LOGFILENAME Name of a saved command history log file. The default path is /var/log/messages, but you can specify a full path to override the default.

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#sh logging cli
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli logfile ipi
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli match-pattern root
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli logfile ipi match-pattern root
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#show logging cli last 2
2017 Mar 1 16:34:26.302 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging info'
2017 Mar 1 16:34:37.317 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging cli last 2'
#show logging logfile list
file1
file2
```

---

## show nsm client

Use this command to display NSM client information including the services requested by the protocols, statistics and the connection time

### Command Syntax

```
show nsm client
```

### Parameters

None

### Default

None

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show nsm client
NSM client ID: 1

NSM client ID: 19
IMI, socket 23
Service: Interface Service, Router ID Service, VRF Service
Message received 1, sent 58
Connection time: Thu Jul 22 11:03:12 2010
Last message read: Service Request
Last message write: Link Up
NSM client ID: 25
ONMD, socket 24
Service: Interface Service, Bridge service, VLAN service
Message received 2, sent 74
Connection time: Thu Jul 22 11:03:15 2010
Last message read: OAM LLDP msg
Last message write: Link Up
#
```

---

## show nsm forwarding-timer

Use this command to display the information of Graceful Restart capable MPLS clients to NSM that are currently shutdown. Use the option LDP or RSVP to see the particular module information.

### Command Syntax

```
show nsm (ldp| rsvp) forwarding-timer
```

### Parameters

ldp	Use this parameter to display the protocol LDP information.
rsvp	Use this parameter to display the protocol RSVP information.

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS-SP version 5.0.

### Example

```
OcNOS#
OcNOS#sh nsm rsvp forwarding-timer
Protocol-Name  GR-State  Time Remaining (sec)  Disconnected-time
RSVP          ACTIVE    100                   2021/08/18 04:49:23
OcNOS#sh nsm ldp forwarding-timer
Protocol-Name  GR-State  Time Remaining (sec)  Disconnected-time
LDP           ACTIVE    111                   2021/08/18 04:50:37
OcNOS#sh nsm forwarding-timer
Protocol-Name  GR-State  Time Remaining (sec)  Disconnected-time
LDP           ACTIVE    110                   2021/08/18 04:50:37
RSVP          ACTIVE    96                    2021/08/18 04:49:23
```

# show process

Use this command to display the OcNOS daemon processes that are running.

## Command Syntax

```
show process
```

## Parameters

None

## Command Mode

Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#show process
PID NAME          TIME      FD
  1 nsm            00:56:29   7
  2 ripd           00:56:29  11
  3 ripngd         00:56:29  12
  4 ospfd          00:56:29   9
  5 ospf6d         00:56:29  10
  6 bgpd           00:56:29  14
  9 isisd          00:56:29   8
#
```

[Table 4-12](#) explains the output fields.

Table 4-12: show process fields

Entry	Description
PID Name	Process identifier name.
TIME	(S): Number of system and user CPU seconds that the process has used. (None, D, and E): Total amount of time that the command has been running.
FD	The Flexible Data-Rates (FD) of the interface.



---

## show running-config

Use this command to show the running system status and configuration.

### Command Syntax

```
show running-config
show running-config full
```

### Parameters

full	Display the full configuration information.
------	---

### Command Mode

Privileged exec mode and configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
(config)#show running-config
no service password-encryption
!
no service dhcp
ip domain-lookup
!
mpls propagate-ttl
!
vrrp vmac enable
spanning-tree mode provider-rstp
no data-center-bridging enable
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 no shutdown
!
interface eth0
 ip address 10.1.2.173/24
 no shutdown
!
interface eth1
 shutdown

!
line con 0
 login
!
end
(config)#
```

---

## show startup-config

Use this command to display the startup configuration.

### Command Syntax

```
show startup-config
```

### Parameters

None

### Default

None

### Command Mode

Privileged exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show startup-config
!    2001/04/21 11:38:52
!
hostname ripd
password zebra
log stdout
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
!
router rip
 redistribute connected
 network 10.10.10.0/24
 network 10.10.11.0/24
!
line vty
 exec-timeout 0 0
```

---

## show timezone

Use this command to display the list of timezone names.

### Command Syntax

```
show timezone (all|africa|america|antarctica|arctic|asia|atlantic|australia|brazil|
canada|chile|europe|indian|mexico|pacific|us)
```

### Parameters

africa	Africa timezone list
all	All timezone list
america	America timezone list
antarctica	Antarctica timezone list
arctic	Arctic timezone list
asia	Asia timezone list
atlantic	Atlantic timezone list
australia	Australia timezone list
brazil	Brazil timezone list
canada	Canada timezone list
chile	Chile timezone list
europe	Europe timezone list
indian	Indian timezone list
mexico	Mexico timezone list
pacific	Pacific timezone list
us	US timezone list

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced in OcNOS 1.3.7

### Examples

```
#show timezone asia
Asia:
Kuwait
Samarkand
Novosibirsk
Hebron
Singapore
Dushanbe
Rangoon
Riyadh
Thimphu
Shanghai
```

Phnom\_Penh  
Taipei  
Qyzylorda  
Ho\_Chi\_Minh  
Urumqi  
Chita  
Khandyga  
Nicosia  
Jerusalem  
Ashkhabad  
Gaza  
Tel\_Aviv  
Baghdad  
Anadyr  
Tehran  
Ashgabat  
Saigon  
Damascus  
Sakhalin  
Yekaterinburg  
Baku  
Bangkok  
Kashgar  
Macao  
Seoul  
Jakarta  
Aden  
Katmandu  
Amman  
Ujung\_Pandang  
Kuching  
Hong\_Kong  
Ulan\_Bator  
Dhaka  
Macau  
Omsk  
Vientiane  
Pyongyang  
Ust-Nera  
Manila  
Srednekolymsk  
Tbilisi  
Kamchatka  
Magadan  
Istanbul  
Chongqing  
Jayapura  
Yerevan  
Makassar  
Colombo  
Karachi  
Hovd  
Novokuznetsk  
Krasnoyarsk  
Irkutsk  
Kabul  
Kolkata

Dacca  
Brunei  
Calcutta  
Kathmandu  
Bishkek  
Qatar  
Tashkent  
Aqtau  
Oral  
Kuala\_Lumpur  
Pontianak  
Harbin  
Aqtobe  
Bahrain  
Muscat  
Vladivostok  
Dubai  
Tokyo  
Chungking  
Almaty  
Choibalsan  
Thimbu  
Beirut  
Dili  
Yakutsk  
Ulaanbaatar

---

## show users

Use this command to display information about current users.

### Command Syntax

```
show users
```

### Parameters

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show users
```

```
Current user          : (*).  Lock acquired by user : (#).
```

```
CLI user              : [C].  Netconf users         : [N].
```

```
Location : Applicable to CLI users.
```

```
Session  : Applicable to NETCONF users.
```

	Line	User	Idle	Location/Session	PID	TYPE	Role
(*)	130 vty 0	[C]root	00:00:36	pts/0	20872	Local	network-admin
(#)	NA	[N]root	NA	1	NA	NA	network-admin
	NA	[N]root	NA	2	NA	NA	network-admin
	131 vty 1	[C]joyce	00:00:26	pts/1	17593	Remote	network-admin

---

## show version

Use this command to display OcNOS version information.

### Command Syntax

```
show version
```

### Parameters

None

### Default

None

### Command Mode

Exec mode and privileged exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show version
Software version: CEL_BELGITE_E1070-OcNOS-DC-IPBASE-6.3.0-Alpha-S5296F 08/30/
2023 15:19:52
Copyright (C) 2023 IP Infusion. All rights reserved

Software Product: OcNOS-DC, Version: 6.3.0
Build Number: 152
Release: Alpha-S5296F
Hardware Model: Celestica E1070
Software Feature Code: IPBASE
Software Baseline Version: 6.0.117

Installation Information:
Image Filename: OcNOS-DC-IPBASE-XGS-6.3.0-152-Alpha-S5296F-installer
ONIE-SysInfo: x86_64-cel_belgite-r0
#
```

**Table 4-13: Show version output**

Entry	Description
Software version	The software version including hardware device name and date.
Software Product	Product name and version.
Hardware Model	Hardware platform.
Software Feature Code	SKU that specifies the capabilities of this version of the software.
System Configuration Code	System configuration number.
Package Configuration Code	ONIE package installer versions.
Software Baseline Version	Version from which this release branch is created.

Table 4-13: Show version output (Continued)

Entry	Description
Installation Information	Information about the installation.
Image Filename	The file name of the installed image.
Install method	The type of server (or USB stick) from which the software was installed.
ONIE SysInfo	ONIE version.



---

## sys-reload

Use this command to cold restart the device.

Note: This command is an alias for the [reload](#) command.

### Command Syntax

```
sys-reload
```

### Parameters

None

### Default

None

### Command Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 1.3.7.

### Example

```
>sys-reload
The system has unsaved changes.
Would you like to save them now? (y/n): y
Building Configuration...
[OK]
Are you sure you would like to reset the system? (y/n): n
```

---

## sys-shutdown

Use this command to shut down the device gracefully. After giving this command, you can remove the device power cable.

**Note:** Some of the switch hardware doesn't support system shutdown. On such devices this command will make the switch to go for a reboot.

### Command Syntax

```
sys-shutdown
```

### Parameters

None

### Default

None

### Command Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 1.3.7.

### Example

```
>sys-shutdown
The system has unsaved changes.
Would you like to save them now? (y/n): y
Building Configuration...
[OK]
Are you sure you would like to shutdown the system? (y/n): y
For both of these prompts, you must specify whether to save or discard the
changes.
For the unsaved changes prompt:
Would you like to save them now?
```

---

## terminal length

Use this command to set the number of lines displayed on the screen.

Use the `no` option to unset the number of lines on a screen.

### Command Syntax

```
terminal length <0-511>
terminal no length <0-511>
```

### Parameters

`<0-511>`                      Number of lines on screen. Specify 0 for no pausing.

### Default

By default, terminal length is 25 lines.

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
>enable
#terminal length 0
```

The following example sets the terminal length to 30 lines.

```
#terminal length 30
```

---

## terminal monitor

Use this command to display debugging output on a terminal.

Use one of the optional parameters to display debugging output for the Privileged Virtual Router (PVR) or VR user. When the command is used without a parameter, it can be used by a PVR user or non-PVR user to display the debug output on the terminal for the user local VR. When used with a parameter, it may be used only by a PVR user.

The `no` form of the command terminates the debug output on the terminal. Both the PVR and VR user can use this command. In addition, the PVR user can cancel a debug output from a specific VR or all VRs.

### Command Syntax

```
terminal monitor
terminal monitor (all|WORD|)
terminal no monitor
terminal no monitor (WORD|)
```

### Parameters

WORD	Used in the PVR context, and contains the VR name to be included in the debugging session.
all	Used the PVR context to include all VR in a PVR debugging session.

### Default

No default value is specified

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
>Enable
#terminal monitor
#terminal no monitor
```

---

## traceroute

Use this command to trace an IPv4/v6 route to its destination.

### Command Syntax

```
traceroute WORD
traceroute WORD (vrf (NAME|management) |)
traceroute ipv6 WORD
traceroute ipv6 WORD (vrf (NAME|management) |)
```

### Parameters

WORD	Destination address (in A.B.C.D format for IPv4 or X:X::X:X for IPv6) or host name.
vrf	Virtual Routing and Forwarding instance.
NAME	Virtual Routing and Forwarding name.
management	Virtual Routing and Forwarding name.
ip	IPv4 echo.
WORD	Destination address in A.B.C.D format or host name.
ipv6	IPv6 echo.
WORD	Destination address in X:X::X:X format or host name.

### Default

No default value is specified

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#traceroute ip 10.10.100.126 vrf management
traceroute to 10.10.100.126 (10.10.100.126), 30 hops max, 38 byte packets
 1  10.1.2.1 (10.1.2.1)  0.386 ms  0.315 ms  0.293 ms
 2  10.10.100.126 (10.10.100.126)  1.944 ms  1.497 ms  1.296 ms
#
```

---

## write

Use this command to write the configuration to the file used at startup or to a specified file. This is the same as the [copy running-config startup-config](#) command.

### Command Syntax

```
write file FILE
write memory
write WORD
```

### Parameters

FILE	Write to a given path and file. If you do not give a file path, the file is added to <code>/root</code> .
memory	Write to non-volatile memory.
WORD	Write to running configuration file path.

### Default

No default value is specified

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

This example shows writing the configuration to the startup configuration file:

```
#write
Building configuration...
[OK]
```

This example shows writing the configuration to a specified file:

```
#write file /home/test.txt
Building configuration...
[OK]
```

---

## write terminal

Use this command to display the current configuration.

### Command Syntax

```
write terminal
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#write terminal

Current configuration:
!
hostname ripd
password zebra
log stdout
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
!
!
router rip
 network 10.10.10.0/24
 network 10.10.11.0/24
 redistribute connected
!
line vty
 exec-timeout 0 0
```





---

## CHAPTER 5 Chassis Management Module Commands

---

This chapter provides a description, syntax, and examples of CMM feature commands:

- [cpu-core-usage](#)
- [debug cmm](#)
- [locator led](#)
- [show hardware-information](#)
- [show system-information](#)
- [system-load-average](#)

You can retrieve the same set of information through SNMP that these commands display. This MIB is defined in `CMM-CHASSIS-MIB.txt`:

IP Infusion Inc. enterprise identifier	36673
Chassis MIB identifier	100

The MIB definition is available at:

- <https://github.com/IPInfusion/OcNOS/branches>

Navigate to the directory for the version of OcNOS that you are using.

---

## cpu-core-usage

Use this command to configure user threshold values for monitoring cpu core uses.

Use no form of this command to set default thresholds.

### Command Syntax

```
cpu-core-usage warning <51-100> alarm <91-100>
```

### Parameters

warning	Warning
<51-100>	51-100
alarm	alarm
<91-100>	91-100

### Default

Check the default thresholds using `show system-information cpu-load` CLI command.

### Command Mode

Config Mode

### Applicability

This command was introduced in OcNOS-1.3.6.

### Example

```
OcNOS#con t
Enter configuration commands, one per line. End with CNTL/Z.
OcNOS(config)#
OcNOS(config)#cpu-core-usage warning 56 alarm 97
OcNOS(config)#cpu-core-usage warning 56 alarm 97
OcNOS(config)#end
OcNOS#show system-information cpu-load

System CPU-Load Information
=====

Uptime                : 64 Days 18 Hours 20 Minutes 12 Seconds

Load Average(1 min)   : 4.24% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)   : 2.87% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)  : 3.37% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage         : 2.02%
CPU core 1 Usage       : 0.89% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 2 Usage       : 0.00% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 3 Usage       : 5.41% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 4 Usage       : 2.68% (Crit Thresh : 56%, Alert Thresh : 97%)
```

```
OcNOS#con t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#no cpu-core-usage
OcNOS(config)#end
OcNOS#show system-information cpu-load
```

System CPU-Load Information  
=====

```
Uptime                : 64 Days 18 Hours 21 Minutes 46 Seconds

Load Average(1 min)    : 2.44% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)    : 2.49% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)   : 3.27% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage          : 1.82%
CPU core 1 Usage       : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage       : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage       : 4.59% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage       : 1.82% (Crit Thresh : 50%, Alert Thresh : 90%)
OcNOS#
```

---

## debug cmm

Use this command to enable or disable debugging for CMM.

### Command Syntax

```
debug cmm
no debug cmm
```

### Parameters

None

### Default

By default, debug command is not configured.

### Command Mode

Configuration mode and exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#debug cmm
(config)#no debug cmm
```

---

## locator led

Use this command to turn on the locator LED.

Use the no form of this command to turn off the locator LED.

### Command Syntax

```
locator-led on
no locator-led on
```

### Parameters

None

### Default

By default, locator LED is turned off.

### Command Mode

Configuration mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#locator-led on
```

# show hardware-information

Use this command to display hardware information.

## Command Syntax

```
show hardware-information (memory|fan|temperature|led|power|transceiver|all)
```

## Parameter

all	Hardware details of all modules.
fan	Fan status of the boards.
led	LED status of the boards.
memory	Memory information of the boards.
power	PSU information.
temperature	Temperature sensor information of the boards.
transceiver	Transceiver presence status and supported list of transceivers.

## Default

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#sh hardware-information all
-----
                        RAM INFORMATION
-----

Total                  : 16015 MB
Used                   : 828 MB (5 %)
Free                   : 15186 MB (95 %)
Shared                 : 9 MB
Buffers                : 64 MB
Total Swap              : 0 MB
Free Swap              : 0 MB
Current Processes      : 215
Total High Memory      : 0 MB
Available High Memory  : 0 MB
Unit Size              : 1 Bytes
Alert Threshold        : 90 %
Critical Threshold     : 80 %
-----

                        HARD DISK INFORMATION
```

```

-----
Serial Number           : EB201807040000000158
Model Number           : FS032GMSI-AC
Firmware Revision      : Q0608A FS032GMSI-AC
Memory Size            : 29 GiB
Cylinders              : 16383
Heads                  : 16
Sectors               : 61865984
Unformatted Bytes/Track : 0
Unformatted Bytes/Sector : 0
Revision No           : 1008.0
Usage Alert Threshold  : 90 %
Usage Critical Threshold : 80 %
-----

```

Filesystem	Total (MB)	Used (MB)	Free (MB)	Use%
/	23818	4701	19117	20%
/cfg	476	96	380	20%
/installers	4911	282	4629	6%

```

-----
                DISK ACTIVITY      (Monitoring : Disabled)
-----

```

```

Monitoring Interval : 600 Sec
Current Read       : 0 KBps
Current Write      : 0 KBps
Average Read       : 0 KBps (Threshold 0 KBps)
Average Write      : 2 KBps (Threshold 0 KBps)
-----

```

```

Codes : R - Rear Fan, F - Front Fan, U - Unknown
-----

```

FAN TRAY	FAN	RPM	MINRPM	MAXRPM
1	1 (F)	8600	6718	21500
1	2 (R)	7300	5625	18000
2	1 (F)	8800	6718	21500
2	2 (R)	7500	5625	18000
3	1 (F)	8600	6718	21500
3	2 (R)	7400	5625	18000
4	1 (F)	8800	6718	21500
4	2 (R)	7500	5625	18000
5	1 (F)	8900	6718	21500
5	2 (R)	7400	5625	18000
6	1 (F)	8700	6718	21500
6	2 (R)	7400	5625	18000

Chassis Management Module Commands

Board Temp Sensors Temperature in Degree C										
-----										
SENSOR TYPE		CURR	EMER	ALRT	CRIT	CRIT	ALRT	EMER	MIN-TEMP	MAX-
TEMP	AVG-TEMP									
		TEMP	MIN	MIN	MIN	MAX	MAX	MAX	(Monitored since	
68 hour,22 min)										
-----										
CPU		33.00	0	10	14	52	57	60	32.00	40.00
35.36										
Mainboard Front middle		41.00	0	10	14	61	66	69	40.00	47.00
42.54										
Mainboard Rear middle		37.00	0	10	14	56	61	67	36.00	43.00
38.78										
Mainboard left		36.00	0	10	14	51	56	59	34.00	42.00
37.30										
BCM Chip		53.50	0	10	14	82	87	95	50.60	60.30
54.69										
Intel CPU Core ID 0		34.00	0	0	0	93	98	98	32.00	42.00
35.74										
Intel CPU Core ID 1		34.00	0	0	0	93	98	98	32.00	41.00
35.73										
Intel CPU Core ID 2		34.00	0	0	0	93	98	98	32.00	42.00
35.94										
Intel CPU Core ID 3		34.00	0	0	0	93	98	98	32.00	41.00
35.85										
BCM Chip Internal Temperature										
-----										
TEMP MONITOR		CURRENT TEMP		PEAK TEMP						
		(Degree C)		(Degree C)						
-----										
1		51.10		53.50						
2		53.50		55.00						
3		52.00		53.50						
4		51.10		53.00						
5		52.50		54.00						
6		52.50		55.50						
7		52.00		53.00						
8		51.60		52.50						
-----										
Hardware Thresholds										
-----										
-----										
System Power Information										
-----										
CMM_PS1_12V_PG			: FAIL							
CMM_PS2_12V_PG			: GOOD							
CMM_PS1_AC_ALERT			: FAIL							



CMM\_PS2\_AC\_ALERT : GOOD

Codes: \* Not Supported by device NA Not Applicable O Over U Under

PSU TEMP-2 (Celsius)	VOLT-IN FAN-1 (Volt) (Rpm)	VOLT-OUT FAN-2 (Volt) (Rpm)	CURR-IN PWR_OUT_MAX (Ampere)	CURR-OUT (Ampere)	PWR-IN (Watt)	PWR-OUT (Watt)	TEMP-1 (Celsius)
2	NA*	NA*	NA*	NA*	NA*	NA*	NA*
NA*	NA*	NA*					

LED	COLOR	DESCRIPTION
POWER 1	RED	PSU1 present, No Power
POWER 2	GREEN	PSU2 operates Normally
FAN TRAY 1	GREEN	Normal
FAN TRAY 2	GREEN	Normal
FAN TRAY 3	GREEN	Normal
FAN TRAY 4	GREEN	Normal
FAN TRAY 5	GREEN	Normal
FAN TRAY 6	GREEN	Normal
SYSTEM	AMBER	Minor Fault
LOCATOR	OFF	Locator Function is disabled
FRONT FAN	GREEN	Fan operates normally

#### Transceiver DDM support list

Type : SFP+

Vendor Name : OCLARO, INC.

Vendor Part Number : TRS7081AHCPA00A

DDM Supported : Yes

Type : QSFP

Vendor Name : AVAGO

Vendor Part Number : AFB-79E4Z

DDM Supported : Yes

Type : QSFP

Vendor Name : FINISAR CORP

Vendor Part Number : FCCN410QD3C

DDM Supported : Yes

Type : QSFP

Vendor Name : FINISAR CORP

Vendor Part Number : FTL410QE4C

DDM Supported : Yes

## Chassis Management Module Commands

---

Type	:QSFP
Vendor Name	:DELL
Vendor Part Number	:119N6
DDM Supported	:Yes
Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:QFP85P1040PD000
DDM Supported	:Yes
Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:QFPQL010400D000
DDM Supported	:Yes
Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:QFPQL010400B000
DDM Supported	:Yes
Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:QFPQL002400D000
DDM Supported	:Yes
Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:QFP85P3040PD000
DDM Supported	:Yes
Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:QFP85P1040PB000
DDM Supported	:Yes
Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:DAPQQC504000000
DDM Supported	:NO
Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:DAPQQM014000000
DDM Supported	:NO
Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:DAPQQM034000000
DDM Supported	:NO

---

Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:DAPQQM054000000
DDM Supported	:NO
Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:QFP1301040PD000
DDM Supported	:Yes
Type	:QSFP
Vendor Name	:Skylane Optics
Vendor Part Number	:QFPQL040400D000
DDM Supported	:Yes
Type	:QSFP
Vendor Name	:E.C.I.NETWORKS
Vendor Part Number	:IPIENQSFP40GSR4
DDM Supported	:Yes
Type	:QSFP28
Vendor Name	:DELL
Vendor Part Number	:4WJ41
DDM Supported	:Yes
Type	:QSFP28
Vendor Name	:FINISAR CORP
Vendor Part Number	:FCBN425QE1C
DDM Supported	:Yes
Type	:QSFP28
Vendor Name	:FINISAR CORP.
Vendor Part Number	:FTLC1151RDPL
DDM Supported	:Yes
Type	:QSFP28
Vendor Name	:FINISAR CORP
Vendor Part Number	:FTLC9551REPM
DDM Supported	:Yes
Type	:QSFP28
Vendor Name	:INPHI CORP
Vendor Part Number	:IN-Q2AY2
DDM Supported	:Yes
Type	:QSFP28
Vendor Name	:FS
Vendor Part Number	:QSFP28-SR4-100G
DDM Supported	:Yes

---

## Chassis Management Module Commands

---

Type :QSFP28  
Vendor Name :FS  
Vendor Part Number :QSFP-PC03  
DDM Supported :NO

Type :QSFP28  
Vendor Name :E.C.I.NETWORKS  
Vendor Part Number :EN-QSFP28-SR4  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :E.C.I.NETWORKS  
Vendor Part Number :EN-QSFP28-LR4  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q28QD010C07D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q2885P30C0PF000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q28QD020C00D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAOQQM01C00D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAOQQM02C00D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAOQQM03C00D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAOQQM05C00D000  
DDM Supported :Yes

---

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAOQQM07C00D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAOQQM10C00D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAOQQM20C00D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAOQQM30C00D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAOQQP10C00D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q2885P10C0PF000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q28QD040C00F000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q28QD010C00D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q28QD010C04D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q28QD040C05F000  
DDM Supported :Yes

## Chassis Management Module Commands

---

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q28QD040C05D000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAPQQM03C000000  
DDM Supported :NO

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAPQQM01C000000  
DDM Supported :NO

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAPQQM02C000000  
DDM Supported :NO

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAPQQM05C000000  
DDM Supported :NO

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :DAPQQC50C000000  
DDM Supported :NO

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q28QL002C00F000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q2C31002C00F000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q2C31P50C00F000  
DDM Supported :Yes

Type :QSFP28  
Vendor Name :Skylane Optics  
Vendor Part Number :Q2B85M70C00D000  
DDM Supported :Yes

Type : QSFP28  
 Vendor Name : Skylane Optics  
 Vendor Part Number : Q28QD080C05F000  
 DDM Supported : Yes

Type : QSFP28  
 Vendor Name : E.C.I.NETWORKS  
 Vendor Part Number : IPIENQSFP28SR4  
 DDM Supported : Yes

TX : Transmit status  
 RX-Los : Receive status  
 RESET : Normal (Out of reset), Reset (In reset)  
 POWER : Power level Low/High  
 - : NotApplicable

SFP:[0-0]

PORT	PRESENCE	Tx	Rx-Los
------	----------	----	--------

QSFP:[1-32]

PORT	PRESENCE	RESET	POWER	LANE				
				1	2	3	4	
1	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
2	Present	Normal	-	Tx	on	on	on	on
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
3	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
4	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
5	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
6	Present	Normal	-	Tx	on	on	on	on
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
7	Present	Normal	-	Tx	on	on	on	on
				Rx-Los	Off	Off	Off	Off

## Chassis Management Module Commands

8	Present	Normal	-	Tx-Los	Off	Off	Off	Off
				Tx	on	on	on	on
				Rx-Los	Off	Off	Off	Off
9	Present	Normal	-	Tx-Los	Off	Off	Off	Off
				Tx	on	on	on	on
				Rx-Los	Off	Off	Off	Off
10	Present	Normal	-	Tx-Los	Off	Off	Off	Off
				Tx	on	on	on	on
				Rx-Los	Off	Off	Off	Off
11	Present	Normal	-	Tx-Los	Off	Off	Off	Off
				Tx	on	on	on	on
				Rx-Los	Off	Off	Off	Off
12	Present	Normal	-	Tx-Los	Off	Off	Off	Off
				Tx	on	on	on	on
				Rx-Los	Off	Off	Off	Off
13	Not Present	Reset	-	Tx-Los	Off	Off	Off	Off
				Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
14	Not Present	Reset	-	Tx-Los	Off	Off	Off	Off
				Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
15	Present	Normal	-	Tx-Los	Off	Off	Off	Off
				Tx	on	on	on	on
				Rx-Los	Off	Off	Off	Off
16	Not Present	Reset	-	Tx-Los	Off	Off	Off	Off
				Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
17	Not Present	Reset	-	Tx-Los	Off	Off	Off	Off
				Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
18	Not Present	Reset	-	Tx-Los	Off	Off	Off	Off
				Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
19	Not Present	Reset	-	Tx-Los	Off	Off	Off	Off
				Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
20	Not Present	Reset	-	Tx-Los	Off	Off	Off	Off
				Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
21	Not Present	Reset	-	Tx-Los	Off	Off	Off	Off
				Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
22	Not Present	Reset	-	Tx-Los	Off	Off	Off	Off
				Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
23	Not Present	Reset	-	Tx-Los	Off	Off	Off	Off
				Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
24	Not Present	Reset	-	Tx-Los	Off	Off	Off	Off
				Tx	off	off	off	off



				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
25	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
26	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
27	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
28	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
29	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
30	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
31	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off
32	Not Present	Reset	-	Tx	off	off	off	off
				Rx-Los	Off	Off	Off	Off
				Tx-Los	Off	Off	Off	Off

System Over all status : Minor Fault

-----  
Components status  
-----

CPU : Normal  
RAM : Normal  
DISK : Normal  
TEMP : Normal  
FAN : Normal  
POWER : Minor Fault  
SOFTWARE : Normal

Codes: H-Mi- High Minor H-Ma- High Major L-Mi- Low Minor L-Ma- Low Major

Component	Fault	Timestamp	Thresh	Violation-Status
-----	-----	-----	-----	-----
CPU	H-Mi	05-11-2019 11:40:49	> 50.00	61.60% (Cpu Core)
POWER	H-Mi	05-11-2019 11:40:27		Psu [1] AC is not OK and 12V Power Failed

#

Table 5-14 explains the show command output fields.

**Table 5-14: show hardware-information all output**

Entry	Description
Ram Information	Displays the used memory, free memory, shared, buffers, total swap, and free swap memory.
Hard Disk Information	Displays hard drive serial number, model, firmware revision, cylinders, heads, and sectors, as well as revision number and total size.
Disk Activity	Display hardware drive disk monitors, read and write current uses of the disks and shows averages usages.
Fans	Displays the fan tray numbers, numbers of fans per tray, and their speed in RPM.
Board Temp Sensors Temperature	Displays sensor type, current temperature, and operating range.
BCM Chip Internal Temperature	Displays broadcom chips current internal temperature, Operating range and average temperature.
System Power Information	Displays system power Information. Shows Voltage on all rails, and whether the power is up or has failed.
Hardware Threshold	Specifies the PSU thresholds of the hardware to take corrective action such as cut down or resume the power.
PSU	Show main power supply statistics – Volts in, Volts out, current in and out Amperes, power in and out in Watts, temperature of each power supply, and fan speed in RPM.
LED	Shows a list of what the LEDs represent, what state the LEDs mean, and a description of what the LEDs current color means.
Transceiver DDM support list	Show a list of transceivers that support Digital Diagnostic Monitoring (DDM) – type, vendor name, part number, and whether DDM is supported.
Port Number	Displays a list of the port numbers, port type (SFP,QSFP, etc) and whether a transceiver is or is not in the port.

---

## show system-information

Use this command to display system information.

### Command Syntax

```
show system-information (all|fan|psu|os|cpu|bios|cpu-load|board-info)
```

### Parameter

all	System information of all modules.
bios	BIOS information.
board-info	Board EEPROM details.
cpu	Processor information.
cpu-load	CPU load information.
fan	Fan Field Replaceable Units (FRU) EEPROM information.
os	OS and Kernel version information.
psu	Power Supply Field Replaceable Units (FRU) EEPROM information.

### Default

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show system-information psu
System PSU FRU Information
=====
PSU 2 Country of Origin      : CN
PSU 2 PPID Part Number      : 0T9FNW
PSU 2 PPID Part Number Rev   : A00
PSU 2 Manufacturer ID       : 28298
PSU 2 Date Code             : 52R
PSU 2 Serial Number         : 0298
PSU 2 Part Number           : 0T9FNW
PSU 2 Part Number Revision   : A00
PSU 2 Number of Fans in the tray : 1
PSU 2 Type                  : AC Normal
PSU 2 Service Tag           : AEIOU
```

The following tables explain the show command output fields.

**Table 5-15: Show fan topic displays**

System Fan FRU Information	Description
Fan Tray “#” PPID Part Number	The vendor's part number for the fan.
Fan Tray Serial Number	As stated
Service Tag	The Service Tag can help identify your device for on-line support and upgrading drivers
Vendor Name	As stated

**Table 5-16: Show system BIOS information**

BIOS Information	Description
# dmidecode	The dmidecode is a tool for dumping a computer's DMI table contents in a human-readable format. This table contains a description of the system's hardware components, as well as other useful pieces of information such as serial numbers and BIOS revisions.
SMBIOS	The System Management BIOS (SMBIOS) defines data structures (and access methods) that can be used to read management information produced by the BIOS of a computer.  Also, it is involved with the DMI Address –
Handle 0x0000, DMI type 0, 24 bytes	Handle of the Desktop Management Interface (DMI) and the DMI type, where type value identifies what the DMI contains. DMI = 0 indicates the following information is specific to BIOS properties, and is 24 bytes long.
BIOS Physical Information	<ul style="list-style-type: none"> <li>• Vendor – The manufacture of the BIOS.</li> <li>• Version – The Version number.</li> <li>• Release Date – as stated.</li> <li>• Address – starting address (in memory) of the BIOS.</li> </ul>
Characteristics	<ul style="list-style-type: none"> <li>• Is PCI supported.</li> <li>• Is BIOS upgradeable.</li> <li>• Is boot from a CD supported.</li> <li>• Is selectable boot devices supported.</li> <li>• Is BIOS ROM socketed.</li> <li>• Is Enhanced Disk Drive (EDD) vectoring supported.</li> <li>• Is 5.25"/1.2 MB floppy services supported (int 13h)</li> <li>• Is 3.5"/720 kB floppy services supported (int 13h)</li> <li>• Is 3.5"/2.88 MB floppy services supported (int 13h)</li> <li>• Is Print screen service supported (int 5h)</li> <li>• Is 8042 keyboard services supported (int 9h)</li> <li>• Is Serial services supported (int 14h)</li> <li>• Is Printer services supported (int 17h)</li> <li>• Is Advanced Configuration and Power Interface (ACPI) supported</li> <li>• Is USB legacy supported</li> <li>• Is BIOS boot specification supported</li> <li>• Is Targeted content distribution supported</li> <li>• Is Unified Extensible Firmware Interface (UEFI) supported</li> </ul>
BIOS Revision	The BIOS revision number.

**Table 5-16: Show system BIOS information (Continued)**

BIOS Information	Description
Handle 0x0043, DMI type 13, 22 bytes	Handle of the Desktop Management Interface (DMI) and the DMI type, where type value identifies what the DMI contains. DMI = 13 indicates the following information is specific to BIOS language information, and is 22 bytes long.
BIOS Language Information	<ul style="list-style-type: none"> <li>Language Description Format – A term that describes the number of bits used to represent the BIOS Language information parameters.</li> <li>Installable Languages – The number of languages that can be used by the BIOS at any time.</li> <li>Currently Installed Language – United States English (or Latin-1) as described by the ISO standard, en US iso8859-1.</li> </ul>

**Table 5-17: Show CPU information**

System CPU Information	Description
processor	The processor number of each CPU
model name	Details about each CPU. For example, Intel(R) Atom(TM) CPU C2538 @ 2.40GHz.

**Table 5-18: Show system CPU load information**

Load Information	Description
Uptime	As stated in days, hours, minutes, and seconds.
Load Average for past 1min	As stated in percent.
Load Average for past 5 min	As stated in percent.
Load Average for past 15 min	As stated in percent.
CPU Usage at this instant	As stated in percent.
Max threshold for CPU-usage	As stated in percent.

**Table 5-19: Show system board information**

System Information	Description
Product Name	Model number of the device.
Serial Number	As stated
Base MAC Address	As stated
Manufacture Date	As state

**Table 5-19: (Continued)Show system board information**

System Information	Description
Platform Name	The platform on which the product is based.
ONIE Version	The version of the Open Network Install Environment (ONIE).
MAC addresses	Number of MAC addresses related to the device.
Manufacture	As stated
Country Code	The code that represents the country of manufacture. For example, US = United States, TW = Taiwan, and so on.
Diag Version	As stated
CRC-32	Cyclic Redundancy Check value.
Switch Chip Revision	As stated
MAIN BOARD REVISION	As stated
CPU CPLD VERSION	The version of the Complex Programmable Logic Device (CPLD) use by the CPU.
SW CPLD VERSION	The version of the Complex Programmable Logic Device (CPLD) use by the switch.
MAIN BOARD TYPE	An identifying string for the main board.
CPU BOARD ID	An identifying string for the CPU board.
CPU BOARD VERSION	As stated
SW BOARD ID	NA
SW BOARD VERSION	As stated
VCC 5V	The state of the VCC 5V power rail (Enabled \ Disabled)
MAC 1V	The state of the MAC 1V power rail Enabled \ Disabled
VCC 1.8V	The state of the VCC 1.8V power rail (Enabled \ Disabled)
MAC AVS 1V	The state of the MAC AVS 1V power rail (Enabled \ Disabled)
HOT SWAP1	Enabled \ Disabled
HOT SWAP2	Enabled \ Disabled

**Table 5-20: Show host system details**

Host Information	Description
OS Distribution	The operating system on which the device is to run.
Kernel Version	A string that identifies the operating kernel.

## system-load-average

Use this command to configure user threshold values for monitoring system load average for last 1 minute, 5 minute and 15 minute.

Use no form of this command to set default thresholds.

### Command Syntax

```
system-load-average (1min warning <41-100> alarm <51-100> 5min alarm <51-100> 15min
alarm <51-100>)
```

### Parameters

1min	1min
warning	Warning
<41-100>	41-100
alarm	alarm
<51-100>	51-100
5min	5min
alarm	alarm
<51-100>	51-100
15min	15min
alarm	alarm
<51-100>	51-100

### Default

Check the default thresholds using `show system-information cpu-load` CLI command.

### Command Mode

Config Mode

### Applicability

This command was introduced in OcNOS-1.3.6.

### Example

```
OcNOS#con t
Enter configuration commands, one per line. End with CNTL/Z.
OcNOS(config)#
OcNOS(config)#system-load-average 1min warning 45 alarm 55 5min alarm 65 15min
alarm 75

OcNOS#show system-information cpu-load

System CPU-Load Information
=====
```

---

```
Uptime                               : 64 Days 17 Hours 56 Minutes 22 Seconds

Load Average(1 min)                  : 5.74% (Crit Thresh : 45%, Alert Thresh : 55%)
Load Average(5 min)                  : 3.71% (Crit Thresh : N/A, Alert Thresh : 65%)
Load Average(15 min)                 : 3.21% (Crit Thresh : N/A, Alert Thresh : 75%)

Avg CPU Usage                        : 4.67%
CPU core 1 Usage                     : 4.42% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage                     : 2.68% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage                     : 6.19% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage                     : 5.36% (Crit Thresh : 50%, Alert Thresh : 90%)
```

```
OcNOS#con t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#no system-load-average
OcNOS(config)#end
OcNOS#show system-information cpu-load
```

```
System CPU-Load Information
=====
```

```
Uptime                               : 64 Days 18 Hours 16 Minutes 34 Seconds

Load Average(1 min)                  : 0.63% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)                  : 1.90% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)                 : 3.11% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage                        : 2.07%
CPU core 1 Usage                     : 1.83% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage                     : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage                     : 6.36% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage                     : 0.93% (Crit Thresh : 50%, Alert Thresh : 90%)
OcNOS#
```



## CHAPTER 6 Configuration Management

This chapter is a reference for commands that copy these types of files:

- Start-up configuration and running configuration
- System files such as boot files, core dumps, and debug logs

You can use these commands to copy files locally or to copy between the local device and a remote system.

The commands in this chapter use the techniques in [Table 6-21](#) to remotely transfer files:

**Table 6-21: File transfer techniques**

Trivial File Transfer Protocol (TFTP)	No authentication or encryption; dangerous to use over the Internet, but might be acceptable in a trusted environment Address format: <code>tftp: [//server[:port]] [/path]</code>
File Transfer Protocol (FTP)	Authenticates, but does not encrypt Address format: <code>ftp: [//server] [/path]</code>
Secure copy (SCP)	Authenticates and encrypts using Secure Shell (SSH1) Address format: <code>scp: [//server] [/path]</code>
SSH File Transfer Protocol (SFTP)	Authenticates and encrypts using Secure Shell (SSH2); this is the most secure technique Address format: <code>sftp: [//server] [/path]</code>
Hyper text Transfer Protocol (HTTP)	Address format: <code>http: [//server] [/path]</code> For download of running and startup configurations

This chapter contains these commands.

- `copy empty-config startup-config`
- `copy running-config`
- `copy running-config (interactive)`
- `copy startup-config`
- `copy startup-config (interactive)`
- `copy system file`
- `copy system file (interactive)`
- `copy ftp startup-config`
- `copy scp startup-config`
- `copy sftp startup-config`
- `copy tftp startup-config`
- `copy http startup-config`
- `copy http startup-config (interactive)`
- `copy ftp startup-config (interactive)`
- `copy scp filepath`
- `copy scp startup-config (interactive)`
- `copy tftp startup-config (interactive)`
- `copy http startup-config (interactive)`
- `copy file startup-config`

---

## copy empty-config startup-config

Use this command to clear the contents of the startup configuration.

### Command Syntax

```
copy empty-config startup-config
```

### Parameters

None

### Default

None

### Command Mode

Privileged exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#copy empty-config startup-config  
#
```

---

## copy running-config

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

### Command Syntax

```
copy running-config (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL|http HTTP-URL) (vrf (NAME|management)|)
```

### Parameters

TFTP-URL	Destination: tftp: [//server[:port]] [/path]
FTP-URL	Destination: ftp: [//server] [/path]
SCP-URL	Destination: scp: [//server] [/path]
SFTP-URL	Destination: sftp: [//server] [/path]
HTTP-URL	Destination: http: [//server] [/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy running-config sftp sftp://sftp.mysite.com/running_conf vrf management
```

---

## copy running-config (interactive)

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

### Command Syntax

```
copy running-config (ftp|tftp|scp|sftp|http) (vrf (NAME|management) |)
```

### Parameters

ftp	Destination: FTP server
tftp	Destination: TFTP server
scp	Destination: SCP server
sftp	Destination: SFTP server
http	Destination: HTTP server
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy running-config sftp vrf management
```

---

## copy startup-config

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

### Command Syntax

```
copy startup-config (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL|http
HTTP_URL) (vrf (NAME|management) |)
```

### Parameters

TFTP-URL	Destination: tftp: [//server[:port]] [/path]
FTP-URL	Destination: ftp: [//server] [/path]
SCP-URL	Destination: scp: [//server] [/path]
SFTP-URL	Destination: sftp: [//server] [/path]
HTTP-URL	Destination: http: [//server] [/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy startup-config sftp sftp://sftp.mysite.com/start-up_conf vrf management
```

---

## copy startup-config (interactive)

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

### Command Syntax

```
copy startup-config (ftp|tftp|scp|sftp|http) (vrf (NAME|management) |)
```

### Parameters

ftp	Destination: FTP server
tftp	Destination: TFTP server
scp	Destination: SCP server
sftp	Destination: SFTP server
http	Destination: HTTP server
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy startup-config sftp vrf management
```

---

## copy system file

Use this command to copy a system file to an FTP server, an SCP server, an SFTP server, or a TFTP server.

**Note:** The names of the options for the source in the first parameter refer to symbolic locations. The specific locations for Linux are noted below. The locations on a specific device can vary depending on the platform.

### Command Syntax

```
copy (core|debug|log|techsupport|filepath) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL) (vrf (NAME|management) |)
```

### Parameters

core	Core file storage; on Linux this refers to /var/log/crash/cores/
debug	Debug file storage; on Linux this refers to /log/
log	Log file storage; on Linux this refers to /var/log/
techsupport	Copy techsupport log files to remote machine
filepath	Copy device file to remote machine
FILE	Source file name
TFTP-URL	Destination: tftp: [//server[:port]] [/path]
FTP-URL	Destination: ftp: [//server] [/path]
SCP-URL	Destination: scp: [//server] [/path]
SFTP-URL	Destination: sftp: [//server] [/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy core myFile sftp sftp://sftp.mysite.com/dst_filename vrf management
```

---

## copy system file (interactive)

Use this command to copy a system file to an FTP server, an SCP server, an SFTP server, or a TFTP server.

**Note:** The names of the options for the source in the first parameter refer to symbolic locations. The specific locations for Linux are noted below. The locations on a specific device can vary depending on the platform.

### Command Syntax

```
copy (core|debug|log|techsupport|filepath) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL) (vrf (NAME|management) |)
```

### Parameters

core	Core file storage; on Linux this refers to /var/log/crash/cores/
debug	Debug file storage; on Linux this refers to /log/
log	Log file storage; on Linux this refers to /var/log/
techsupport	Copy techsupport log files to remote machine
filepath	Copy device file to remote machine
FILE	Source file name
ftp	Destination: FTP server
tftp	Destination: TFTP server
scp	Destination: SCP server
sftp	Destination: SFTP server
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy log myFile sftp vrf management
```



---

## copy ftp startup-config

Use this command to copy the start up configuration from an FTP server to the local device.

### Command Syntax

```
copy ftp FTP-URL startup-config (vrf (NAME|management) |)
```

### Parameters

FTP-URL	Configuration source: ftp: [//server] [/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy ftp ftp://ftp.mysite.com/scr filename startup-config vrf management
```

---

## copy scp startup-config

Use this command to copy the start up configuration from a SCP server to the local device.

### Command Syntax

```
copy scp SCP-URL startup-config (vrf (NAME|management) |)
```

### Parameters

SCP-URL	Configuration source: scp: [//server] [/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy scp scp://scp.mysite.com/scr filename startup-config vrf management
```

---

## copy sftp startup-config

Use this command to copy the start up configuration from a SFTP server to the local device.

### Command Syntax

```
copy sftp SFTP-URL startup-config (vrf (NAME|management) |)
```

### Parameters

SFTP-URL	Configuration source: sftp:[//server] [/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy sftp sftp://sftp.mysite.com/scr filename startup-config vrf management
```

---

## copy tftp startup-config

Use this command to copy the start up configuration from a TFTP server to the local device.

### Command Syntax

```
copy tftp TFTP-URL startup-config (vrf (NAME|management) |)
```

### Parameters

TFTP-URL	Configuration source: tftp: [//server] [/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy tftp tftp://tftp.mysite.com/scr filename startup-config vrf management
```

---

## copy http startup-config

Use this command to copy the start up configuration from an HTTP server to the local device.

### Command Syntax

```
copy http HTTP-URL startup-config (vrf (NAME|management) |)
```

### Parameters

HTTP-URL	Configuration source: http: [//server] [/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy http http://http.mysite.com/scr filename startup-config vrf management
```

---

## copy ftp startup-config (interactive)

Use this command to copy the start up configuration from an FTP server to the local device.

### Command Syntax

```
copy ftp startup-config (vrf (NAME|management))
```

### Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy ftp startup-config vrf management
```

---

## copy scp filepath

Use this command to copy the remote system file using SCP to the local device.

**Note:** OcNOS has a dedicated partition called `/cfg` for storing system level configurations, OcNOS configurations and license data. This is persistent across reboots and upgrades and consists of directories `/cfg/` and `/usr/local/etc`. Copying `user/general` files under `/cfg` partition is discouraged because the size of this partition is very small and impacts normal system operations like `bootup/upgrades` and important system files copy when it doesn't have enough space. Users are recommended to use `/home` to copy the general files. Please note that the contents placed in `/home` directory are deleted upon software upgrade.

### Command Syntax

```
copy scp SCP-URL (filepath FILEPATH) (vrf (NAME|management) |)
```

### Parameters

SCP-URL	Configuration source: <code>scp://server[/path]</code>
FILEPATH	Enter the local filesystem path with filename
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced in OcNOS version 1.3.9.

### Examples

```
#copy scp scp://10.12.65.89/root/cmlsh filepath /root/cmlsh vrf management
```

---

## copy scp startup-config (interactive)

Use this command to copy the start up configuration from a SCP server to the local device.

### Command Syntax

```
copy scp startup-config (vrf (NAME|management))
```

### Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy scp startup-config vrf management
```



---

## copy sftp startup-config (interactive)

Use this command to copy the start up configuration from an SFTP server to the local device.

### Command Syntax

```
copy sftp startup-config (vrf (NAME|management) |)
```

### Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy sftp startup-config vrf management
```

---

## copy tftp startup-config (interactive)

Use this command to copy the start-up configuration from a TFTP server to the local device.

### Command Syntax

```
copy tftp startup-config (vrf (NAME|management) |)
```

### Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy tftp startup-config vrf management
```

---

## copy http startup-config (interactive)

Use this command to copy the start-up configuration from an HTTP server to the local device.

### Command Syntax

```
copy http startup-config (vrf (NAME|management) |)
```

### Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy http startup-config vrf management
```

---

## copy file startup-config

Use this command to copy and store a local file into the startup configuration.

### Command Syntax

```
copy file FILE startup-config
```

### Parameters

FILE	File name
------	-----------

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#copy file myFile startup-config
```

## CHAPTER 7 Control Plane Policing Commands

---

This chapter is a reference for the Control Plane Policing (CoPP) commands.

- [clear interface cpu counters](#)
- [cpu-queue](#)
- [show interface cpu counters queue-stats](#)
- [show cpu-queue details](#)

---

## clear interface cpu counters

Use this command to clear the CPU queue counters.

### Command Syntax

```
clear interface cpu counters
```

### Parameter

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear interface cpu counters
```

## cpu-queue

Use this command to set protocol queues shaper and enable/disable queue monitoring for drop.

### Command Syntax

```
cpu-queue (acl|arp|best-effort|bgp|bpdu|ccm|dhcp|daivm|igmp|ipmc-miss|isis|l3-
miss|mpls|nd|ospf|pim|ptp|rip|sflow|bfd| vrrp|vxlan) (lossy | lossless|)
(monitor|no-monitor|) (rate <0-100000>|)

no cpu-queue (acl|arp|best-effort|bgp|bpdu|ccm|dhcp|daivm|igmp|ipmc-miss|isis|l3-
miss|mpls|nd|ospf|pim|ptp|rip|sflow|bfd| vrrp|vxlan) (lossy | lossless|)
(monitor|no-monitor|) (rate <0-100000>|)
```

### Parameters

acl	ACL queue parameters (for acl logging)
arp	ARP queue parameters
best-effort	Best-effort queue parameters
bfd	BFD queue parameters
bgp	BGP queue parameters
bpdu	BPDU queue parameters
ccm	CCM queue parameters
dhcp	DHCP queue parameters
igmp	IGMP queue parameters
ipmc-miss	IPMC-Miss queue parameters
isis	ISIS queue parameters
l3-miss	L3-Miss queue parameters
nd	ND queue parameters
ospf	OSPF queue parameters
pim	PIM queue parameters
rip	RIP queue parameters
sflow	SFLOW queue parameters
vrrp	VRRP queue parameters
vxlan	VXLAN queue parameters
monitor	Monitor CPU queue usage
no-monitor	Do not monitor CPU queue usage
lossless	Configure cpu queue as lossless
lossy	Configure cpu queue as lossy
rate	Set CPU queue rate <0-100000>

## Default

CPU queues are set with the default values as shown in [Table 2-1](#).

## Command Mode

Exec mode and Privileged exec mode

## Applicability

This command was introduced before OcNOS version 1.3.8.

## Example

Use the following command to configure rate/monitor/no-monitor for protocol queues:

```
#configure terminal
#cpu-queue bpdu rate 500 lossy no-monitor
```

Use the following command to verify the rate received on each protocol queue:

```
#show int cpu counters rate kbps
```

Load interval: 30 second

CPU Queue (%)	Rx kbps	Rx pps	Tx kbps	Tx pps
bpdu ( 0%)	-	-	0.54	1

Use the following command to verify the maximum, configured, and default configuration values:

```
#show cpu-queue details
```

Cpu queue Name	Rate In PPS			Monitor Status		Lossy Status	
	Configured	Default	Max Rate Allowed	Configured	Default	Configured	Default
best-effort	-	2113	2113	-	* no-monitor	-	* lossy
ipmc-miss	-	2113	2113	-	* no-monitor	-	* lossy
l3-miss	-	211	211	-	* no-monitor	-	* lossy
sflow	-	32000	100000	-	monitor	-	* lossy
bgp	-	1500	1500	-	monitor	-	lossless
vrrp	-	500	500	-	monitor	-	lossless
ldp-rsvp	-	500	500	-	monitor	-	lossless
rip	-	500	500	-	monitor	-	lossless
ospf	-	2000	2000	-	monitor	-	lossless
dhcp	-	100	2048	-	no-monitor	-	lossy
nd	-	6000	6000	-	monitor	-	lossless
mpls	-	500	500	-	no-monitor	-	lossy
pim	-	4000	4000	-	* no-monitor	-	* lossy
arp	-	6000	6000	-	monitor	-	lossless
igmp	-	4000	4000	-	* no-monitor	-	* lossy
bpdu	500	10000	10000	no-monitor	monitor	lossy	lossless
ccm	-	500	500	-	no-monitor	-	lossy
bfd	-	2000	2000	-	no-monitor	-	lossy
ptp	-	1000	1000	-	no-monitor	-	lossy
isis	-	500	1000	-	monitor	-	lossless
trill-isis	-	1000	1000	-	monitor	-	lossless
acl	-	200	1000	-	* no-monitor	-	* lossy
vxlan	-	500	500	-	monitor	-	lossy
daivm	-	100	500	-	no-monitor	-	lossy



---

## show interface cpu counters queue-stats

Use this command to display the counters of packets destined to the CPU.

For details about this command, see [show interface counters queue-stats](#).

### Example

```
#show interface cpu counter queu-stats
```

```
E - Egress, I - Ingress, Q-Size is in bytes
```

Queue/Class-map	Q-Size	Tx pkts	Tx bytes	Dropped pkts	Dropped bytes
nd	(E) 0	17	1998	0	0
bpdu	(E) 86320	253462	16221568	69227330	4430536320

## show cpu-queue details

Use this command to display CPU queue details.

### Command Syntax

```
show cpu-queue details
```

### Parameters

None

### Default

Not applicable

### Command Mode

Exec mode and Privileged exec mode

### Applicability

This command was introduced before OcNOS version 1.3.8.

### Example

Use the following command to configure rate/monitor/no-monitor for protocol queues:

```
#show cpu-queue details
```

Can not configure the parameter

Cpu queue		Rate In PPS		Monitor Status		Lossy Status	
Name	Configured	Default	Max Rate Allowed	Configured	Default	Configured	Default
best-effort	-	2113	2113	-	* no-monitor	-	* lossy
ipmc-miss	-	2113	2113	-	* no-monitor	-	* lossy
l3-miss	-	211	211	-	* no-monitor	-	* lossy
sflow	-	32000	100000	-	monitor	-	* lossy
bgp	-	1500	1500	-	monitor	-	lossless
vrrp	-	500	500	-	monitor	-	lossless
ldp-rsvp	-	500	500	-	monitor	-	lossless
rip	-	500	500	-	monitor	-	lossless
ospf	-	2000	2000	-	monitor	-	lossless
dhcp	-	100	2048	-	no-monitor	-	lossy
nd	-	6000	6000	-	monitor	-	lossless
mpls	-	500	500	-	no-monitor	-	lossy
pim	-	4000	4000	-	* no-monitor	-	* lossy
arp	-	6000	6000	-	monitor	-	lossless
igmp	-	4000	4000	-	* no-monitor	-	* lossy
bpdu	-	10000	10000	-	monitor	-	lossless
ccm	-	500	500	-	no-monitor	-	lossy
bfd	-	2000	2000	-	no-monitor	-	lossy
ptp	-	1000	1000	-	no-monitor	-	lossy
isis	-	500	1000	-	monitor	-	lossless
trill-isis	-	1000	1000	-	monitor	-	lossless
acl	-	200	1000	-	* no-monitor	-	* lossy
vxlan	-	500	500	-	monitor	-	lossy
daivm	-	100	500	-	no-monitor	-	lossy

---

## CHAPTER 8 Common Management Layer Commands

---

This chapter is a reference for the Common Management Layer (CML) commands.

Transaction are enabled by default. You can disable the feature by using the [cmlsh transaction](#) command outside of configuration mode, but IP Infusion Inc. does *not* recommend this.

These are the steps to follow to use transactions:

- When transactions are enabled, 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 [commit](#) 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.

This chapter describes these commands:

- [abort transaction](#)
- [cancel-commit](#)
- [cml force-unlock config-datastore](#)
- [cml lock config-datastore](#)
- [cml logging](#)
- [cml netconf translation](#)
- [cml notification](#)
- [cml unlock config-datastore](#)
- [cmlsh multiple-config-session](#)
- [cmlsh notification](#)
- [cmlsh transaction](#)
- [cmlsh transaction limit](#)
- [commit](#)
- [confirm-commit](#)
- [debug cml](#)
- [module notification](#)
- [show cml config-datastore lock status](#)
- [show cml notification status](#)
- [show cmlsh multiple-config-session status](#)
- [show cmlsh notification status](#)
- [show max-transaction limit](#)
- [show module-info](#)
- [show running-config notification](#)
- [show system restore failures](#)

- `show transaction current`
- `show transaction last-aborted`
- `show (xml|json) running-config|candidate-config`

---

## abort transaction

Use this command to end a configuration session and discard all uncommitted changes.

### Command Syntax

```
abort transaction
```

### Parameters

None

### Default

N/A

### Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 5.0.

### Example

```
(config) #  
(config) #interface eth2  
(config-if) #ip address 10.12.3.4/24  
(config-if) #exit  
(config) #abort transaction  
(config) #exit  
#show running-config interface eth2  
!  
interface eth2  
!  
#
```

---

## cancel-commit

Use this command to revert configuration changes immediately before the timeout in a “confirmed commit” operation.

Note: This command does not support the <persist-id> parameter as specified in RFC 6241.

### Command Syntax

```
cancel-commit
```

### Parameters

None

### Default

N/A

### Mode

All configuration modes

### Applicability

This command was introduced in OcNOS version 6.3.0.

### Example

```
(config)#router ospf 1
(config-router)#router ospf 2
(config-router)#commit confirmed timeout 100 description This is a test for confirmed
commit
(config-router)#
(config-router)#cancel-commit
```

---

# cml force-unlock config-datastore

Use this command to release a configuration lock previously obtained with the [cml lock config-datastore](#) command by a *different* user.

This command is available only to users with the `network-admin` role.

A notification message is sent to the lock holder when forced out.

## Command Syntax

```
cml force-unlock config-datastore (running|startup|candidate) (<0-600>|)
```

## Parameters

<0-600>	Timeout interval to force out lock acquired by another user session. Zero (0) is immediate and is the default.
running	Release the lock on the running datastore.
startup	Release the lock on the startup datastore.
candidate	Release the lock on the candidate datastore.

## Default

The default timeout is zero (0) which is immediate.

## Mode

Exec mode

## Applicability

This command was introduced in OcNOS version 5.1.

## Example

```
#cml force-unlock config-datastore running
```

---

## cml lock config-datastore

Use this command to lock the entire configuration datastore of a device. Such locks are intended to be short-lived and allow you to make a change without fear of interaction with other users.

When the lock is acquired, the server prevents any changes to the locked resource other than those requested by this session.

The duration of the lock is defined as beginning when the lock is acquired and lasting until either the lock is released or the user session closes. The session closure can be explicitly performed by the user, or implicitly performed by the server based on criteria such as failure of the underlying transport, simple inactivity timeout, or detection of abusive behavior on the part of the client.

A lock will not be granted if any of the following conditions is true:

- A lock is already held by any user session or another entity.
- The target configuration is candidate, it has already been modified, and these changes have not been committed or rolled back.
- The target configuration is running, and another user session has an ongoing confirmed commit.

### Command Syntax

```
cml lock config-datastore (running|startup|candidate)
```

### Parameters

running	Lock on this datastore will not allow other sessions to perform operations with the target as running like commit, copy candidate to running and so on.
startup	Lock on this datastore will not allow other sessions to perform operations like copy-config and delete-config with the target startup
candidate	Lock on this datastore will not allow other sessions to perform operations with the target as candidate like edit-config, copy file candidate and so on. (Not supported in OcNOS version 5.1.)

### Default

All three datastores are in the unlocked state.

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 5.1.

### Example

```
#cml lock config-datastore running
#
#show users
Current user      : (*).  Lock acquired by user : (#).
CLI user          : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.
```

Line	User	Idle	Location/Session	PID	TYPE	Role
(#) (*) 130 vty 0	[C]ocnos	0d00h00m	pts/0	10732	Local	network-admin



---

## cml logging

Use this command to enable or disable CML logging. The logging level and [debug cml](#) should also be configured.

### Command Syntax

```
cml logging (enable | disable)
```

### Parameters

enable	Enable CML logging
disable	Disable CML logging

### Default

By default CML Logging is enabled.

### Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 5.0.

### Example

```
(config)#cml logging disable
```

---

## cml netconf translation

Use this command to enable or disable NetConf support for OpenConfig-based YANG translation. This allows OcNOS to handle OpenConfig YANG files in its NetConf server.

### Command Syntax

```
cml netconf translation (disable|openconfig)
```

### Parameters

disable	Do not translate NetConf to YANG
openconfig	Translate NetConf to YANG

### Default

By default NetConf-to-YANG translation is disabled.

### Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 4.2.

### Example

```
#cml netconf translation openconfig
```

# cml notification

Use this command to enable or disable notification for a given CML client.

## Command Syntax:

```
cml notification (enable|disable) (netconf|snmp|cmlsh|all)
```

## Parameters

disable	Disable notification subscription
enable	Enable notification subscription
all	All CML clients
cmlsh	CML client CMLSH
netconf	CML client NETCONF
snmp	CML client SNMP

## Default

By default, notification is enabled for all CML clients.

## Mode

Exec mode

## Applicability

This command was introduced in OcNOS version 6.0.0.

## Example

To enable notification for NETCONF client:

```
#cml notification enable netconf
```

To disable notification for NETCONF client:

```
#cml notification disable netconf
```

---

## cml unlock config-datastore

Use this command to release a configuration lock previously obtained with the [cml lock config-datastore](#) command.

An unlock operation will not succeed if either of the following conditions is true:

- The specified lock is not currently active.
- The session calling this command is not the same session that obtained the lock.

### Command Syntax

```
cml unlock config-datastore (running|startup|candidate)
```

### Parameters

running	Release the lock on the running datastore.
startup	Release the lock on the startup datastore.
candidate	Release the lock on the candidate datastore.

### Default

N/A

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 5.1.

### Example

```
#cml unlock config-datastore running
```

```
#
```

```
#show users
```

```
Current user      : (*). Lock acquired by user : (#).
```

```
CLI user         : [C]. Netconf users       : [N].
```

```
Location : Applicable to CLI users.
```

```
Session  : Applicable to NETCONF users.
```

	Line	User	Idle	Location/Session	PID	TYPE	Role
	(*) 130 vty 0	[C]ocnos	0d00h00m	pts/0	10732	Local	network-admin

```
#
```

---

## cmlsh multiple-config-session

Use this command to enable or disable multiple CLI sessions to enter into configuration mode simultaneously.

With this support, multiple CLI users can enter into configuration mode simultaneously and do configurations in parallel and commit into the running datastore. This is similar to NetConf multiple session support described in RFC 6241.

When multiple configuration mode sessions are disabled, only one user can enter configuration mode and it will lock the running datastore.

If any CLI session is already there in configuration mode, error will be given when user tries to enable this mode.

A datastore lock can be acquired using the [cml lock config-datastore](#) command if you want to do configuration without fear of interaction with other user sessions.

This command is available only to users with the `network-admin` role.

This configuration is retained across reboots.

### Command Syntax

```
cmlsh multiple-config-session (enable|disable)
```

### Parameters

<code>enable</code>	Enable multiple configuration mode sessions.
<code>disable</code>	Disable multiple configuration mode sessions.

### Default

By default, multiple CLI sessions are disabled.

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 5.1.

### Example

```
#cmlsh multiple-config-session enable
#
#show cmlsh multiple-config-session status
CMLSh multiple configuration session mode : Enabled
#
```

### Usage

Multiple users can enter into configuration mode simultaneously and do configurations in parallel and commit into the running datastore. Examples of when you need this feature are:

- Migrating to replace an existing device. If an existing device has a large configuration and it is only done by one person, it will take more time to configure. If multiple users can configure at same time, it will take less time.
- Troubleshooting and operating. Sometimes a single device has 2 or more links to troubleshoot. If only one user only can do configuration, it will take more time to resolve the problem.

When multiple sessions are doing parallel configurations, there is a chance that one user's configuration might conflict with another user's configuration.

If you do not lock the datastore before doing a configuration, a parallel candidate datastore can be created and will be allowed to commit to the datastore. So the datastore can change while the previous user is still having the configuration in its candidate. Now when the previous user tries to commit, if the configurations conflict, it will fail.

For example, if the previous user was adding a BGP neighbor and the BGP router itself is removed from the datastore via the parallel transaction, when this user tries to commit, it will fail. The reason is when commands are added to candidate, it only checks the running datastore at that point and allows them to be added to candidate configuration datastore. But later if the running datastore itself is changed, these configurations can be irrelevant and will cause an error on commit. So the user will have to abort the transaction.

---

## cmlsh notification

Use this command to enable or disable notification for the current CMLSH session.

### Command Syntax

```
cmlsh notification (enable|disable)
```

### Parameters

disable	Disable notification subscription for current CMLSH session
enable	Enable notification subscription for current CMLSH session

### Default

By default, notification is enabled for the CMLSH session.

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 6.0.0.

### Example

To enable notification for current CMLSH session:

```
#cmlsh notification enable
```

To disable notification for current CMLSH session:

```
#cmlsh notification disable
```

---

## cmlsh transaction

Use this command to enable or disable the transaction-based command-line interface.

Note: IP Infusion Inc. recommends that you do *not* disable transactions.

### Command Syntax

```
cmlsh transaction (enable | disable)
```

### Parameters

enable	Enable transaction-based command-line interface
disable	Disable transaction-based command-line interface

### Default

The transaction-based command-line interface is enabled by default.

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 5.0.

### Example

```
>en
#cmlsh transaction disable
% Deprecated CLI. Disabling transaction mode is not recommended
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#router ipv6 ospf test
(config-router)#exit
(config)#show running-config router ipv6 ospf
!
router ipv6 ospf test
!
(config)#
```



---

## cmlsh transaction limit

Use this command to set the maximum number of transactions.

To verify, give the [show max-transaction limit](#) command in exec mode.

### Command Syntax

```
cml transaction limit <0-300000>
```

### Parameters

`<0-300000>` Maximum number of transactions with zero (0) indicating unlimited transactions.

### Default

300,000 transactions

### Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 5.0.

### Example

```
(config)#cml transaction limit 1500
(config)#exit
#show max-transaction limit
Max-Transaction Limit is 1500
```

---

## commit

Use this command to commit the candidate configuration to the running configuration.

**Note:** After a successful `commit` command, you must give the [write](#) command to save the running configuration to the startup configuration.

**Note:** Multiple configurations cannot be removed with a single `commit`. You must remove each configuration followed by a `commit`.

Optionally with “confirmed commit”, you can commit the configuration on a trial basis for a time specified in seconds. If you do not confirm within the specified time, the configuration will be reverted after the timeout.

- To revert the configuration before timeout, then give the [cancel-commit](#) command.
- To retain the configuration before timeout, then give the [confirm-commit](#) command.

See RFC 6241 “Confirmed Commit Capability”.

**Note:** A `commit` command without any parameters is treated as permanent and an explicit [confirm-commit](#) command is not required to confirm the commit.

**Note:** Multiple confirmed commits in the same session or different sessions are not supported. The `commit` command does not support the `<persist-id>` parameter as specified in RFC 6241.

### Command Syntax

```
commit (confirmed (timeout <1-500>|)) (description LINE|)
```

### Parameters

<code>confirmed</code>	Commits the configuration on a trial basis.
<code>&lt;1-500&gt;</code>	Timeout in seconds after which configuration should be reverted if a confirmation is not given with <a href="#">confirm-commit</a> . If not specified, the default timeout is 300 seconds.
<code>LINE</code>	Commit description up to 65 characters

### Default

The default timeout is 300 seconds.

### Mode

All configuration modes

### Applicability

This command was introduced in OcNOS version 5.0 and the `confirmed` clause added in OcNOS version 6.3.0.

### Example

```
(config)#router ospf 1
(config-router)#exit
(config)#router isis 3
(config-router)#commit
(config-router)#exit
(config)#show running-config ospf
!
router ospf 1
```

```
!  
(config)#show running-config isis  
!  
router isis 3  
!  
(config)#
```

If you try to exit or end, you are prompted to commit or abort first:

```
(config)#router bgp 10  
(config-router)#bgp as-local-count 34  
(config-router)#exit  
(config)#exit  
% Un-committed transactions present. Please do commit or abort before exiting.  
(config)#end  
% Un-committed transactions present. Please do commit or abort before exiting.  
(config)#commit  
(config)#show running-config bgp  
!  
router bgp 10  
  bgp as-local-count 34  
!  
(config)#
```

This is an example of a “confirmed commit”:

```
(config)#router ospf 1  
(config-router)#router ospf 2  
(config-router)#commit confirmed timeout 100 description This is Test for confirmed  
commit
```

---

## Usage

OcNOS validates dependencies when you commit. In this example, bridge 1 must exist before you can create a VLAN on it:

```
(config)#vlan database  
(config-vlan)#vlan 10 bridge 1  
(config-vlan)#exit  
(config)commit
```

Because of the unmet dependency, you get an error when you try to commit.

If you also create the bridge, the commit succeeds:

```
(config)#bridge 1 protocol mstp  
(config)#vlan database  
(config-vlan)#vlan 10 bridge 1  
(config-vlan)#exit  
(config)commit
```

In a single transaction, dependent configurations can be given in any order. Using the same example as before, you can create the bridge *after* the VLAN:

```
(config)#vlan database  
(config-vlan)#vlan 10 bridge 1
```

```
(config-vlan)#exit
(config)#bridge 1 protocol mstp
(config)commit
```

OcNOS supports “hitless merges” and does not write to the candidate configuration if you make the same configuration in separate transactions. In this example, subinterface xe1.1 is not created the second time because it already exists:

```
(config)#interface xe1.1
(config-if)#commit
(config)#interface xe1.1
(config-if)#commit
```

OcNOS does not write to the candidate configuration if you create and delete the same entity in the same transaction. You must create the entity and delete it with separate commits.

Mode changes, action items (such as `clear interface counters`), and `show` commands are not part of a transaction and are not displayed by the `show transaction current` command.

---

## confirm-commit

Use this command to commit configuration changes before the timeout in a “confirmed commit” operation.

Note: This command does not support the <persist-id> parameter as specified in RFC 6241.

### Command Syntax

```
confirm-commit
```

### Parameters

None

### Default

N/A

### Mode

All configuration modes

### Applicability

This command was introduced in OcNOS version 6.3.0.

### Example

```
(config)#router ospf 1
(config-router)#router ospf 2
(config-router)#commit confirmed timeout 100 description This is a test for confirmed
commit
(config-router)#
(config-router)#confirm-commit
```

---

## debug cml

Use this command to enable or disable CML sub-module logging.

### Command Syntax

```
debug cml (enable | disable) (events | engine | transaction | database | replace |  
smi | notification | all)
```

### Parameters

enable	Enable debugging.
disable	Disable debugging.
events	Enable/disable events debugging
engine	Enable/disable engine debugging
transaction	Enable/disable transaction debugging
database	Enable/disable database debugging
replace	Enable/disable replace debugging
smi	Enable/disable SMI debugging
notification	Enable/disable notification debugging
all	Enable/disable all debugging

### Default

By default, CML sub-module logging is disabled for all sub-modules.

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 4.2 and the `notification` parameter added in OcNOS version 6.1.0.

### Example

```
#debug cml enable transaction
```

---

## module notification

Use this command to enable or disable notification for a given protocol at a given notification severity level.

### Command Syntax

```
module PROTOCOL_NAME notification (enable|disable) (severity
    (all|info|warning|minor|major|critical) |)
```

### Parameters

PROTOCOL_NAME	Protocol name. Specify <code>all</code> for all protocols.
enable	Enable notification subscription
disable	Disable notification subscription
severity	If notification is enabled, then all notifications having severity higher than or equal to this severity allowed. If notification disabled then all the notifications having severity lower than or equal to this severity not allowed.
all	Notification severity all
critical	Notification severity critical
info	Notification severity info
major	Notification severity major
minor	Notification severity minor
warning	notification severity warning

### Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 6.0.0.

### Example

To enable notification for NSM for all severity levels:

```
#module nsm notification enable
```

To disable notifications for NSM for all severity levels:

```
#module nsm notification disable
```

To enable notifications for NSM for severity levels higher than or equal to major (major and critical):

```
#module nsm notification enable severity major
```

To disable notifications for NSM for severity levels lower than or equal to minor (info, warning, and minor):

```
#module nsm notification disable severity minor
```

---

## show cml config-datastore lock status

Use this command to display the configuration datastore lock state and its holder. The identifier of the process holding the lock is shown in parenthesis.

### Command Syntax

```
show cml config-datastore lock status
```

### Parameters

None

### Default

N/A

### Mode

Privileged exec mode

### Applicability

This command was introduced in OcNOS version 6.0.0.

### Example

```
#cml lock config-datastore candidate
#show cml config-datastore lock status
```

```
Running datastore is unlocked
Candidate datastore is locked by client cmlsh(2831)
Startup datastore is unlocked
#
```



---

## show cml notification status

Use this command to display notification status (enabled or disabled) for all CML clients.

### Command Syntax

```
show cml notification status
```

### Parameters

None

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 6.0.0.

### Example

To show notification status for all clients:

```
#show cml notification status
NETCONF notification enabled
CMLSH notification enabled
SNMP notification enabled
```

---

## show cmlsh multiple-config-session status

Use this command to display the multiple configuration mode session setting.

### Command Syntax

```
show cmlsh multiple-config-session status
```

### Parameters

None

### Default

N/A

### Mode

Privileged exec mode

### Applicability

This command was introduced in OcNOS version 5.1.

### Example

```
#cmlsh multiple-config-session enable
#
#show cmlsh multiple-config-session status
CMLSh multiple configuration session mode : Enabled
#
```

---

## show cmlsh notification status

Use this command to display the notification status (enabled or disabled) for the current CMLSH session.

### Command Syntax

```
show cmlsh notification status
```

### Parameters

None

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 6.0.0.

### Example

To show notification status for the CMLSH session.

```
# OcNOS#show cmlsh notification status  
CMLSH notification enabled.
```

---

## show max-transaction limit

Use this command to display the maximum number of transactions.

### Command Syntax

```
show max-transaction limit
```

### Parameters

None

### Default

N/A

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 5.0.

### Example

```
#show max-transaction limit  
Max-Transaction Limit is 30000
```

## show module-info

Use this command to display module's config and state configuration for any top-level object in the data model. This command can be used to display module configuration in XML or JSON format. This command is equivalent to a NETCONF GET operation.

### Command Syntax

```
show module-info OBJECT_NAME format (xml|json)
```

### Parameters

OBJECT_NAME	Name of the object, such as ISIS or OSPF
xml	XML output format
json	JSON output format

### Mode

All modes

### Applicability

This command was introduced in OcNOS version 6.0.0.

### Example

To display the user-session module's config and state configuration in XML format:

```
#show module-info user-session format xml
<user-session xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-user-session-management">
  <sessions>
    <session>
      <id>pts/0</id>
      <state>
        <id>pts/0</id>
        <user-role>network-admin</user-role>
        <type>Local</type>
        <process-identifier>1099</process-identifier>
        <idle-time>0d00h00m</idle-time>
        <client-type>CLI</client-type>
        <user-name>root</user-name>
        <line>130 vty 0</line>
      </state>
    </session>
  </sessions>
</user-session>
```

To display the user-session module's config and state configuration in JSON format:

```
#show module-info user-session format json
{
  "user-session": {
    "sessions": {
      "session": [
```

```
{
  "id": "pts/0",
  "state": {
    "id": "pts/0",
    "user-role": "network-admin",
    "type": "Local",
    "process-identifier": "1099",
    "idle-time": "0d00h00m",
    "client-type": "CLI",
    "user-name": "root",
    "line": "130 vty 0"
  }
}
]
```

---

## show running-config notification

Use this command to display the notification status (enabled or disabled) and notification severity levels.

### Command Syntax:

```
show running-config notification
```

### Parameters

None

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 6.0.0.

### Example

To display the notification status and notification severity levels.

```
#show running-config notification
!
module nsm notification enable severity major
!
```

---

## show system restore failures

Use this command to display configuration restoration status after save reload device.

### Command Syntax

```
show system restore failures
```

### Parameters

None

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 5.1.

### Example

Configuration restoration successful status information after save reload device:

```
#show system restore failures
Configuration restore from DB is completed.
Total no. of failed configuration objects = 0
```

Configuration restoration failure status information after save reload device:

```
#show system restore failures
Configuration restore from DB is completed.
Total no. of failed configuration objects = 1.
```

Failed Protocols information :

Protocol Name=ipi-interface, Protocol Id=3 :

Failed configuration object information :

Total no. of failed configuration objects = 1.

Object Name = config, DN = cmlAutoDummy3074=3074,name=eth0,cmlAutoDummy3073=3073 :

Error Information :

Total no. of configuration errors = 1.

ErrorCode = -16946, ErrorMessage = % No such VRF, ErrorXpath = /interfaces/  
interface[name='eth0']/config.



---

## show transaction current

Use this command to display the current transaction.

Mode changes, action items (such as `clear interface counters`), and `show` commands are not part of a transaction and are not displayed by this command.

### Command Syntax

```
show transaction current
```

### Parameters

None

### Default

N/A

### Mode

Exec mode and configure mode

### Applicability

This command was introduced in OcNOS version 5.0.

### Example

```
(config)#interface eth3
(config-if)#description testing
(config-if)#mtu 664
(config-if)#exit
(config)#show transaction current
interface eth3
description testing
mtu 664
```

---

## show transaction last-aborted

Use this command to display the last aborted transaction.

### Command Syntax

```
show transaction last-aborted
```

### Parameters

None

### Default

N/A

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 5.0.

### Example

```
(config)#router isis 4
(config-router)#isis wait-timer 45
(config-router)#net 11.22.33
(config-router)#exit
(config)#commit
%% Invalid NET length - /isis/isis-instance[instance='4']/config
(config)#show running-config isis
!
!
(config)#abort transaction
(config)#exit
#show transaction last-aborted
router isis 4
isis wait-timer 45
net 11.22.33
#
```

## show (xml|json) running-config|candidate-config

Use this command to display the running or candidate system configuration for any top-level object in the data model. This CLI can also be used for display full running or candidate system configuration for all protocol modules. This command can be used to display running or candidate system configuration in xml or json format. This command is equivalent to a NETCONF GET-CONFIG operation.

### Command Syntax

```
show (xml|json) (running-config| candidate-config) OBJECT_NAME
```

### Parameters

xml	XML output format
json	JSON output format
candidate-config	Candidate system configuration
running-config	Running system configuration
OBJECT_NAME	Name of the object, such as ISIS or OSPF

### Mode

All modes

### Applicability

This command was introduced before OcNOS version 4.2 and updated in OcNOS version 6.0.0.

### Example

To display the top level objects:

```
#show xml running-config
arp          bfd          bgp          dhcp          evpn          evpn-mpls
interfaces   ip-global  isis         key-chains    lacp          layer2-global
ldp          lldp       logging      mpls          neighbor-discovery network-instances
ospfv2       pcep       ping         prefixes       routemaps     routing
rsvp-te      segment-routing system-info  tacacs        time-ranges   vlan-classifier
vpls        vpws       vxlan
```

To display the ISIS running configuration in XML format:

```
#show xml running-config isis
<isis xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-isis">
  <isis-instance xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-isis">
    <instance>1</instance>
    <config xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-isis">
      <instance>1</instance>
      <vrf-name>default</vrf-name>
    </config>
  </isis-instance>
</isis>
```

To display the logging running configuration in XML format:

```
#show xml running-config logging
<logging xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-logging">
```

```
<rsyslog>
  <vrf>default</vrf>
  <config>
    <vrf>default</vrf>
    <enable-rsyslog>rsyslog</enable-rsyslog>
  </config>
</rsyslog>
</logging>
```

To display the logging running configuration in JSON format:

```
#show json running-config logging
{
  "logging":{
    "rsyslog":[
      {
        "vrf":"default",
        "config":{
          "vrf":"default",
          "enable-rsyslog":"rsyslog"
        }
      }
    ]
  }
}
```

To display the OSPFv2 candidate configuration in XML format:

```
#show xml candidate-config ospfv2
<ospfv2 xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-ospf">
  <processes>
    <process>
      <ospf-id>1</ospf-id>
      <config>
        <ospf-id>1</ospf-id>
        <vrf-name>default</vrf-name>
      </config>
    </process>
  </processes>
</ospfv2>
```

To display the OSPFv2 candidate configuration in JSON format:

```
#show json candidate-config ospfv2
{
  "ospfv2":{
    "processes":{
      "process":[
        {
          "ospf-id":"1",
          "config":{
            "ospf-id":"1",
            "vrf-name":"default"
          }
        }
      ]
    }
  }
}
```

```
}  
  ]  
    }  
  }  
}
```



---

## CHAPTER 9 DHCP Snooping Commands

---

This chapter describe the commands for DHCP snooping.

- [debug ip dhcp snooping](#)
- [ip dhcp snooping database](#)
- [renew ip dhcp snooping binding database](#)
- [show debugging ip dhcp snooping](#)
- [show debugging ip dhcp snooping](#)
- [show ip dhcp snooping arp-inspection statistics bridge](#)
- [show ip dhcp snooping bridge](#)
- [show ip dhcp snooping binding bridge](#)

---

## debug ip dhcp snooping

Use this command to enable the debugging DHCP snooping.

Use the `no` parameter to disable the debug options.

### Command Syntax

```
debug ip dhcp snooping (event|rx|tx|packet|all)
no debug ip dhcp snooping (event|rx|tx|packet|all)
```

### Parameters

event	Enable event debugging
rx	Enable receive debugging
tx	Enable transmit debugging
packet	Enable packet debugging
all	Enable all debugging

### Default

By default all debugging options are disabled.

### Command Mode

Exec mode and configure mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
#debug ip dhcp snooping all
#no debug ip dhcp snooping packet
```



---

## ip dhcp snooping database

Use this command to write the entries in the binding table to persistent storage.

### Command Syntax

```
ip dhcp snooping database bridge <1-32>
```

### Parameters

<1-32>	Bridge number
--------	---------------

### Default

No default value is specified.

### Command Mode

Privileged Exec Mode and Exec mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
#ip dhcp snooping database bridge 1
```

---

## renew ip dhcp snooping binding database

Use this command to populate the binding table by fetching the binding entries from persistent storage.

### Command Syntax

```
renew ip dhcp snooping (source|) binding database bridge <1-32>
```

### Parameters

<1-32>	Bridge number
source	IP source guard

### Default

No default value is specified.

### Command Mode

Privileged Exec Mode and Exec mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
#renew ip dhcp snooping binding database bridge 1
```

---

## show debugging ip dhcp snooping

Use this command to display the enabled debugging options.

### Command Syntax

```
show debugging ip dhcp snooping
```

### Parameters

None

### Command Mode

Privileged Exec Mode and Exec mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
#show debugging ip dhcp snooping
DHCP snoop debugging status:
DHCP snoop event debugging is on
DHCP snoop tx debugging is on
```

# show ip dhcp snooping arp-inspection statistics bridge

Use this command to show dhcp dynamic ARP inspection related statistics on bridge.

## Command Syntax

```
show ip dhcp snooping arp-inspection statistics bridge <1-32>
```

## Parameters

<1-32> Bridge number.

## Command Mode

Exec mode

## Applicability

This command was introduced in OcNOS-SP version 5.0.

## Examples

```
#show ip dhcp snooping arp-inspection statistics bridge 1
```

```
bridge      forwarded  dai dropped
-----
1           9          1
```

[Table 9-22](#) explains the fields in the output.

**Table 9-22: show ip dhcp snooping arp-inspection statistics bridge fields**

Field	Description
bridge	Bridge number.
forwarded	Number of forwarded packets.
dai dropped	Number of dropped packets.

---

## show ip dhcp snooping bridge

Use this command to display the DHCP configuration, including trusted ports, configured VLAN, active VLAN, and strict validation status.

### Command Syntax

```
show ip dhcp snooping bridge <1-32>
```

### Parameters

<1-32>                      Bridge number

### Command Mode

Exec mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
#show ip dhcp snooping bridge 1
```

```
Bridge Group                               : 1
DHCP snooping is                           : Enabled
DHCP snooping option82 is                  : Disabled
Verification of hwaddr field is            : Disabled
Strict validation of DHCP packet is         : Disabled
DB Write Interval(secs)                    : 300
DHCP snooping is configured on following VLANs : 20,30
DHCP snooping is operational on following VLANs : 20,30
```

DHCP snooping trust is configured on the following Interfaces

```
Interface           Trusted
-----
xe1                  Yes
```

DHCP snooping IP Source Guard is configured on the following Interfaces

```
Interface           Source Guard
-----
```

[Table 9-23](#) explains the fields in the output.

**Table 9-23: show ip dhcp snooping bridge fields**

Field	Description
Bridge Group	Bridge number
DHCP snooping is	Whether DHCP snooping is enabled

**Table 9-23: show ip dhcp snooping bridge fields (Continued)**

Field	Description
DHCP snooping option82 is	Whether DHCP snooping option 82 is enabled
Verification of hwaddr field is	Whether verification of hwaddr field is enabled
Strict validation of DHCP packet is	Whether strict validation of DHCP packets is enabled
DB Write Interval(secs)	Database write interval in seconds
DHCP snooping is configured on following VLANs	VLANs on which DHCP snooping is enabled
DHCP snooping is operational on following VLANs	VLANs on which DHCP snooping is operating
Interface	Interface name
Trusted	Whether DHCP snooping trust is enabled on the interface
Source Guard	Whether DHCP snooping IP source guard is enabled on the interface

## show ip dhcp snooping binding bridge

Use this command to display the DHCP snooping binding table.

### Command Syntax

```
show ip dhcp snooping binding bridge <1-32>
```

### Parameters

<1-32>                      Bridge number

### Command Mode

Exec mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
#show ip dhcp snooping binding bridge 1
```

```
Total number of static IPV4 entries           : 0
Total number of dynamic IPV4 entries           : 2
Total number of static IPV6 entries            : 0
Total number of dynamic IPV6 entries           : 0
```

MacAddress	IpAddress	Lease (sec)	Type	VLAN	Interface
3cfd.fe0b.06e0	12.12.12.10	30	dhcp-snooping	20	xe12
3cfd.fe0b.06e0	30.30.30.30	480	dhcp-snooping	30	xe12

[Table 9-24](#) explains the output .

**Table 9-24: show ip dhcp snooping binding bridge fields**

Field	Description
Total number of static IPV4 entries	Number of static IPV4 entries.
Total number of dynamic IPV4 entries	Number of dynamic IPV4 entries.
Total number of static IPV6 entries	Number of static IPV6 entries.
Total number of dynamic IPV6 entries	Number of dynamic IPV6 entries .
MacAddress	MAC address of the interface.
IP Address	IP address of the peer device.
Lease (sec)	DHCP lease time in seconds provided to untrusted IP addresses.
Type	Configured either statically or dynamically by the DHCP server.

**Table 9-24: show ip dhcp snooping binding bridge fields**

Field	Description
VLAN	Identifier of the number.
Interface	Interface is being snooped.



## CHAPTER 10 DHCPv6 Prefix delegation Commands

---

This chapter describes the Dynamic Host Configuration Protocol (DHCP) v6 Prefix delegation commands.

The prefix delegation feature lets a DHCP server assign prefixes chosen from a global pool to DHCP clients. The DHCP client can configure an IPv6 address on its LAN interface using the prefix it received. Then it send router advertisements including the prefix, allowing other devices to auto configure their own IPv6 addresses.

Enable OcNOS device DHCP Client to receive the prefixes from external DHCP Server and enable IPv6 address autoconfiguration of LAN interfaces and the respective host machines.

This feature enables the service providers to assign IP for the Customer Premise Equipment acting as a router between the service providers core network and subscribers internal network.

This chapter contains these commands:

- `ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER`
- `ipv6 address PREFIX_FROM_SERVER X:X::X:X/M`
- `ipv6 address autoconfig`
- `show ipv6 dhcp interface`

---

## ipv6 dhcp prefix-delegation PREFIX\_FROM\_SERVER

Use this command to enable the DHCPv6 client to request the prefix (IA\_PD) for the interface.

Prefixes delegated by the DHCP server are stored in the general prefix called PREFIX\_FROM\_SERVER.

Use the no form of command to remove the IA\_PD option from the DHCPv6 client request. And this CLI deletes the learned prefix if there are any.

### Command Syntax

```
ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER
no ipv6 dhcp prefix-delegation
```

### Parameters

PREFIX\_FROM\_SERVER

String with length of no more than 255 characters and designates the name of the learnt prefix.

### Default

DHCPv6 Prefix delegation client is not enabled by default.

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS version 1.3.9

### Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ipv6 dhcp prefix-delegation prefix_xe1
(config-if)#
```

---

## ipv6 address PREFIX\_FROM\_SERVER X:X::X:X/M

Use this command to configure the global IPv6 address using the learned prefix and user provided suffix.

Use the `no` form of this command to remove the configuration.

### Command Syntax

```
ipv6 address PREFIX_FROM_SERVER X:X::X:X/M
no ipv6 address PREFIX_FROM_SERVER X:X::X:X/M
```

### Parameters

PREFIX\_FROM\_SERVER

Name of the prefix which stores the address-prefix learnt using prefix delegation enabled in the client interface

X:X::X:X/M

Suffix address consists subnet id and host address. This value must start with '::', and end with /64 bit prefix.

### Default

DHCPv6 IA\_PD option is not requested by default.

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS version 1.3.9

### Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ipv6 address dhcp
(config-if)#ipv6 dhcp prefix-delegation prefix_xe1
(config-if)#

(config)#interface xe3
(config-if)#ipv6 address prefix_xe1 ::1:0:0:0:1/64
(config-if)#
```

---

## ipv6 address autoconfig

Use this command to enable autoconfiguration of IPv6 address in host interface. IPv6 address are formed using the Prefix learnt from RA and suffix formed using EUI-64 method.

Autoconfiguration of ipv6 address will be successful only when the received prefix length is 64.

Use the `no` form of this command to disable the ipv6 address autoconfiguration.

### Command Syntax

```
ipv6 address autoconfig
```

### Parameters

None

### Default

No default value specified.

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS version 1.3.9

### Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 address autoconfig
```

---

## show ipv6 dhcp interface

Use this command to display the DHCPv6 Prefix delegation information in the Requesting Router device

### Command Syntax

```
show ipv6 dhcp interface
```

### Parameters

None

### Command Mode

Executive mode

### Applicability

This command was introduced in OcNOS version 1.3.9

### Examples

```
#show ipv6 dhcp interface
xe1 is in client mode
prefix name: prefix_xe1
learned prefix: 1212:501:102::/48
preferred lifetime 600, valid lifetime 600
interfaces using the learned prefix
xe3      1212:501:102:1::1
```



## CHAPTER 11 Digital Diagnostic Monitoring Commands

---

This chapter provides a description, syntax, and examples of DDM feature commands:

- [clear ddm transceiver alarm](#)
- [clear ddm transceiver alarm all](#)
- [ddm monitor](#)
- [ddm monitor all](#)
- [ddm monitor interval](#)
- [debug ddm](#)
- [service unsupported-transceiver](#)
- [show controller details](#)
- [show supported-transceiver](#)
- [show interface transceiver details](#)

---

## clear ddm transceiver alarm

Use this command to clear the transceiver alarm in the DDM monitor at interface level.

### Command Syntax

```
clear ddm transceiver alarm
```

### Default

None

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

To configure at interface level:

```
(config)#interface xe1  
(config-if)#clear ddm transceiver alarm
```



---

## clear ddm transceiver alarm all

Use this command to clear the transceiver DDM alarm for all interfaces.

### Command Syntax

```
clear ddm transceiver alarm all
```

### Parameters

None

### Default

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

To configure at overall interface level:

```
OcNOS#clear ddm transceiver alarm all
```

---

## ddm monitor

Use this command to enable DDM monitoring for interfaces which have a supported transceiver.

Use the `no` form of this command to disable DDM monitoring for all transceivers.

### Command Syntax

```
ddm monitor
no ddm monitor
```

### Parameters

None

### Default

By default, DDM monitoring is disabled.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#interface xe1
(config-if)#ddm monitor
(config-if)#exit

(config)#interface xe1
(config-if)#no ddm monitor
(config-if)#exit
```

---

## ddm monitor all

Use this command to enable DDM monitoring for all transceiver.s

Use the `no` form of this command to disable DDM monitoring for all transceivers.

### Command Syntax

```
ddm monitor all
no ddm monitor all
```

### Parameters

None

### Default

By default, DDM monitoring is disabled.

### Command Mode

Configuration mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#ddm monitor all

(config)#no ddm monitor all
```

---

## ddm monitor interval

Use this command to set the monitoring interval for the transceiver.

Use no form with this command to set the monitoring interval to its default.

### Command Syntax

```
ddm monitor interval <60-3600>
no ddm monitor interval
```

### Parameters

<60-3600>            Interval period in seconds.

### Default

The default monitoring interval is 60 seconds.

### Command Mode

Configuration mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#ddm monitor interval 60
```

---

## debug ddm

Use this command to enable or disable debugging for DDM.

### Command Syntax

```
debug ddm
no debug ddm
```

### Parameters

None

### Default

By default, debug command is not configured.

### Command Mode

Configuration mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#debug ddm
(config)#no debug ddm
```

---

## service unsupported-transceiver

Use this command to allow an unsupported transceiver to be enabled for DDM monitoring.

Use the `no` form of this command to disable DDM on an unsupported transceiver.

### Command Syntax

```
service unsupported-transceiver
no service unsupported-transceiver
```

### Parameters

None

### Default

By default, DDM on an unsupported transceiver is disabled.

### Command Mode

Configuration mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#service unsupported-transceiver

(config)#no service unsupported-transceiver
```

---

## show controller details

Use this command to display the EEPROM details of transceiver.s

### Command Syntax

```
show interface (IFNAME|) controllers
```

### Parameters

IFNAME	Interface name. If not specified, this command displays details of all connected transceivers.
--------	--

### Default

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show interface xe52/1 controllers
```

```
Port Number           : 52
Vendor oui             : 0x0 0x17 0x6a
Vendor name           : AVAGO
Vendor part_no        : AFBR-79E4Z
serial_number         : QB380161
transceiver_type      : QSFP OR LATER
connector_type        : MPO 1x12
qsfp_transceiver_code : 1X-LX
vendor_rev            : 01
date_code             : 110920   (yymmddvv, v=vendor specific)
encoding              : SONET
br_nominal            : 103      (100 MHz)
length_km             : 0
length_mtr            : 50
length_50mt           : 0
length_62_5mt         : 0
length_cu             : 0
cc_base               : 0x7d
cc_ext                : 0x28
DDM Support           : yes
```

---

# show supported-transceiver

Use this command to display supported transceivers.

## Command Syntax

```
show supported-transceiver
```

## Parameters

None

## Default

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#show supported-transceiver
-----
                Transceiver DDM support list
-----
Type                :SFP
Vendor Name          :FINISAR CORP
Vendor Part Number   :FTLF8519P2BNL
DDM Supported        :Yes

Type                :SFP
Vendor Name          :EVERTZ
Vendor Part Number   :SFP10G-TR13S
DDM Supported        :Yes

Type                :QSFP
Vendor Name          :AVAGO
Vendor Part Number   :AFBR-79E4Z
DDM Supported        :Yes
```



---

## show interface transceiver details

Use this command to display details of transceivers and threshold violations.

### Command Syntax

```
show interface (IFNAME|) transceiver (detail|threshold violation|)
```

### Parameters

IFNAME	Interface name. If not specified, this command displays details of all connected transceivers.
detail	Transceiver information such as voltage, temperature, power, and current.
threshold violation	Transceiver threshold violations.

### Default

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show interface transceiver detail
PORT      Temp      High Alarm High Warn Low Warn Low Alarm
          (Celsius) (Celsius) (Celsius) (Celsius) (Celsius)
-----
5          30.060      95          90          -20         -25
6          30.463      95          90          -20         -25
52         34.486      75          70           0          -5
53         30.764      75          70           0          -5

          Voltage  High Alarm High Warn Low Warn Low Alarm
          (Volts)  (Volts)   (Volts)   (Volts)   (Volts)
-----
5          3.339      3.900      3.700      2.900      2.700
6          3.365      3.900      3.700      2.900      2.700
52         3.360      3.630      3.465      3.135      2.970
53         3.353      3.630      3.465      3.135      2.970

          Current  High Alarm High Warn Low Warn Low Alarm
          (mA)     (mA)       (mA)       (mA)       (mA)
-----
5          6.468      17.000     14.000     2.000      0.034
6          7.014      17.000     14.000     2.000      0.034
52         7.250      10.000     9.500      1.000      0.500
53         7.284      10.000     9.500      1.000      0.500
```

	RxPower (dBm)	High Alarm (dBm)	High Warn (dBm)	Low Warn (dBm)	Low Alarm (dBm)
5	0.332	1.259	0.794	0.016	0.010
6	0.321	1.259	0.794	0.016	0.010
52	0.727	2.188	1.738	0.112	0.000
53	0.352	2.188	1.738	0.112	0.000

	TxPower (mW)	High Alarm (mW)	High Warn (mW)	Low Warn (mW)	Low Alarm (mW)
5	0.342	0.631	0.631	0.079	0.067
6	0.342	0.631	0.631	0.079	0.067

Table 11-25 explains the output fields.

Table 11-25: show interface transceiver details output

Field	Description
Port	The number of the transceiver port.
Temp	Temperature in degrees Celsius of the transceiver.
Voltage	Voltage in Volts on the transceiver.
Current	Current in Milliampere used by the transceiver.
Rx Power	Power received in Decibel-milliwatts (dBm) by the transceiver.
Tx Power	Power being transmitted in milliWatts by the transceiver.
High Alarm	The level that is needed to be reached to trigger a high alarm.
High Warn	The level that is needed to be reached to trigger a high warning.
Low Warn	The level that is needed to be reached to trigger a low warning.
Low Alarm	The level that is needed to be reached to trigger a low alarm.

## CHAPTER 12 Dynamic Host Configuration Protocol Client

---

This chapter describes the Dynamic Host Configuration Protocol (DHCP) client commands.

DHCP is used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). DHCP is implemented in a client-server model where DHCP clients request configuration data, such as an IP address, a default route, or DNS server addresses from a DHCP server.

This chapter contains these commands:

- `feature dhcp`
- `ip address dhcp`
- `ip dhcp client request`
- `ipv6 address dhcp`
- `ipv6 dhcp address-prefix-length`
- `ipv6 dhcp client request`
- `ipv6 dhcp client`
- `show ipv6 dhcp vendor-opts`

---

## feature dhcp

Use this command to enable the DHCP client and DHCP relay on the device.

Use the `no` form of this command to disable the DHCP client and DHCP relay and delete any DHCP-related configuration.

### Command Syntax

```
feature dhcp
no feature dhcp
```

### Parameters

None

### Default

By default, feature dhcp is disabled

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#feature dhcp
```

---

## ip address dhcp

Use this command to get an IP address from a DHCP server for this interface.

Use the `no` form of this command to disable the DHCP client for this interface.

You can give the [ip dhcp client request](#) command before giving this command to request additional options.

### Command Syntax

```
ip address dhcp
no ip address dhcp
```

### Parameters

None

### Default

No default value is specified.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip address dhcp
(config-if)#
```

---

## ip dhcp client request

Use this command to add an option to a DHCP request.

Use the `no` form of this command to remove an option from a DHCP request.

### Command Syntax

```
ip dhcp client request dns-nameserver
ip dhcp client request host-name
ip dhcp client request log-server
ip dhcp client request ntp-server
no ip dhcp client request dns-nameserver
no ip dhcp client request host-name
no ip dhcp client request log-server
no ip dhcp client request ntp-server
```

### Parameters

<code>dns-nameserver</code>	List of DNS name servers (DHCP option 6)
<code>host-name</code>	Name of the client (DHCP option 12)
<code>ntp-server</code>	List of NTP servers (DHCP option 42)
<code>log-server</code>	List of log servers (DHCP option 7)

### Default

By default, `ip dhcp client request` is enabled

### Command Mode

Interface mode

### Applicability

This command was introduced before OcnOS version 1.3.

### Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip dhcp client request ntp-server
```

---

## ipv6 address dhcp

Use this command to get an IPV6 address from a DHCP server for this interface.

Use the `no` form of this command to disable the DHCP client for this interface.

You can give the `ipv6 dhcp client request` command before giving this command to request additional options.

### Command Syntax

```
ipv6 address dhcp
no ipv6 address dhcp
```

### Parameters

None

### Default

No default value is specified.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 address dhcp
(config-if)#
```

---

## ipv6 dhcp address-prefix-length

Use this command to configure the prefix-length for dynamically allocated IPv6 address.

Use the `no` form of this command to unconfigure the prefix-length.

### Command Syntax

```
ipv6 dhcp address-prefix-length <1-128>
no ipv6 dhcp address-prefix-length
```

### Parameters

<1-128>	IPv6 address prefix length
---------	----------------------------

### Default

Default ipv6 address prefix length is 128

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ipv6 dhcp address-prefix-length 64
(config-if)
```



---

## ipv6 dhcp client request

Use this command to add an option to a DHCPv6 request.

Use the `no` form of this command to remove an option from a DHCPv6 request.

Note:

- Vendor-specific options allow a specific vendor to define a set of DHCP options that really make sense for their device or operating system.
- By default DHCPv6 uses four messages exchange (Solicit, Advertise, Request, and Reply) to obtain configuration parameters from a server. But when rapid-commit is specified, `dhcp6-client` will include a rapid-commit option in solicit messages and wait for an immediate reply instead of advertisements. The Rapid Commit option is used to signal the use of the two message exchange for address assignment.

### Command Syntax

```
ipv6 dhcp client request dns-nameserver
ipv6 dhcp client request ntp-server
ipv6 dhcp client request domain-search
ipv6 dhcp client request vendor-specific-information
ipv6 dhcp client request rapid-commit
no ipv6 dhcp client request rapid-commit
no ipv6 dhcp client request vendor-specific-information
no ipv6 dhcp client request domain-search
no ipv6 dhcp client request ntp-server
no ipv6 dhcp client request dns-nameserver
```

### Parameters

<code>dns-nameserver</code>	List of DNS name servers
<code>ntp-server</code>	Request for IPv6 NTP server
<code>domain-search</code>	Request for IPv6 domain search
<code>vendor-specific-information</code>	Request for IPv6 vendor-specific-information
<code>rapid-commit</code>	Request to enable rapid-commit

### Default

No default value is specified.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3 and modified in OcNOS-DC version 5.0

## Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 dhcp client request dns-nameserver
(config-if)#

(config)#interface eth0
(config-if)#ipv6 dhcp client request ntp-server
(config-if)#exit

(config)#interface eth0
(config-if)#ipv6 dhcp client request domain-search
(config-if)#exit

(config)#interface eth0
(config-if)#ipv6 dhcp client request vendor-specific-information
(config-if)#exit

(config)#interface eth0
(config-if)#ipv6 dhcp client request rapid-commit
(config-if)#exit
```

---

## ipv6 dhcp client

Use this command to configure DHCP client options to a DHCPv6 request.

Use the `no` form of this command to remove client options from a DHCPv6 request.

Note:

- `ipv6 dhcp client information-request` is used to get only stateless configuration parameters (i.e., without address).
- DAD-wait-time value is the maximum time (in seconds) that the client should wait for the duplicate address detection (DAD) to complete on an interface.
- DUID option override the default when selecting the type of DUID to use. By default, DHCPv6 dhclient creates an identifier based on the link-layer address (DUID-LL) if it is running in stateless mode (with `-S`, not requesting an address), or it creates an identifier based on the link-layer address plus a timestamp (DUID-LLT) if it is running in stateful mode (without `-S`, requesting an address).

### Command Syntax

```
ipv6 dhcp client information-request
ipv6 dhcp client dad-wait-time <1-600>
ipv6 dhcp client duid (ll | llt)
no ipv6 dhcp client duid
no ipv6 dhcp client dad-wait-time
no ipv6 dhcp client information-request
```

### Parameters

<code>information-request</code>	Request to enable information-request
<code>&lt;1-600&gt;</code>	DAD wait-time in seconds
<code>ll</code>	Link-layer address
<code>llt</code>	Link-layer address plus timestamp

### Default

No default value is specified.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3 and modified in OcNOS-DC version 5.0

### Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 dhcp client information-request
(config-if)#exit
```

```
(config)#interface eth0
(config-if)#ipv6 dhcp client dad-wait-time 20
(config-if)#exit
```

```
(config)#interface eth0
(config-if)#ipv6 dhcp client duid 11
(config-if)#exit
```

---

## show ipv6 dhcp vendor-opts

Use this command to display vendor-specific-information option value given by DHCP server.

### Command Syntax

```
show ipv6 dhcp vendor-opts
```

### Parameters

None

### Command Mode

Executive mode

### Applicability

This command is introduced in OcNOS-DC version 5.0

### Examples

```
OcNOS#sh ipv6 dhcp vendor-opts
ifName          vendor-opts
=====
xe5              IP Infusion Inc
OcNOS#
```



---

## CHAPTER 13 Dynamic Host Configuration Protocol Relay

---

This chapter describes the Dynamic Host Configuration Protocol (DHCP) relay commands.

In small networks with only one IP subnet, DHCP clients communicate directly with DHCP servers. When DHCP clients and associated servers do not reside on the same subnet, a DHCP relay agent can forward DHCP client messages to a DHCP server.

The DHCP client broadcasts on the local link, the relay agents receive the broadcast DHCP messages, and then generates a new DHCP message to send out on another interface.

The relay agent sets the gateway IP address (`giaddr` field of the DHCP packet) and, if configured, adds the relay agent information option (option 82) to the packet and forwards it to the DHCP server. The DHCP server replies to the client and the relay agent then retransmits the response on the local network.

This chapter contains these commands:

- `clear ip dhcp relay option statistics`
- `clear ip dhcp relay statistics`
- `ip dhcp relay (configure mode)`
- `ip dhcp relay (interface mode)`
- `ip dhcp relay address`
- `ip dhcp relay address global`
- `ip dhcp relay information option`
- `ip dhcp relay information option always-on`
- `ip dhcp relay information source-ip`
- `ip dhcp relay (L3VPN)`
- `ipv6 dhcp relay (configure mode)`
- `ipv6 dhcp relay (interface mode)`
- `ipv6 dhcp relay address`
- `ipv6 dhcp relay address global`
- `ipv6 dhcp relay subscriber-id`
- `ipv6 dhcp relay (L3VPN)`
- `show ip dhcp relay`
- `show ip dhcp relay address`
- `show ip dhcp relay option statistics`
- `show ip dhcp relay statistics`
- `show ipv6 dhcp relay`
- `show ipv6 dhcp relay address`
- `show running-config dhcp`

---

## clear ip dhcp relay option statistics

Use this command to clear ipv4 relay option statistics.

### command syntax

```
clear ip dhcp relay option statistics
```

### Parameters

None

### Command Mode

Executive mode

### Applicability

This command was introduced in OcNOS version 1.3.9.

### Examples

```
OcNOS#clear ip dhcp relay option statistics
```



---

## clear ip dhcp relay statistics

Use this command to clear ipv4 relay statistics.

### Command syntax

```
clear ip dhcp relay statistics
```

### Parameters

None

### Command Mode

Executive mode

### Applicability

This command was introduced in OcNOS version 1.3.9.

### Examples

```
OcNOS#clear ip dhcp relay statistics
```

---

## ip dhcp relay (configure mode)

Use this command to enable the DHCP relay agent. The DHCP relay starts forwarding packets to the DHCP server address once configured.

Use the `no` form of this command to disable the DHCP relay agent.

### Command Syntax

```
ip dhcp relay
no ip dhcp relay
```

### Parameters

None

### Default

By default, this feature is enabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip dhcp relay

#configure terminal
(config)#no ip dhcp relay
```

---

## ip dhcp relay (interface mode)

Use this command to configure an interface as a DHCP client-facing port.

Use the `no` form of this command to remove an interface as a DHCP client-facing port.

### Command Syntax

```
ip dhcp relay
no ip dhcp relay
```

### Parameters

None

### Default

By default, this feature is enabled

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS version 1.3.8.

### Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ip dhcp relay
```

---

## ip dhcp relay address

Use this command to set an IPv4 address of a DHCP server to which a DHCP relay agent forwards client requests.

Use the `no` form of this command to remove the IP address of a DHCP server.

You must enable the DHCP relay feature with the [ip dhcp relay \(configure mode\)](#) command before you give this command.

### Command Syntax

```
ip dhcp relay address A.B.C.D
no ip dhcp relay address A.B.C.D
```

### Parameters

A.B.C.D	IPv4 address of the DHCP server
---------	---------------------------------

### Default

No default value is specified

### Command Mode

Configure mode

VRF mode

### Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

### Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay address 198.51.100.127

#configure terminal
(config)#ip dhcp relay address 198.51.100.127
```

---

## ip dhcp relay address global

When the IPv4 DHCP server resides in a different VPN or global space that is different from the VPN, then use this command to specify the name of the VRF or global space in which the DHCP server resides.

Use the no form of this command to remove the VRF in which IPv4 DHCP server resides.

### Command Syntax

```
ip dhcp relay address A.B.C.D global (|VRF-NAME)
no ip dhcp relay address A.B.C.D global
```

### Parameters

A.B.C.D	IPv4 address of the DHCP server
VRF-NAME	Name of VRF where the DHCP server is present

### Default

If no input given, default VRF is the default Value.

### Command Mode

Configure mode

VRF mode

### Applicability

This command was introduced in OcNOS-DC version 5.1.

### Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay address 198.51.100.127 global

#configure terminal
(config)#ip dhcp relay address 198.51.100.127 global vrf1
```

---

## ip dhcp relay information option

Use this command to enable the device to insert and remove option 82 information in DHCP packets forwarded by the relay agent.

The option 82 suboption remote-id can be configured either as hostname or any string you provide.

Use the `no` form of this command to disable inserting and removing option-82 information.

### Command Syntax

```
ip dhcp relay information option (|remote-id (hostname|WORD))
no ip dhcp relay information option (|remote-id)
```

### Parameters

remote-id	Remote host Identifier, either the system hostname or a user-specified string.
hostname	Name of the host
WORD	Specify a string as remote-id(Maximum 255 alphanumeric characters)

### Default

No default value is specified

### Command Mode

Configure mode

VRF mode

### Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

### Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay information option remote-id hostname

#configure terminal
(config)#ip dhcp relay information option

#configure terminal
(config)#no ip dhcp relay information option
```

---

## ip dhcp relay information option always-on

Use this command to enable the device to insert options 82 information in DHCP packets forwarded by the relay-agent and keep them while forwarding to client.

Use the `no` form of this command to disable the option-82 always-on information.

### Command Syntax

```
ip dhcp relay information option always-on
no ip dhcp relay information option always-on
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Configure mode

VRF mode

### Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 6.2.0.

### Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay information option always-on

#configure terminal
(config)#ip dhcp relay information option always-on

#configure terminal
(config)#no ip dhcp relay information option always-on
```

---

## ip dhcp relay information source-ip

Use this command to enable DHCP relay option 82 link selection.

Use the `no` form of this command to disable DHCP relay option 82 link selection.

### Command Syntax

```
ip dhcp relay information source-ip A.B.C.D
no ip dhcp relay information source-ip
```

### Parameters

A.B.C.D	IPv4 address
---------	--------------

### Command Mode

Configure mode

VRF mode

### Default

No default value is specified.

### Applicability

This command was introduced before OcNOS version 1.3.6.

### Example

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay information option source-ip 2.2.2.2

#configure terminal
(config)#ip dhcp relay information option source-ip 3.3.3.3
```



---

## ip dhcp relay (L3VPN)

Use this command to specify IPv4 DHCP relay to use tunnel interfaces as Uplink/Downlink.

Use the `no` form of this command to remove the usage of tunnel interfaces in IPv4 DHCP relay.

### Command Syntax

```
ip dhcp relay (uplink|downlink) (l3vpn)
no ip dhcp relay (uplink|downlink) (l3vpn)
```

### Parameters

uplink	DHCP Relay uplink interface
downlink	DHCP Relay downlink interface
l3vpn	L3VPN interface

### Default

No default value is specified.

### Command Mode

Configure and VRF mode

### Applicability

This command was introduced in OcNOS-DC version 5.0.

### Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay uplink l3vpn
(config-vrf)#end

#configure terminal
(config)#ip dhcp relay uplink l3vpn
```

---

## ipv6 dhcp relay (configure mode)

Use this command to enable the DHCP IPv6 relay agent.

Use the `no` form of this command to disable the DHCP IPv6 relay agent.

### Command Syntax

```
ipv6 dhcp relay
no ipv6 dhcp relay
```

### 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)#ipv6 dhcp relay

#configure terminal
(config)#no ipv6 dhcp relay
```

---

## ipv6 dhcp relay (interface mode)

Use this command to configure an interface as a DHCP IPv6 client-facing port.

Use the no form of this command to remove an interface as a DHCP IPv6 client-facing port.

### Command Syntax

```
ipv6 dhcp relay
no ipv6 dhcp relay
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS version 1.3.8.

### Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 dhcp relay
```

---

## ipv6 dhcp relay address

Use this command to set an IPv6 address of a DHCP server to which a DHCP relay agent forwards client requests.

Use the `no` form of this command to remove an IPv6 address of a DHCP server.

You must enable the IPv6 DHCP relay feature with the [ipv6 dhcp relay \(configure mode\)](#) command before you give this command.

### Command Syntax

```
ipv6 dhcp relay address X:X::X:X  
no ipv6 dhcp relay address X:X::X:X
```

### Parameters

X:X::X:X	IPv6 address of the DHCP server
----------	---------------------------------

### Default

No default value is specified

### Command Mode

Configure mode

VRF mode

### Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

### Examples

```
#configure terminal  
(config)#ip vrf vrf1  
(config-vrf)#ipv6 dhcp relay address 2001:db8::7F  
  
#configure terminal  
(config)#ipv6 dhcp relay address 2001:db8::7F
```

---

## ipv6 dhcp relay address global

When the IPv6 DHCP server resides in a different VPN or global space that is different from the VPN, then use this command to specify the name of the VRF or global space in which the DHCP server resides.

Use the no form of this command to remove the VRF in which IPv6 DHCP server resides.

### Command Syntax

```
ipv6 dhcp relay address X:X::X:X global (|VRF-NAME)
no ipv6 dhcp relay address X:X::X:X global
```

### Parameters

X:X::X:X	IPv6 address of the DHCP server
VRF-NAME	Name of VRF where the DHCP server is present

### Default

If no input given, default VRF is the default Value.

### Command Mode

Configure mode

VRF mode

### Applicability

This command was introduced in OcNOS-DC version 5.1.

### Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp relay address 2001:db8::7F global

#configure terminal
(config)#ipv6 dhcp relay address 2001:db8::7F global vrf1
```

---

## ipv6 dhcp relay subscriber-id

Use this command to configure subscriber-ID for IPv6 DHCP relay.

Use `no` form of this command to disable subscriber-id.

### Command Syntax

```
ipv6 dhcp relay information option subscriber-id WORD
no ipv6 dhcp relay information option subscriber-id
```

### Parameters

WORD	Subscriber ID
------	---------------

### Default

No default value is specified.

### Command Mode

Configuration mode and VRF mode

### Applicability

This command is introduced in OcNOS-DC version 5.0

### Examples

```
#configure terminal
(config)#ipv6 dhcp relay information option subscriber-id test
(config)#exit
```

---

## ipv6 dhcp relay (L3VPN)

Use this command to specify IPv6 DHCP relay to use tunnel interfaces as Uplink/Downlink.

Use the `no` form of this command to remove the usage of tunnel interfaces in IPv6 DHCP relay.

### Command Syntax

```
ipv6 dhcp relay (uplink|downlink) (l3vpn)
no ipv6 dhcp relay (uplink|downlink) (l3vpn)
```

### Parameters

uplink	DHCP Relay uplink interface
downlink	DHCP Relay downlink interface
l3vpn	L3VPN interface

### Default

No default value is specified.

### Command Mode

Configure and VRF mode

### Applicability

This command was introduced in OcNOS-DC version 5.0.

### Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp relay uplink l3vpn
(config-vrf)#end

#configure terminal
(config)#ipv6 dhcp relay uplink l3vpn
```

# show ip dhcp relay

Use this command to display DHCP snooping relay status including DHCP server addresses configured on interfaces.

## Command Syntax

```
show ip dhcp relay
```

## Parameters

None

## Command Mode

Executive mode

## Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

## Examples

```
#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: vrfl
  Option 82: Enabled
  Remote Id: ocnos-device
  Link selection Source-IP: 1.4.5.6
  DHCP Servers configured: 9.9.9.9 8.8.8.8
  Interface                Uplink/Downlink
  -----                -
  ge10                      Uplink
  ge28                      Downlink
VRF Name: default
  Option 82: Enabled
  Remote Id: OcNOS
  Link selection Source-IP: 1.2.3.4
  DHCP Servers configured: 1.1.1.1 2.2.2.2
  Interface                Uplink/Downlink
  -----                -
  ge11                      Uplink
  ge27                      Downlink
```

Table 13-26 explains the output fields.

Table 13-26: show ip dhcp relay fields

Entry	Description
DHCP relay service	Whether the DHCP relay service is enabled.
VRF Name	Name of the VRF.
Option 82	Whether option 82 is enabled.
Remote Id	Remote host Identifier.



**Table 13-26: show ip dhcp relay fields (Continued)**

Entry	Description
Link selection Source-IP	Option 82 link selection source IP address
DHCP Servers configured	Addresses of DHCP servers configured
Interface	Interface name
Uplink/Downlink	Whether the interface is a server-facing port (uplink) or a client-facing port (downlink).

# show ip dhcp relay address

Use this command to display DHCP relay addresses.

## Command Syntax

```
show ip dhcp relay address
```

## Parameters

None

## Command Mode

Executive mode

## Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

## Examples

```
#show ip dhcp relay address
VRF Name: vrf1
  DHCP Servers configured: 9.9.9.9 8.8.8.8
VRF Name: default
  DHCP Servers configured: 1.1.1.1 2.2.2.2
```

[Table 13-27](#) explains the output.

Table 13-27: show ip dhcp relay address interface fields

Entry	Description
VRF Name	Name of the VRF.
DHCP Servers configured	Addresses of DHCP servers configured

---

## show ip dhcp relay option statistics

Use this command to display IPv4 DHCP Relay Agent Option(Option82) packet statistics

### command syntax

```
show ip dhcp relay option statistics
```

### Parameters

None

### Command Mode

Executive mode

### Applicability

This command was introduced in OcNOS version 1.3.9.

### Examples

```
OcNOS#sh ip dhcp relay option statistics
VRF Name: default
Remote ID : OcNOS
Circuit ID : ge5
Number of packets forwarded without agent options : 0
Dropped pkts due to bad relay agent information option : 0
Dropped pkts due to no RAI option match found : 0
Circuit ID option is not matching with known circuit ID : 0
Circuit ID option in matching RAI option was missing : 0
OcNOS#
```

---

## show ip dhcp relay statistics

Use this command to display IPv4 DHCP relayed packet statistics.

### command syntax

```
show ip dhcp relay statistics
```

### Parameters

None

### Command Mode

Executive mode

### Applicability

This command was introduced in OcNOS version 1.3.9.

### Examples

```
OcNOS#sh ip dhcp relay statistics
VRF Name: default
Packets sent with a bogus giaddr : 0
Packets relayed from client to server : 12
Errors sending packets to servers : 0
Packets relayed from server to client : 1
Errors sending packets to clients : 0
OcNOS#
```

---

## show ipv6 dhcp relay

Use this command to display DHCP IPv6 snooping relay status including DHCP IPv6 server addresses configured on interfaces.

### Command Syntax

```
show ipv6 dhcp relay
```

### Parameters

None

### Command Mode

Executive mode

### Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

### Examples

```
#show ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: vrfl
  DHCPv6 Servers configured: 2001::1
  Interface                  Uplink/Downlink
  -----
  ge35                       Uplink
  xe50                       Downlink
VRF Name: default
  DHCPv6 Servers configured: 3001::1
  Interface                  Uplink/Downlink
  -----
  ge34                       Uplink
  xe49                       Downlink
```

[Table 13-28](#) explains the output fields.

**Table 13-28: show ipv6 dhcp relay fields**

Entry	Description
IPv6 DHCP relay service	Whether the DHCP relay service is enabled.
VRF Name	Name of the VRF.
DHCPv6 Servers configured	Addresses of DHCP servers configured
Interface	Interface name
Uplink/Downlink	Whether the interface is a server-facing port (uplink) or a client-facing port (downlink).

# show ipv6 dhcp relay address

Use this command to display DHCP IPv6 relay addresses.

## Command Syntax

```
show ipv6 dhcp relay address
```

## Parameters

None

## Command Mode

Executive mode

## Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

## Examples

```
#show ipv6 dhcp relay address
VRF Name: vrf1
  DHCPv6 Servers configured: 2001::1
VRF Name: default
  DHCPv6 Servers configured: 3001::1
```

[Table 13-29](#) explains the output fields.

Table 13-29: show ipv6 dhcp relay address fields

Entry	Description
VRF Name	Name of the VRF.
DHCPv6 Servers configured	Addresses of DHCP servers configured

---

## show running-config dhcp

Use this command to display DHCP settings in the running configuration.

### Command Syntax

```
show running-config dhcp
```

### Parameters

None

### Command Mode

Executive mode

### Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

### Examples

```
#show running-config dhcp
ip vrf vrfl
  ip dhcp relay information option remote-id hostname
  ip dhcp relay address 1.1.1.2
ip dhcp relay information option remote-id hostname
ip dhcp relay information source-ip 5.4.3.2
ip dhcp relay address 1.1.1.1
```





## CHAPTER 14 IP Source Guard Commands

---

This chapter describes the commands for IP Source Guard (IPSG):

- [hardware-profile filter ipsg](#)
- [hardware-profile filter ipsg-ipv6](#)
- [ip verify source dhcp-snooping-vlan](#)

---

## hardware-profile filter ipsg

Use this command to enable or disable the ingress IPSG TCAM group for IPv4.

### Command Syntax

```
hardware-profile filter ipsg (disable | enable)
```

### Parameters

enable	Enable the ingress IPSG TCAM group
disable	Disable the ingress IPSG TCAM group

### Default

N/A

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 5.0.

### Examples

```
#configure terminal
(config)# hardware-profile filter ipsg enable
```

---

## hardware-profile filter ipsg-ipv6

Use this command to enable or disable the ingress IPSG TCAM group for IPv6.

### Command Syntax

```
hardware-profile filter ipsg-ipv6 (disable | enable)
```

### Parameters

enable	Enable the ingress IPSG TCAM group
disable	Disable the ingress IPSG TCAM group

### Default

N/A

### Command Mode

Config mode

### Applicability

This command was introduced in OcNOS version 5.0.

### Examples

```
#configure terminal
(config)# hardware-profile filter ipsg-ipv6 disable
```

---

## ip verify source dhcp-snooping-vlan

Use this command to enable the IPSG feature at the interface level.

Use the no form of this command to disable the IPSG on an interface.

### Command Syntax

```
ip verify source dhcp-snooping-vlan
no ip verify source dhcp-snooping-vlan
```

### Parameters

None

### Default

N/A

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS version 5.0.

### Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ip verify source dhcp-snooping-vlan

(config-if)#no ip verify source dhcp-snooping-vlan
```

## CHAPTER 14 Domain Name System

---

This chapter describes Domain Name System (DNS) commands. DNS translates easily-to-remember domain names into numeric IP addresses needed to locate computer services and devices. By providing a worldwide, distributed keyword-based redirection service, DNS is an essential component of the Internet.

The DNS database is hierarchical. When a client such as a Web browser gives a request that specifies a host name, the DNS resolver on the client first contacts a DNS server to determine the server's IP address. If the DNS server does not contain the needed mapping, it forwards the request to a different DNS server at the next higher level in the hierarchy. After potentially several forwarding and delegation messages are sent within the DNS hierarchy, the IP address for the given host eventually arrives at the resolver, that in turn completes the request over Internet Protocol (IP).

Note: The commands below are supported only on the “management” VRF.

The chapter contains these commands:

- `debug dns client`
- `ip domain-list`
- `ip domain-lookup`
- `ip domain-name`
- `ip host`
- `ip name-server`
- `show hosts`
- `show running-config dns`

---

## debug dns client

Use this command to display DNS debugging messages.

Use the `no` form of this command to stop displaying DNS debugging messages.

### Command Syntax

```
debug dns client
no debug dns client
```

### Parameters

None

### Default

By default, disabled.

### Command Mode

Exec mode, Privileged Exec mode, and Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#debug dns client
```

---

## ip domain-list

Use this command to define a list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.

The `ip domain-list` command is similar to the [ip domain-name](#) command, except that with the `ip domain-list` command you can define a list of domains, each to be tried in turn.

If there is no domain list, the default domain name specified with the `ip domain-name` command is used. If there is a domain list, the default domain name is not used.

Use the `no` form of this command to remove a domain.

### Command Syntax

```
ip domain-list (vrf management|) DOMAIN-NAME
no ip domain-list (vrf management|) DOMAIN-NAME
```

### Parameters

management	Virtual Routing and Forwarding name
DOMAIN-NAME	Domain string (e.g. company.com)(Max Size 64)

### Default

No default is specified.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip domain-list mySite.com
```

---

## ip domain-lookup

Use this command to enable DNS host name-to-address translation.

Use the `no` form of this command to disable DNS.

### Command Syntax

```
ip domain-lookup (vrf management|)
no ip domain-lookup (vrf management|)
```

### Parameters

<code>management</code>	Virtual Routing and Forwarding name
-------------------------	-------------------------------------

### Default

No default is specified.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip domain-lookup
```



---

## ip domain-name

Use this command to set the default domain name used to complete unqualified host names (names without a dotted-decimal domain name).

The [ip domain-list](#) command is similar to the `ip domain-name` command, except that with the `ip domain-list` command you can define a list of domains, each to be tried in turn.

If a domain list has been created with `ip domain-list`, the default domain name is not used. If there is no domain list, the default domain name is used.

Use the `no` form of this command to disable DNS.

### Command Syntax

```
ip domain-name (vrf management|) DOMAIN-NAME
no ip domain-name (vrf management|) DOMAIN-NAME
```

### Parameters

management	Virtual Routing and Forwarding name
DOMAIN-NAME	Domain string (e.g. company.com)(Max Size 64)

### Default

No default is specified.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip domain-name company.com
```

---

## ip host

Use this command to define static hostname-to-address mappings in DNS. You can specify one or two mappings in a command.

Use the `no` form of this command remove a hostname-to-address mapping.

### Command Syntax

```
ip host (vrf management|) WORD A.B.C.D
ip host (vrf management|) WORD A.B.C.D A.B.C.D
ip host (vrf management|) WORD (X:X::X:X | A.B.C.D)
ip host (vrf management|) WORD (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)
no ip host (vrf management|) WORD A.B.C.D
no ip host (vrf management|) WORD A.B.C.D A.B.C.D
no ip host (vrf management|) WORD (X:X::X:X | A.B.C.D)
no ip host (vrf management|) WORD (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)
```

### Parameters

management	Virtual Routing and Forwarding name
WORD	Host name, such as company.com
X:X::X:X	IPv6 address of the host
A.B.C.D	IPv4 address of the host

### Default

No default is specified.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip host company.com 192.0.2.1
```

---

## ip name-server

Use this command to add a DNS server address that is used to translate hostnames to IP addresses.

Use the no form of this command to remove a DNS server address.

### Command Syntax

```
ip name-server (vrf management|) (X:X::X:X | A.B.C.D)
no ip name-server (vrf management|) (X:X::X:X | A.B.C.D)
```

### Parameters

management	Virtual Routing and Forwarding name
A.B.C.D	IPv4 address of the host
X:X::X:X	IPv6 address of the host

### Default

No default is specified.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip name-server 123.70.0.23
```

## show hosts

Use this command to display the DNS name servers and domain names.

## Command Syntax

```
show hosts (vrf management|all)
```

## Parameters

vrf	management or all VRFs
-----	------------------------

## Command Mode

## Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

### Example

The following is a sample output of this command displaying two name servers: 10.10.0.2 and 10.10.0.88.

[illegible]

Table 14-30 explains the output fields.

### Table 14-30: show hosts fields

Entry	Description
VRF: management	DNS configuration of specified VRF.
DNS lookup is enabled	DNS feature enabled or disabled.
Default domain	Default domain name used to complete unqualified host names (names without a dotted decimal domain name).
Additional Domain	A list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.
Name Servers	DNS server addresses that are used to translate hostnames to IP addresses.

Table 14-30: show hosts fields

Entry	Description
Host	Static hostname-to-address mappings in DNS.
Test	Static hostname-to-address mappings in DNS.
* - Values assigned by DHCP Client.	Name-server indicates it has been learned dynamically.

---

## show running-config dns

Use this command to show the DNS settings of the running configuration.

### Command Syntax

```
show running-config dns (vrf management|)
```

### Parameters

vrf	management
-----	------------

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show running-config dns
ip domain-lookup vrf management
ip domain-name vrf management .com
ip domain-list vrf management .in
ip domain-list vrf management .ac
ip name-server vrf management 10.12.3.23
ip host vrf management test 10.12.12.67 10::23
```

---

## CHAPTER 15 Interface Commands

---

This chapter is a reference for each of the interface commands.

- [admin-group](#)
- [bandwidth](#)
- [bandwidth-measurement static uni-available-bandwidth](#)
- [bandwidth-measurement static uni-residual-bandwidth](#)
- [bandwidth-measurement static uni-utilized-bandwidth](#)
- [clear hardware-discard-counters](#)
- [clear interface counters](#)
- [clear interface cpu counters](#)
- [clear interface fec](#)
- [clear ip prefix-list](#)
- [clear ipv6 neighbors](#)
- [clear ipv6 prefix-list](#)
- [debounce-time](#)
- [delay-measurement dynamic twamp](#)
- [delay-measurement a-bit-min-max-delay-threshold](#)
- [delay-measurement static](#)
- [delay-measurement a-bit-delay-threshold](#)
- [description](#)
- [duplex](#)
- [fec](#)
- [flowcontrol](#)
- [hardware-profile portmode](#)
- [if-arbiter](#)
- [interface](#)
- [ip address A.B.C.D/M](#)
- [ip address dhcp](#)
- [ip forwarding](#)
- [ip prefix-list](#)
- [ip proxy-arp](#)
- [ip remote-address](#)
- [ip unnumbered](#)
- [ip vrf forwarding](#)
- [ipv6 address](#)
- [ipv6 forwarding](#)
- [ipv6 prefix-list](#)

- `ipv6 unnumbered`
- `link-debounce-time`
- `load interval`
- `loopback`
- `loss-measurement uni-link-loss`
- `monitor speed`
- `monitor queue-drops`
- `monitor speed threshold`
- `mtu`
- `multicast`
- `show flowcontrol`
- `show hardware-discard-counters`
- `show interface`
- `show interface capabilities`
- `show interface counters`
- `show interface counters drop-stats`
- `show interface counters error-stats`
- `show interface counters (indiscard-stats|outdiscard-stats)`
- `show interface counters protocol`
- `show interface counters queue-drop-stats`
- `show interface counters queue-stats`
- `show interface counters rate`
- `show interface counters speed`
- `show interface counters summary`
- `show interface fec`
- `show ip forwarding`
- `show ip interface`
- `show ip prefix-list`
- `show ip route`
- `show ip vrf`
- `show ipv6 forwarding`
- `show ipv6 interface brief`
- `show ipv6 route`
- `show ipv6 prefix-list`
- `show hosts`
- `show running-config interface`
- `show running-config interface ip`
- `show running-config interface ipv6`
- `show running-config ip`



- [show running-config ipv6](#)
- [show running-config prefix-list](#)
- [shutdown](#)
- [speed](#)
- [switchport](#)
- [switchport allowed ethertype](#)
- [switchport protected](#)
- [transceiver](#)

---

## admin-group

Use this command to create an administrative group to be used for links. Each link can be a member of one or more, or no administrative groups.

When used in the interface mode, this command adds a link between an interface and a group. The name is the name of the group previously configured. There can be multiple groups per interface. The group is created in configure mode, then interfaces are added to the group in interface mode.

Use the `no` parameter with this command to disable this command.

### Command Syntax

```
admin-group NAME
no admin-group NAME
```

### Parameters

NAME	Name of the admin group to add.
------	---------------------------------

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

In the following example, the `eth3` interface is added to the group `myGroup`:

```
#configure terminal
(config)#interface eth3
(config-if)#admin-group myGroup
```

---

## bandwidth

Use this command to specify a discrete, maximum bandwidth value for the interface.

Use the `no` parameter resets the interface's bandwidth to the default value.

### Command Syntax

```
bandwidth BANDWIDTH
no bandwidth
```

### Parameter

BANDWIDTH	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

### Default

Default bandwidth will be default speed of the interface. For LAG, default bandwidth will be collective bandwidth of its member ports. For VLAN interface, default bandwidth is 1 gigabits/sec.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#interface xe4
(config-if)#bandwidth 100m
```

---

## bandwidth-measurement static uni-available-bandwidth

Use this command to advertise the available bandwidth between two directly connected OSPF/ISIS neighbors.

Use the `no` parameter with this command to unset available bandwidth on the current interface.

### Command Syntax

```
bandwidth-measurement static uni-available-bandwidth BANDWIDTH
no bandwidth-measurement static uni-available-bandwidth
```

### Parameter

BANDWIDTH	<0-999>k for 0 to 999 kilo bits/s
	<0-999>m for 0 to 999 mega bits/s
	<0-100>g for 0 to 100 giga bits/s

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
(config)#int eth2
(config-if)#bandwidth-measurement static uni-available-bandwidth 10k
(config-if)#commit

(config)#int eth2
(config-if)#no bandwidth-measurement static uni-available-bandwidth
(config-if)#commit
```

---

## bandwidth-measurement static uni-residual-bandwidth

Use this command to advertise the residual bandwidth between two directly connected OSPF/ISIS neighbors.

Use the `no` parameter with this command to unset residual bandwidth on the current interface.

### Command Syntax

```
bandwidth-measurement static uni-residual-bandwidth BANDWIDTH
no bandwidth-measurement static uni-residual-bandwidth
```

### Parameter

BANDWIDTH	<0-999>k for 0 to 999 kilo bits/s
	<0-999>m for 0 to 999 mega bits/s
	<0-100>g for 0 to 100 giga bits/s

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
(config)#interface ethernet 2
(config-if)#bandwidth-measurement static uni-residual-bandwidth 10g
(config-if)#commit

(config)#interface ethernet 2
(config-if)#no bandwidth-measurement static uni-residual-bandwidth
(config-if)#commit
```

---

## bandwidth-measurement static uni-utilized-bandwidth

Use this command to advertise the utilized bandwidth between two directly connected OSPF/ISIS neighbors.

Use the `no` parameter with this command to unset utilized bandwidth on the current interface.

### Command Syntax

```
bandwidth-measurement static uni-utilized-bandwidth BANDWIDTH
no bandwidth-measurement static uni-utilized-bandwidth
```

### Parameter

BANDWIDTH	<0-999>k for 0 to 999 kilo bits/s
	<0-999>m for 0 to 999 mega bits/s
	<0-100>g for 0 to 100 giga bits/s

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
(config)#int eth2
(config-if)#bandwidth-measurement static uni-utilized-bandwidth 10m
(config-if)#commit

(config)#int eth2
(config-if)#no bandwidth-measurement static uni-utilized-bandwidth
(config-if)#commit
```

---

## clear hardware-discard-counters

Use this command to clear device level discard counters.

### Command Syntax

```
clear hardware-discard-counters
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

The command is introduced before OcNOS version 1.3.

### Examples

```
#clear hardware-discard-counters
```

---

## clear interface counters

Use this command to clear the statistics on a specified interface or on all interfaces.

Note: This command is not supported on loopback interfaces or the out-of-band management (OOB) management interface.

### Command Syntax

```
clear interface (IFNAME|) counters
```

### Parameter

IFNAME	Interface name.
--------	-----------------

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear interface xe0 counters
```



---

## clear interface cpu counters

Use this command to clear the CPU queue counters.

### Command Syntax

```
clear interface cpu counters
```

### Parameter

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear interface cpu counters
```

---

## clear interface fec

Use this command to clear FEC (forward error correction) statistics on a specified interface or on all interfaces.

Note: This command is not supported on loop-back interfaces or the out-of-band (OOB) management interface.

### Command Syntax

```
clear interface (IFNAME|) fec
```

### Parameters

IFNAME	Physical Interface name.
--------	--------------------------

### Default

None

### Command Mode

Exec mode and Privileged exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear interface ce1/1 fec
```

---

## clear ip prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv4 interface.

### Command Syntax

```
clear ip prefix-list  
clear ip prefix-list WORD  
clear ip prefix-list WORD A.B.C.D/M
```

### Parameters

WORD	Name of the prefix-list.
A.B.C.D/M	IP prefix and length.

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear ip prefix-list List1
```

---

## clear ipv6 neighbors

Use this command to clear all dynamic IPv6 neighbor entries.

### Command Syntax

```
clear ipv6 neighbors
```

### Parameters

None

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear ipv6 neighbors
```

---

## clear ipv6 prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv6 interface.

### Command Syntax

```
clear ipv6 prefix-list  
clear ipv6 prefix-list WORD  
clear ipv6 prefix-list WORD X:X::X:X/M
```

### Parameters

WORD	Name of the prefix-list.
X:X::X:X/M	IP prefix and length.

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear ipv6 prefix-list List1
```

---

## debounce-time

Use this command to set the debounce time for an interface.

The debounce timer avoids frequent updates (churn) to higher layer protocol during interface flapping. If the status of a link changes quickly from up to down and then back to up, the port debounce timer suppresses the link status notification. If the link transitions from up to down, but does not come back up, the port debounce timer delays the link status notification.

Note: Keep the following in mind when using the debounce timer:

- Debounce is not applicable for admin down operations.
- Debounce timer is supported only for physical L2 and L3 interfaces.
- The debounce flap-count refers to the number of flaps OcNOS receives while the debounce timer is running:
  - The flap-count is only updated if the timer is still running and OcNOS receives a link status event for the interface.
  - The flap-count is reset at the subsequent start of the debounce timer.
- Protocol-specific timers such as BFD which depend on the link status should be configured to a minimum of 1.5 times the value of the debounce timer. Otherwise it could affect the protocol states if the debounce timer is still running.

Use the `no` form of this command to turn-off the debounce timer on an interface.

### Command Syntax

```
debounce-time <250-5000>
no debounce-time
```

### Parameters

`<250-5000>`      Timer value in milliseconds.

### Default

By default, disabled.

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS version 1.3.8.

### Example

```
#configure terminal
(config)#interface eth1
(config-if)#debounce-time 4000
```

## delay-measurement dynamic twamp

This command will start the measurement on the interface by using the "interfaces" profile.

The user should be aware that the IP used as a reflector IP must be a directly connected IP.

In case hostname needs to be used, the user must be sure about the hostnames configured in the network.

In case the user configures the delay-measurement with a certain hostname and then the hostname entry in the DNS changes, the delay-measurement must be unconfigured and configured again for the new configuration to take effect (a clear command would not be sufficient in this situation)

Use the `no` form of this command to stop the delay measurement.

### Command Syntax

```
delay-measurement dynamic twamp reflector-ip (HOSTNAME | X:X::X:X | A.B.C.D)
(reflector-port <1025-65535>|) (sender-ip (HOSTNAME | X:X::X:X | A.B.C.D)|) (dscp
WORD|)

no delay-measurement dynamic twamp reflector-ip (HOSTNAME | X:X::X:X | A.B.C.D)
```

### Parameters

twamp	This parameter specifies the protocol to be used to do the measurement. It is the only protocol available in this implementation. The subsequent parameters in this command are specific to the protocol chosen (TWAMP).
reflector-ip	Specify the reflector ip/hostname used to send the TWAMP packets to
HOSTNAME	The hostname of the reflector
X:X::X:X	The ip address of the reflector
A.B.C.D	The ip address of the reflector
reflector-ports	specify the UDP port of the TWAMP reflector
<1025-65535>	The reflector port value
sender-ip	Specify the IP used to send the TWAMP packets from (must be an IP configured on the current interface)
HOSTNAME	The hostname of the reflector
X:X::X:X	The ip address of the reflector
A.B.C.D	The ip address of the reflector
dscp	Specify the dscp value used during this measurement
WORD	The dscp value

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 5.1.

### Example

```
OcNOS(config)#
OcNOS(config)#interface xe7
```

```
OcNOS(config-if)#delay-measurement dynamic twamp reflector-ip 23.1.1.2 sender-  
ip 23.1.1.1 dscp 24  
OcNOS(config-if)#commit
```

```
OcNOS(config-if)#no delay-measurement dynamic twamp reflector-ip 23.1.1.2  
OcNOS(config-if)#commit
```



---

## delay-measurement a-bit-min-max-delay-threshold

Use this command to advertise the minimum and maximum delay values between two directly connected IS-IS/OSPF neighbors.

The A bit is set when one or more measured values exceed a configured maximum threshold. The A bit is cleared when the measured value falls below its configured reuse threshold.

Use the `no` parameter with this command to unset a-bit-min-max-delay-threshold on the current interface.

### Command Syntax

```
delay-measurement a-bit-min-max-delay-threshold min <1-16777215> <1-16777215> max  
  <1-16777215> <1-16777215>)  
no delay-measurement a-bit-min-max-delay-threshold
```

### Parameter

min	Reuse threshold
<1-16777215>	Reuse threshold value of Min-Delay in microseconds
<1-16777215>	Reuse threshold value of Max-Delay in microseconds
a-bit-threshold	Threshold values to set/clear A-bit
max	Maximum threshold
<1-16777215>	Maximum threshold value of Min-Delay in microseconds
<1-16777215>	Maximum threshold value of Max-Delay in microseconds

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#configure terminal  
(config)#interface eth1  
  (config-if)#delay-measurement a-bit-min-max-delay-threshold min 11 22 max 33  
44  
(config-if)#no delay-measurement a-bit-min-max-delay-threshold
```

---

## delay-measurement static

Use this command to advertise static the minimum and maximum delay values or average link delay variation or average link delay values between two directly connected IS-IS/OSPF neighbors.

Use the `no` parameter with this command to unset min-max-uni-link-delay, uni-delay-variation and uni-link-delay static values on the current interface.

### Command Syntax

```
delay-measurement static (min-max-uni-link-delay <1-16777215> <1-16777215> | uni-  
  delay-variation <0-16777215> | uni-link-delay <1-16777215>)  
  
no delay-measurement static (min-max-uni-link-delay | uni-delay-variation | uni-  
  link-delay)
```

### Parameter

<code>min-max-uni-link-delay</code>	Min/Max Unidirectional Link Delay
<1-16777215>	Minimum Unidirectional Link Delay in microseconds
<1-16777215>	Maximum Unidirectional Link Delay in microseconds
<code>uni-delay-variation</code>	Unidirectional Delay Variation
<0-16777215>	Value in microseconds
<code>uni-link-delay</code>	Unidirectional Link Delay
<1-16777215>	Value in microseconds

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#configure terminal  
(config)#interface eth1  
(config-if)#delay-measurement uni-delay-variation static 12  
(config-if)#no delay-measurement uni-delay-variation static  
#configure terminal  
(config)#interface eth1  
(config-if)#delay-measurement static uni-link-delay 12  
(config-if)#no delay-measurement static uni-link-delay  
(config-if)#delay-measurement static min-max-uni-link-delay 1 3  
(config-if)#no delay-measurement static min-max-uni-link-delay
```

---

## delay-measurement a-bit-delay-threshold

Use this command to advertise average link delay between two directly connected IS-IS/OSPF neighbors.

a-bit-threshold represents the Anomalous (A) bit. The A bit is set when the static value exceeds its configured maximum threshold. The A bit is cleared when the static value falls below its configured reuse threshold.

Use the `no` parameter with this command to unset uni-link-delay on the current interface.

### Command Syntax

```
delay-measurement a-bit-delay-threshold min <1-16777215> max <1-16777215>))  
no delay-measurement a-bit-delay-threshold
```

### Parameter

min	Reuse threshold
<1-16777215>	Reuse threshold value in microseconds
max	Maximum threshold
<1-16777215>	Maximum threshold value in microseconds

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#configure terminal  
(config)#interface eth1  
(config-if)#delay-measurement a-bit-delay-threshold min 11 max 22  
(config-if)#no delay-measurement a-bit-delay-threshold
```

---

## description

Use this command to assign an description to an interface.

Use the `no` parameter to remove an interface description.

### Command Syntax

```
description LINE
no description
```

### Parameter

<code>LINE</code>	Interface description. Avoid the special characters “?”, “,”, “>”, “[”, and “=” in the description. The “[” is allowed only for interface <code>description CLI</code> .
-------------------	--

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

The following example provides information about the connecting router for interface `eth1`.

```
Router#configure terminal
Router(config)#interface eth1
Router(config-if)#description Connected to Zenith's fas2/0
```

---

## duplex

Use this command to set the duplex mode for each interface.

Use the `no` parameter to remove the duplex mode.

Note: Interface duplex setting is not supported on Management interface `eth0`.

### Command Syntax

```
duplex {half|full}
no duplex
```

### Parameter

<code>half</code>	Half-duplex mode.
<code>full</code>	Full-duplex mode.

### Default

By default, duplex mode is full duplex.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#interface eth3
(config-if)#duplex full

(config-if)#no duplex
```

## fec

Use this command to force/auto configure forward error correction (FEC) on a physical port.

Use the `no` parameter to enable automatic FEC configuration provisioning based on medium.

### Command Syntax

```
fec (on (c174|c191)|off|auto)
no fec
```

### Parameter

<code>on</code>	Enable FEC.
<code>on c174</code>	Enable Base-R FEC if H/W supports it
<code>on c191</code>	Enable RS-528 FEC if H/W supports it
<code>off</code>	Disable FEC.
<code>auto</code>	Automatically apply FEC for the below transceiver Ethernet compliance codes. Transceiver compliance codes can be fetched via the "show interface controller" command. Also, "fec auto" behavior is the same as no fec. 100G AOC (Active Optical Cable) or 25GAUI C2M AOC 100G ACC (Active Copper Cable) or 25GAUI C2M ACC 100G ACC or 25GAUI C2M ACC 100G AOC or 25GAUI C2M AOC 100GBASE-SR4 or 25GBASE-SR 100G AOC (Active Optical Cable) or 25GAUI C2M AOC

### Default

By default, FEC mode is set to auto.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 4.1. The CLI is updated for options `c174|c191` in OcNOS version 6.3.1

### Examples

```
(config)#interface eth3
(config-if)#fec on
(config-if)#fec off
(config-if)#fec auto
(config-if)#fec on c174
(config-if)#fec on c191
```

---

## flowcontrol

Use this command to enable or disable flow control.

Flow control enables connected Ethernet ports to control traffic rates during periods of congestion by allowing congested nodes to pause link operations at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When a local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the period of congestion.

Use the `no` parameter with this command to disable flow control.

### Command Syntax

```
flowcontrol both
flowcontrol send on
flowcontrol send off
flowcontrol receive on
flowcontrol receive off
no flowcontrol
```

### Parameters

<code>both</code>	Specify flow control mode for sending or receiving.
<code>send</code>	Specify flow control mode for sending.
<code>receive</code>	Specify the flow control mode for receiving.
<code>off</code>	Turn off flow control.
<code>on</code>	Turn on flow control.

### Default

The flow control is enabled globally and auto-negotiation is on, flow control is enabled and advertised on 10/100/1000M ports. If auto-negotiation is off or if the port speed was configured manually, flow control is neither negotiated with nor advertised to the peer.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#interface eth1
(config-if)#flowcontrol receive off

#configure terminal
(config)#interface eth1
(config-if)#flowcontrol receive on
```

```
(config)#interface eth1  
(config-if)#no flowcontrol
```



---

## hardware-profile portmode

Use this command to set the global port mode.

Note: This command is deprecated in ocnos-6.3.0.

### Command Syntax

```
hardware-profile portmode (4X10g|40g)
```

### Parameter

4X10g	Split all the 40G flex ports on the system
40g	Disable splitting on all flex ports and make all ports 40G

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#hardware-profile portmode 40g
```

---

## if-arbiter

Use this command to discover new interfaces recently added to the kernel and add them to the OcnOS database.

This command starts the arbiter to check interface information periodically. OcnOS dynamically finds any new interfaces added to the kernel. If an interface is loaded dynamically into the kernel when OcnOS is already running, this command polls and updates the kernel information periodically.

Use the `no` parameter with this command to revert to default.

### Command syntax

```
if-arbiter (interval <1-65535>|)
no if-arbiter
```

### Parameter

<code>interval</code>	Interval (in seconds) after which NSM sends a query to the kernel.
-----------------------	--

### Default

By default, `if-arbiter` is disabled. When interface-related operations are performed outside of OcnOS (such as when using the `ifconfig` command), enable `if-arbiter` for a transient time to complete synchronization. When synchronization is complete, disable it by giving the `noif-arbiter` command.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcnOS version 1.3.

### Example

```
#configure terminal
(config)#if-arbiter interval 5
```

---

## interface

Use this command to select an interface to configure, and to enter the `Interface` command mode.

Use the `no` parameter with this command to remove this configuration.

### Command Syntax

```
interface IFNAME
no interface IFNAME
```

### Parameter

IFNAME	Name of the interface.
--------	------------------------

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

This example shows the use of this command to enter the `Interface` mode (note the change in the prompt).

```
#configure terminal
(config)#interface eth3
(config-if)#
```

---

## ip address A.B.C.D/M

Use this command to specify that an IP address and prefix length will be used by this interface. If the `secondary` parameter is not specified, this command overwrites the primary IP address. If the `secondary` parameter is specified, this command adds a new IP address to the interface. The secondary address cannot be configured in the absence of a primary IP address. The primary address cannot be removed when a secondary address is present.

Use the `no` parameter with this command to remove the IP address from an interface.

### Command Syntax

```
ip address A.B.C.D/M label LINE
ip address A.B.C.D/M (secondary|)
ip address A.B.C.D/M secondary label LINE
no ip address A.B.C.D/M label LINE
no ip address A.B.C.D/M secondary label LINE
no ip address (A.B.C.D/M (secondary|))
```

### Parameters

<code>LINE</code>	Label of this address.
<code>secondary</code>	Make the IP address secondary.

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
(config)#interface eth3
(config-if)#ip address 10.10.10.50/24
(config-if)#ip address 10.10.11.50/24 secondary
```

---

## ip address dhcp

Use this command to specify that a DHCP client will be used to obtain an IP address for an interface.

Use the `no` parameter with this command to remove the IP address from an interface.

### Command Syntax

```
ip address dhcp
no ip address dhcp
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
(config)#interface eth3
(config-if)#ip address 10.10.10.50/24
(config-if)#ip address 10.10.11.50/24 secondary
(config-if)#ip address dhcp
```

---

## ip forwarding

Use this command to turn on IP forwarding.

Use the `no` parameter with this command to turn off IP forwarding.

### Command Syntax

```
ip forwarding
ip forwarding vrf NAME
no ip forwarding
no ip forwarding vrf NAME
```

### Parameters

NAME	Virtual Routing and Forwarding name
------	-------------------------------------

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ip forwarding
```

## ip prefix-list

Use this command to create an entry for a prefix list.

A router starts to match prefixes from the top of the prefix list and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

Use the parameters `ge` and `le` specify the range of the prefix length to be matched. When setting these parameters, set `le` to be less than 32 and `ge` to be less than `le` value.

Use the `no` parameter with this command to delete the prefix-list entry.

### Command Syntax

```
ip prefix-list WORD
(deny|permit) (A.B.C.D/M|any)
(deny|permit) A.B.C.D/M eq <0-32>
(deny|permit) A.B.C.D/M ge <0-32>
(deny|permit) A.B.C.D/M ge <0-32> le <0-32>
(deny|permit) A.B.C.D/M le <0-32>
(deny|permit) A.B.C.D/M le <0-32> ge <0-32>
seq <1-4294967295> (deny|permit) (A.B.C.D/M|any)
seq <1-4294967295> (deny|permit) A.B.C.D/M eq <0-32>
seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32>
seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32> le <0-32>
seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32>
seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32> ge <0-32>
description LINE
no seq <1-4294967295> (deny|permit) (A.B.C.D/M|any)
no description LINE
no description
no ip prefix-list WORD
ip prefix-list sequence-number
no ip prefix-list sequence-number
```

### Parameters

WORD	Name of the prefix list.
deny	Reject packets.
permit	Accept packets.
A.B.C.D/M	IP address mask and length of the prefix list mask.
eq	Exact prefix length match
le	Maximum prefix length match
ge	Minimum prefix length match

<0-32>	Prefix length to match
<1-4294967295>	Sequence number of the prefix list.
any	Take all packets of any length. This parameter is the same as using 0.0.0.0/0 le 32 for A.B.C.D/M.
sequence-number	<p>To suppress sequence number generation, give the <code>no ip prefix-list sequence-number</code> command. If you disable the generating sequence numbers, you must specify the sequence number for each entry using the sequence number parameter in the <code>ip prefix-list</code> command.</p> <p>To enable sequence number generation, give the <code>ip prefix-list sequence-number</code> command.</p>
LINE	Up to 80 characters describing this prefix-list.

### Default

No default value is specified

### Command Mode

Configure mode

IP prefix-list mode

### Applicability

This command was introduced before OcNOS Version SP 4.0.

### Examples

In this configuration, the `ip prefix-list` command matches all, but denies the IP address range, 76.2.2.0.

```
#conf t
(config)#router bgp 100
(config-router)#network 172.1.1.0
(config-router)#network 172.1.2.0
(config-router)#
(config-router)#neighbor 10.6.5.3 remote-as 300
(config-router)#neighbor 10.6.5.3 prefix-list mylist out
(config-router)#exit
(config)#ip prefix-list mylist
(config-ip-prefix-list)#seq 5 deny 76.2.2.0/24
(config-ip-prefix-list)#seq 10 permit 0.0.0.0/0
```



---

## ip proxy-arp

Use this command to enable the proxy ARP feature on an interface.

Use the `no` parameter to disable the proxy ARP feature on an interface.

### Command Syntax

```
ip proxy-arp
no ip proxy-arp
```

### Parameters

None

### Default

By default, the `ip proxy-arp` is disabled

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#interface eth3
(config-if)#ip proxy-arp
```

---

## ip remote-address

Use this command to set the remote address (far end) on a point-to-point non multi-access link. This command can be used only on unnumbered interfaces. When a new remote-address is configured, the old address gets overwritten.

Use the `no` parameter to disable this function.

### Command Syntax

```
ip remote-address A.B.C.D/M
no ip remote-address
```

### Parameter

A.B.C.D/M	IP address and prefix length of the link remote address.
-----------	--

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
(config)#interface ppp0
(config-if)#ip unnumbered eth1
(config-if)#ip remote-address 1.1.1.1/32
```

---

## ip unnumbered

Use this command to enable IP processing without an explicit address on a point-to-point non multi-access link. Moreover, this command lets an interface borrow the IP address of a specified interface to enable IP processing on a point-to-point interface without assigning it an explicit IP address. In this way, the IP unnumbered interface can borrow the IP address of another interface already configured on the router to conserve network and address space.

Use the `no` parameter with this command to remove this feature on an interface.

### Command Syntax

```
ip unnumbered IFNAME
no ip unnumbered
```

### Parameter

IFNAME	Interface name.
--------	-----------------

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

The following example creates a tunnel on `eth1`.

```
(config)#interface lo
(config-if)#ip address 127.0.0.1/8
(config-if)#ip address 33.33.33.33/32 secondary
(config-if)#exit
(config)#interface eth1
(config-if)#ip address 10.10.10.145/24
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode vxlan
(config-if)#ip unnumbered eth1
(config-if)#exit
(config)#router ospf
(config-router)#network 10.10.10.0/24 area 0
```

---

## ip vrf forwarding

This command associates an interface with a VRF.

Use the `no` parameter with this command to unbind an interface.

**Note:** When you give this command in interface configuration or subinterface configuration mode of the parent VR, the IP address and other attributes of the interface are deleted from the interface. After giving this command, the IP attributes must then be configured in the context of the VRF.

**Note:** The Out Of Band (OOB) management port is part of the “management” VRF. Also, this port cannot be moved out of “management” VRF.

### Command Syntax

```
ip vrf forwarding WORD
no ip vrf forwarding WORD
```

### Parameter

WORD	Name of the VRF.
------	------------------

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#ip vrf myVRF
(config-vrf)#exit
(config)#interface eth1
(config-if)#ip vrf forwarding myVRF
```

---

## ipv6 address

Use this command to set the IPv6 address of an interface.

Use the `no` form of this command to disable this function.

Note: This command is also used to configure an IPv6 link-local address for an interface.

### Command Syntax

```
ipv6 address X:X::X:X/M
ipv6 address X:X::X:X/M anycast
no ipv6 address X:X::X:X/M
```

### Parameters

<code>X:X::X:X/M</code>	IP destination prefix and a mask length.
<code>anycast</code>	Make an anycast address which is assigned to a set of interfaces that belong to different devices. A packet sent to an anycast address is delivered to the closest interface (as defined by the routing protocols in use) identified by the anycast address

### 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 eth3
(config-if)#ipv6 address 3ffe:506::1/64

#configure terminal
(config)#interface eth4
(config-if)#ipv6 address fe80::ab8/64
```

---

## ipv6 forwarding

Use this command to turn on IPv6 forwarding.

Use the `no` parameter with this command to turn off IPv6 forwarding.

### Command Syntax

```
ipv6 forwarding
ipv6 forwarding vrf NAME
no ipv6 forwarding
no ipv6 forwarding vrf NAME
```

### Parameters

NAME	Virtual Routing or Forwarding name
------	------------------------------------

### Default

No default value is specified

### Command Mode

Command mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#ipv6 forwarding
```

## ipv6 prefix-list

Use this command to create an entry for an ipv6 prefix-list.

Router starts to match prefixes from the top of the prefix list, and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

The parameters `ge` and `le` specify the range of the prefix length to be matched.

Use the `no` parameter with this command to delete the prefix-list entry.

### Command Syntax

```

ipv6 prefix-list WORD
(deny|permit) (X:X::X:X/M|any)
(deny|permit) X:X::X:X/M ge <0-128>
(deny|permit) X:X::X:X/M ge <0-128> le <0-128>
(deny|permit) X:X::X:X/M le <0-128>
(deny|permit) X:X::X:X/M le <0-128> ge <0-128>
seq <1-4294967295> (deny|permit) (X:X::X:X/M|any)
seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128>
seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128> le <0-128>
seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128>
seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128> ge <0-128>
description LINE
no seq <1-4294967295> (deny|permit) (X:X::X:X/M|any)
no description
no ipv6 prefix-list WORD
ipv6 prefix-list sequence-number
no ipv6 prefix-list sequence-number

```

### Parameters

WORD	Name of the prefix list.
deny	Reject packets.
permit	Accept packets.
X:X::X:X/M	IP address mask and length of the prefix list mask.
any	Take all packets of any length. This is the same as specifying ::/0 for X:X::X:X/M.
eg	Exact prefix length match
le	Maximum prefix length match
ge	Minimum prefix length match
<0-128>	Prefix length to match
<1-4294967295>	Sequence number of the prefix list.
sequence-number	

To suppress sequence number generation, give the `no ipv6 prefix-list sequence-number` command. If you disable the generating sequence numbers, you must specify the sequence number for each entry using the sequence number parameter in the `ipv6 prefix-list` command.

To enable sequence number generation, give the `ipv6 prefix-list sequence-number` command.

LINE

Up to 80 characters describing this prefix-list.

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ipv6 prefix-list mylist
(config-ipv6-prefix-list)#seq 12345 deny 3ffe:345::/16 le 22 ge 14
```



---

## ipv6 unnumbered

Use this command to enable IPv6 processing without an explicit address, on a point-to-point non multi-access link.

This command lets an interface borrow the IPv6 address of a specified interface to enable IPv6 processing on a point-to-point interface without assigning it an explicit IPv6 address. In this way, the IPv6 unnumbered interface can borrow the IPv6 address of another interface already configured on the router to conserve network and address space.

Use the `no` parameter with this command to remove this feature on an interface.

### Command Syntax

```
ipv6 unnumbered IFNAME
no ipv6 unnumbered
```

### Parameter

IFNAME	Interface name.
--------	-----------------

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

The following example creates a tunnel on eth1:

```
#configure terminal
(config)#interface lo
(config-if)#ipv6 address::1/128
(config-if)#exit
(config)#interface eth1
(config-if)#ipv6 address fe80::20e:cff:fe6e:56dd/64
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode vxlan
(config-if)#ipv6 unnumbered eth1
(config-if)#ipv6 router ospf area 0 tag 1
(config-if)#exit
(config)#router ipv6 ospf 1
(config-router)#router-id 10.70.0.145
```

---

## link-debounce-time

Use this command to set the debounce time for linkup and linkdown transitions for the interface.

User can set only one of the timers (either linkup or linkdown) by setting the other one to 0.

Use the `no` form of this command to turn off the link debounce timer on the interface.

### Command Syntax

```
link-debounce-time <0-5000> <0-5000>
no link-debounce-time
```

### Parameter

<0-5000>	timer value in milliseconds for the linkup transition
<0-5000>	timer value in milliseconds for the linkdown transition

### Default

By default, it is disabled.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS-SP version 5.0.

### Example

```
#configure terminal
(config)#interface eth1
(config-if)#link-debounce-time 4000 5000
(config-if)#link-debounce-time 0 5000
(config-if)#link-debounce-time 3000 0
```

---

## load interval

Use this command to configure the interval for which average traffic rate need to be shown. Intervals can be configured in steps of 30 seconds.

Use the no parameter with this command to set the load interval to its default.

### Command Syntax

```
load-interval <30-300>
no load-interval
```

### Parameter

<30-300>	Load period in multiples of 30 seconds.
----------	---

### Default

By default, load interval is 300 seconds

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#load-interval 30
(config-if)#no load-interval
```

---

## loopback

Use this command to set the ethernet loopback mode on the interface.

Use the `no` form of this command to remove loopback on the interface.

**Note:** Remote PHY loopback supported only on a single serdes lane of serdes-quad at a time. So below cases are not supported:

1. 100G and 40G interface mode.
2. 2x50G port breakout mode.
3. In 4x10 or 4x25G breakout mode, at a time only one interface is supported.
4. If interface is part of port-group, at a time only one interface is supported.

### Command Syntax

```
loopback ((tx (mac|phy))|(rx phy))
```

### Parameter

The parameters for Tx are MAC or PHY and for Rx is PHY.

### Default

No default value is specified.

### Command Mode

Interface mode

### Applicability

This command is introduced before OcNOS-DC version 5.0.

### Example

```
#configure terminal
(config)#interface xe0
(config-if)#loopback tx mac
(config-if)#exit

(config)#interface xe0
(config-if)#loopback tx phy
(config-if)#exit

(config)#interface xe0
(config-if)#loopback rx phy
(config-if)#exit
```

## loss-measurement uni-link-loss

Use this command to advertise the loss (as a packet percentage) between two directly connected IS-IS/OSPF neighbors.

The A bit is set when the measured value of this parameter exceeds its configured maximum threshold. The A bit is cleared when the measured value falls below its configured reuse threshold.

Use the `no` parameter with this command to unset uni-link-loss on the current interface.

### Command Syntax

```
loss-measurement uni-link-loss ((static VALUE) | (a-bit-threshold min VALUE max VALUE))
no loss-measurement uni-link-loss (static | a-bit-threshold)
```

### Parameter

<code>static</code>	Static value
<code>VALUE</code>	Loss percentage in six precision float format. eg: 3.123456
<code>a-bit-threshold</code>	Threshold values to set/clear A-bit
<code>min</code>	Reuse threshold
<code>VALUE</code>	Reuse threshold percentage in six precision float format. eg:3.123456
<code>max</code>	Maximum threshold
<code>VALUE</code>	Maximum threshold percentage in six precision float format. eg:3.123456

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#configure terminal
(config)#interface eth1
(config-if)#loss-measurement uni-link-loss static 12.3
(config-if)#no loss-measurement uni-link-loss static
(config-if)#loss-measurement uni-link-loss a-bit-threshold min 1.12 max 2.2
(config-if)#no loss-measurement uni-link-loss a-bit-threshold
```

---

## monitor speed

Use this command to enable speed monitoring on interface.

Use the `no` parameter with this command to disable monitoring.

### Command Syntax

```
monitor speed
no monitor speed
```

### Default

By default, speed monitoring will be disabled

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 1.0.

### Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#monitor speed
(config-if)#no monitor speed
```

---

## monitor queue-drops

Use this command to enable queue-drops monitoring on interface.

Use the `no` parameter with this command to disable monitoring.

### Command Syntax

```
monitor queue-drops
no monitor queue-drops
```

### Default

By default, queue-drops monitoring will be disabled

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 1.0.

### Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#monitor queue-drops
(config-if)#no monitor queue-drops
```

---

## monitor speed threshold

Use this command to modify default speed monitor threshold on interface.

Use the `no` parameter with this command to set the monitor speed threshold to its default.

**Note:** Warning threshold must be greater than recovery threshold and it is recommended to keep a difference of 10 percent to avoid frequent notifications caused by variations in average speed.

### Command Syntax

```
monitor speed threshold warning <1-100> recovery <1-100>
no monitor speed threshold
```

### Parameter

<1-100>	Warning level threshold value in percentage
<1-100>	Recovery level threshold value in percentage

### Default

By default, warning threshold is 90 percentage and recovery is 80 percentage.

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 1.0.

### Example

```
#configure terminal
(config)#interface xe1/1
(config-if)# monitor speed threshold warning 80 recovery 70
(config-if)#no monitor speed threshold
```



## mtu

Use this command to set the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) for an interface

Use the `no` parameter with this command to set the MTU to its default.

**Note:** To allow jumbo frames over SVI interfaces, it is mandatory to configure the applicable MTU for the specific SVI interfaces.

### Limitation for MTU configuration on Label-Switching:

Creating a sub-interface automatically increases the physical interface MTU size by 8 bytes to accommodate double VLAN tag encapsulation.

Configuring label switching for physical layer-3 interfaces adds 20 bytes internally to the MTU to accommodate up-to five labels. However, configuring label-switching on sub-interface does not change the MTU of physical interface. Hence, the physical interface requires a manual increase in MTU size.

During the BGP update, in case the control packet contains 1500 bytes when it reaches the hardware, the hardware adds the Encapsulation for the sub-interface and MPLS header (Additional bytes). Now, the hardware drops it as physical port MTU is limited to 1500 bytes.

While configuring MTU on label-switching enabled with Subinterface/SVI/LAG and the Parent Physical port follow guide lines mentioned below:

It is recommended to configure higher MTU on network ports in comparison with access ports. Hence, increase the MTU on both physical and sub-interfaces to accommodate the PDU.

When using sub-interface for MPLS network interfaces, considering the default MTU of 1500, minimum MTU configuration recommendation is as follows

- **Sub-interface:** MTU 1520 (to accommodate 5 MPLS labels)
- **Physical interface:** MTU 1528: (Default MTU 1500 + double encap 8 + MPLS up-to 5 labels 20) = 1528).  
 Note: MTU configuration is considered from IP header onwards. Hence, OcNOS adds 14 bytes to MTU internally to accommodate L2 header. The effective MTU in hardware will be  $1528 + 14 = 1542$ .
- **LAG interface:** MTU is applied on all members internally
- **SVI:** When label-switching enabled on VLAN interface, MTU value must be manually increased by at least 20 bytes on Parent interfaces of VLAN.  
 Example, default MTU must be set as 1520 instead of 1500 on label-switching parent interface label switched VLAN interface. (Parent Interface MTU  $\geq$  label switched VLAN interface MTU + 20).

### Command Syntax

```
mtu <64-65536>
no mtu
```

### Parameter

<code>&lt;64-65536&gt;</code>	Specify the size of MTU in bytes:
	<code>&lt;64-16338&gt;</code> for L2 packet
	<code>&lt;576-9216&gt;</code> for L3 IPv4 packet
	<code>&lt;1280-9216&gt;</code> for L3 IPv6 packet

<576–65536> for IPv4 packet

<1280–65536> for IPv6 packet on loopback interface

### Default

By default, MTU is 1500 bytes

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#interface eth3
(config-if)#mtu 120
```

---

## multicast

Use this command to set the multicast flag for the interface.

Use the `no` form of this command to disable this function.

### Command Syntax

```
multicast
no multicast
```

### Parameters

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 eth3
(config-if)#multicast
```

# show flowcontrol

Use this command to display flow control information.

## Command Syntax

```
show flowcontrol
show flowcontrol interface IFNAME
```

## Parameters

interface IFNAME      Specify the name of the interface to be displayed.

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

The following is a sample output of the `show flowcontrol interface` command displaying flow control information:

```
#show flowcontrol interface ge1
Port      Send FlowControl   Receive FlowControl RxPause TxPause
          admin    oper      admin    oper
-----
ge1       on      on        on      on          0      0
#
```

[Table 15-31](#) explains the show command output fields.

**Table 15-31: show flow control output**

Entry	Description
Port	Interface being checked for flowcontrol.
Send admin	Displays whether the flowcontrol send process is administratively on or off.
FlowControl oper	Displays whether send flowcontrol is on or off on this interface.
Received admin	Displays whether the flowcontrol receive process is administratively on or off.
FlowControl oper	Displays whether receive flowcontrol is on or off on this interface.
RxPause	Number of received pause frames.
TxPause	Number of transmitted pause frames.

---

## show hardware-discard-counters

Use this command to check device level discard counters.

### Command Syntax

```
show hardware-discard-counters
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

The command is introduced before OcNOS version 1.3.

Qumran devices do not support discard counters per interface. Only global level counters are available for advanced debugging using the [show hardware-discard-counters](#) command.

### Examples

```
#show hardware-discard-counters
+-----+-----+
| Registers                                | Core 0          |
+-----+-----+
CGM_VOQ_SRAM_ENQ_RJCT_PKT_CTR           437
Reason : QNUM_NOT_VALID                  Y
EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER   8894
Reason : SRC_EQUAL_DEST_INT              Y
```

See [Table 15-32](#) and [Table 15-33](#) for details:

**Table 15-32: Table detailing about counters supported**

Register	Description
CGM_VOQ_SRAM_ENQ_RJCT_PKT_CTR for QAX	Drop is due to PPdecision to drop, or invalid destination received from PPblocks.
IQM_QUEUE_ENQ_DISCARDED_PACKET_COUNTER for QMX	The packet DP (Drop Precedence) is higher than the configured Drop DP.
EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER	Seen with unknown unicast frames, source and destination learnt from same interface.

**Table 15-33: Table detailing about reasons supported**

Register	Description
QNUM_NOT_VALID for QAX	Seen with Vlan Discards, ACL Drops, Storm Control, STP Blocked Port.  Seen with Policer Discards.
QUEUE_NOT_VALID_STATUS for QMX	
DP_LEVEL_RJCT for QAX	
DP_LEVEL_STATUS for QMX	
SRC_EQUAL_DEST_INTF	Seen when traffic is not learned, but is still forwarded/flooded.

---

## show interface

Use this command to display interface configuration and status information.

### Command Syntax

```
show interface (IFNAME|)
```

### Parameter

IFNAME	Interface name.
--------	-----------------

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show interface xe1/1
Interface xe1/1
  Scope: both
  Flexport: Breakout Control Port (Active): Break Out Enabled
  Hardware is ETH   Current HW addr: ecf4.bb6e.934b
  Physical:ecf4.bb6e.934b   Logical:(not set)
  Port Mode is access
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full(auto) link-speed 1g(auto)
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  DHCP client is disabled.
  Last Flapped: 2016 Nov 05 22:40:23 (00:19:25 ago)
  Statistics last cleared: 2016 Nov 05 04:49:55 (18:09:53 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 256 bits/sec, 0 packets/sec
  RX
    unicast packets 39215813 multicast packets 0 broadcast packets 0
    input packets 39215813 bytes 2666662432
    jumbo packets 0
    runs 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 38902 multicast packets 437 broadcast packets 0
    output packets 437 bytes 28018
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```

Table 15-34 explains the output fields.

**Table 15-34: show interface output details**

Field	Description
Scope	Interface can be used for communication within the device and outside the device (Both).
Flexport	Specifies whether the ports has Breakout capabilities or is a Non-Control Port.
Breakout Control Port (Active)	Specifies whether Breakout is active or disabled.
Hardware is ETH Current HW addr	The MAC address of the interface.
Physical	Displays the physical MAC address of the interface.
Logical	Displays the logical MAC address (if any) of the interface.
Port Mode	Displays the port mode: Router, VLAN access, switch, or trunk.
Interface index	Index number, Metric, MTU size, duplex-full (auto) or half-duplex, minimum link speed in gigabits, and if the interface is up, broadcasting, and multicasting.
VRF Binding	Show whether the interface is VRF bound and (if bound) with what VRF, if Label Switching is enabled or disabled, and if a virtual circuit is configured.
DHCP client	The state of the DHCP client – whether this interface is connected to a DHCP server.
Last Flapped	Date and time when the interface last flapped.
Statistics last cleared	Date and time when the interface's statistics were cleared.
5 minute input rate	Input rate in bits/second and packets/second
5 minute output rate	Output rate in bits/second and packets/second
RX	Counters for unicast packets, multicast packets, broadcast packets, input packets, bytes, jumbo packets, runs, giants, CRC errors, fragments, jabbers, input errors, input with dribble input discards, and receive pause.
TX	Counters for unicast packets, multicast packets, broadcast packets, output packets, bytes, jumbo packets, output errors, collisions, differed packets, input late collisions, output discards, and transmit pause.



---

## show interface capabilities

Use this command to display interface capabilities

### Command Syntax

```
show interface (IFNAME|) capabilities
```

### Parameters

IFNAME	Displays the name of a specific interface for which status and configuration data is desired.
--------	---

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show interface xe1/1 capabilities
xe1/1
Speed(FD) : 10MB,100MB,1000MB,10GB,20GB,40GB
Interface : xgmii
Medium : copper
Loopback : none,MAC,PHY
Pause : pause_tx,pause_rx,pause_asymm
Flags : autoneg
Encap : IEEE,HIGIG,HIGIG2
```

[Table 15-35](#) explains the show command output fields.

**Table 15-35: show interface capabilities output details**

Field	Description
Interface number	The identifying ID number of the interface – eht0, xe1, etc.
Speed (FD)	The Flexible Data-Rates (FD) of the interface
interface	XAUI is a standard for extending the XGMII (10 Gigabit Media Independent Interface) between the MAC and PHY layer of Gigabit Ethernet.
Medium	Members have to have the same medium type configured. This only applies to Ethernet port-channel. Copper, fiber optics, etc.
Loop back	The loop back between the MAC and PHY layers.
Pause	Pause transmit, pause receive, pause asymmetrically.

Table 15-35: show interface capabilities output details

Field	Description
Flags	Interface flags set for Auto-negotiation.
Encap	Encapsulation – IEEE, HIGIG, and HIGIG2 specifications – HIGIG is a proprietary protocol that is implemented by Broadcom. The HIGIG protocol supports various switching functions. The physical signaling across the interface is XAUI, four differential pairs for receive and transmit (SerDes), each operating at 3.125 Gbit/s.

---

## show interface counters

Use this command to display the ingress and egress traffic counters on the interface.

**Note:** Counters are meant for debugging purpose and the accuracy of the transmit discard counter is not guaranteed in all scenarios.

### Command Syntax

```
show interface (IFNAME|) counters (active|)
show interface cpu counters
```

### Parameter

IFNAME	Interface name.
active	Statistics for link-up interfaces.
cpu	CPU interface.

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show interface xel1/1 counters
Interface xel1/1
  Scope: both
  Rx Packets: 1000
  Rx Bytes: 1000000
  Rx Unicast Packets: 1000
  Rx Packets from 512 to 1023 bytes: 1000
  Tx Packets: 3897
  Tx Bytes: 249408
  Tx Multicast Packets: 3897
  Tx Packets with 64 bytes: 3897
  Tx Packet rate: 1 pps
  Tx Bit rate: 255 bps

#show interface cpu counters
CPU Interface
  Tx Packets: 104508
  Tx Bytes: 7106272
  Tx Discard Packets: 89613672
  Tx Discard Bytes: 5735237844
  Rx Discard Packets: 11938
```

[Table 15-36](#) explains the output fields.

Table 15-36: show interface counters output details

Field	Description
Receive Counters	Rx Packets Rx Bytes Rx Unicast Packets Rx Multicast Packets Rx Broadcast Packets Rx Packets with 64 bytes Rx Packets from 65 to 127 bytes Rx Packets from 128 to 255 bytes Rx Packets from 256 to 511 bytes Rx Packets from 512 to 1023 bytes Rx Packets from 1024 to 1518 bytes Rx Packets from 1519 to 2047 bytes Rx Packets from 2048 to 4095 bytes Rx Packets from 4096 to 9216 bytes Rx Jumbo Packets Rx Discard Packets (not applicable for Qumran platform) Rx Packets with error Rx CRC Error Packets Rx Undersized Packets Rx Oversized Packets Rx Fragment Packets Rx Jabber Packets Rx MAC error Packets Rx Pause Packets Rx Unrecognized MAC Control Packets Rx Drop Events Rx Packet rate Rx Bit rate

**Table 15-36: show interface counters output details**

Field	Description
Transmit Counters	Tx Packets Tx Bytes Tx Unicast Packets Tx Multicast Packets Tx Broadcast Packets Tx Packets with 64 bytes Tx Packets from 65 to 127 bytes Tx Packets from 128 to 255 bytes Tx Packets from 256 to 511 bytes Tx Packets from 512 to 1023 bytes Tx Packets from 1024 to 1518 bytes Tx Packets from 1519 to 2047 bytes Tx Packets from 2048 to 4095 bytes Tx Packets from 4096 to 9216 bytes Tx Jumbo Packets Tx Discard Packets (not applicable for Qumran platform) Tx Packets with error Tx Collisions Tx Late Collisions Tx Excessive Collisions Tx Pause Packets Tx Packet rate Tx Bit rate
CPU Interface Counters	Tx Packets Tx Bytes Tx Discard Packets Tx Discard Bytes Rx Discard Packets

## show interface counters drop-stats

Use this command to display the ingress and egress traffic discard reason counters on the interface.

- Note: You can only display statistics for physical ports and cpu ports, but not for the out-of-band management (OOB) management port or logical interfaces.
- Note: Drops in the CPU queue are listed under Tx Multicast Queue Drops, whether the packet is unicast or multicast

### Command Syntax

```
show interface (IFNAME|) counters drop-stats
show interface cpu counters drop-stats
```

### Parameter

IFNAME	Physical interface name
cpu	CPU interface

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.1.

For Qumran devices, only error statistics are applicable and discard counters are not applicable. Only global level counters are available for advanced debugging using the command [show hardware-discard-counters](#).

### Example

```
#show interface xe32/2 counters drop-stats
+-----+-----+-----+-----+
| Counter Description | Count          | Last Increment | Last Increment Time |
+-----+-----+-----+-----+
Rx Bad CRC errors    0                0
Rx Undersize errors  0                0
Rx Oversize errors   0                0
Rx Fragments errors  0                0
Rx Jabbers errors    0                0
Rx Port Block Drops  6                1                2016 Nov 09 08:59:33
Rx Vlan Discards     0                0
Rx ACL/QOS Drops     0                0
Rx Policy Discards   0                0
Rx EGR Port Unavail  38784           5                2016 Nov 09 18:19:31
Rx IBP Discards      0                0
Tx Port Block Drops  359             1                2016 Nov 09 08:59:33
Tx Vlan Discards     0                0
Tx TTL Discards      0                0
Tx Unknown Discards  359             1                2016 Nov 09 08:59:33
Tx Ucast Queue Drops 0                0
Tx Mcast Queue Drops 0                0
+-----+-----+-----+-----+
```

Table 15-37 explains the output fields.

**Table 15-37: show interface counters drop-stats output details**

Field	Description
Counter Description	Shows the type of packet and/or the reason why the packet was dropped.
Count	The number of packets dropped for each reason.
Last Increment	Number of packets dropped since this command was last entered.
Last Increment Time	Date and time when the last packet was dropped.
Rx Bad CRC errors	Received packets dropped because they didn't pass the cyclic Redundancy Check (CRC).
Rx Undersize errors	Number of received runt packets dropped.
Rx Oversize errors	Number of received giant packets dropped
Rx Fragments errors	Number of received packet fragments dropped
Rx Jabbers errors	Received packets dropped because of jabber – long packet error.
Rx Port Block Drops	Received packets dropped because port blocking is enabled (not applicable for Qumran platform).
Rx Vlan Discards	VLAN received packets dropped because there is no VLAN configured on the port (not applicable for Qumran platform).
Rx ACL/QOS Drops	Received packets match a field processing entry with a drop or color drop action, such as: User-configured ACL that denies traffic Service policy with a police action that drops the traffic received at a rate higher than the configured limit. (not applicable for Qumran platform)
Rx Policy Discards	Received packets dropped because of device policies violated, such as a storm control rate violation (not applicable for Qumran platform).
Rx EGR Port Unavail	No output port can be determined for these received packets. This counter increments along with other counter types in this table because it is a “catchall” for multiple types of discards as shown below (not applicable for Qumran platform):  VLAN check failed MTU check failed ACL/QoS drops Policy discards Source MAC is null Destination IP/source IP address is null Source MAC address and destination MAC address are the same Forwarding lookup failure
Rx IBP Discards	Ingress Back Pressure (ingress congestion) when the ingress packets buffer is full for an interface. (not applicable for Qumran platform)
Tx Port Block Drops	Transmitted packets dropped because port blocking is enabled (not applicable for Qumran platform).
Tx Vlan Discards	Transmitted VLAN packets dropped because there is no VLAN configured on the port (not applicable for Qumran platform).

Table 15-37: show interface counters drop-stats output details (Continued)

Field	Description
Tx TTL Discards	Transmitted packets discarded because their Time To Live (TTL) has ended. (not applicable for Qumran platform)
Tx Unknown Discards	Transmitted packets dropped for unknown reason. May have something to do with the condition/configuration of the port at the other end of the connection (not applicable for Qumran platform).
Tx Ucast Queue Drops	Transmitted packets dropped as a result of Unicast buffer overflow.
Tx Mcast Queue Drops	Transmitted packets dropped as a result of Multicast buffer overflow.



## show interface counters error-stats

Use this command to display the ingress error traffic counters on the interface.

### Command Syntax

```
show interface (IFNAME|) counters error-stats
```

### Parameter

IFNAME                      Interface name.

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show interface xe1/1 counters error-stats
+-----+-----+-----+-----+-----+-----+-----+
|Interface|Total errors|Bad CRC|Undersize|Oversize|Fragments|Jabbers|
+-----+-----+-----+-----+-----+-----+-----+
|xe1/1    |120         |8      |100      |10       |2         |0       |
```

Table 15-38 explains the columns in the output.

**Table 15-38: error traffic counters**

Column	Description	Causes
Interface	Name of the interface	Point of interconnection in network.
Total errors	Total number of all types of errors	Number of errors in network.
Bad CRC	Number of packets received by the port from the network, where the packets have no CRC or a bad CRC.	Packet data modified making the CRC invalid.
Undersize	Total number of packets received that are less than 64 octets long (which exclude framing bits, but include the FCS) and have a good FCS value.	Bad frame generated by the connected device.
Oversize	Number of packets received by the port from the network, where the packets were more than maximum transmission unit size.	Faulty hardware, dot1q, or ISL trunking configuration issues.
Fragments	Total number of frames whose length is less than 64 octets (which exclude framing bits, but which include the FCS) and have a bad FCS value.	Ports are configured at half-duplex. Change the setting to full-duplex.
Jabbers	Total number of frames whose length is more than the maximum MTU size. (which exclude framing bits, but which include FCS) and have a bad FCS value.	Ports are configured at half-duplex. Change the setting to full-duplex.

## show interface counters (indiscard-stats|outdiscard-stats)

Use this command to display the ingress and egress traffic discard reason counters on the interface.

Note: You can only display statistics for data ports and CPU ports, not for the out-of-band management (OOB) management port or logical interfaces.

### Command Syntax

```
show interface (IFNAME|) counters (indiscard-stats|outdiscard-stats)
show interface cpu counters (indiscard-stats|outdiscard-stats)
```

### Parameter

IFNAME	Physical Interface name.
indiscard-stats	Discard reasons for ingress dropped packets.
outdiscard-stats	Discard reasons for egress dropped packets.
cpu	CPU Interface.

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

### Examples

```
#show interface xe1/3 counters indiscard-stats
+-----+-----+-----+-----+
| Counter Description | Count      | Last Increment | Last Increment Time |
+-----+-----+-----+-----+
STP Discards         0              0
Vlan Discards         0              0
ACL Drops             0              0
Policy Discards       0              0
EGR Port Unavail    1092867      1092867      2016 Oct 25 19:54:58
IBP Discards         0              0
+-----+-----+-----+-----+

#show interface counters indiscard-stats
+-----+-----+-----+-----+-----+-----+-----+-----+
| Interface | Port Block Drops | Vlan Discards | ACL/QOS Drops | Policy Discards | EGR Port Unavail | IBP Discards | Total Discards |
+-----+-----+-----+-----+-----+-----+-----+-----+
xe1        0              0          35703          0              11              0          35714
xe2        0              0          295744         0              13604           0          309348
xe3        0              0           9501          0              20405           0          29906
xe5        0              0              0          0              13602           0          13602
xe49/1     0              0              0          0              0             20658          20658
xe52/1     0              3          856029        10             13613           0          869642
xe54/1     0             5371          0              0             5371           0          5371
cpu        0              0              0          0              6              0           N/A

#show interface counters outdiscard-stats
```

Interface Discards	Port Block Drops	Vlan Discards	TTL Discards	Unknown Discards	UcastQ Drops	McastQ Drops	Total
xe1	0	0	0	204338	0	0	204338
xe2	0	0	0	1094368	0	0	1094368
xe3	0	0	0	818672	0	0	818672
xe52/1	0	0	0	1275156	0	0	1275156
xe54/1	0	0	0	13575	0	0	13575
cpu	0	0	0	0	N/A	1014224	N/A

Table 15-39 explain the fields in the command output.

**Table 15-39: indiscard statistic output details**

Statistic	Description
STP Discards	Packets received when the ingress interface is not in STP forwarding state.
Port Block Drops	Packets discarded on an ingress interface where port blocking is configured.
VLAN Discards	VLAN tagged packets received on a port which is not a member of the VLAN or untagged packets received on a trunk port.
ACL/QoS Drops	Incoming packets match a field processing entry with a drop or color drop action, such as: 1. User-configured ACL that denies traffic 2. Service policy with a police action that drops the traffic received at a rate higher than the configured limit
Policy Discards	Device policies violated, such as a storm control rate violation, source or destination discards when L2 tagged traffic received on router interface.
EGR (Egress) Port Unavail	No output port can be determined for this packet. This counter increments along with other counter types in this table because it is a "catchall" for multiple types of discards as shown below: 1. VLAN check failed 2. MTU check failed 3. ACL/QoS drops 4. Policy discards 5. Source MAC is null 6. Destination IP/source IP address is null 7. Source MAC address and destination MAC address are the same 8. Source MAC is configured as static on other interface 9. Forwarding lookup failure
IBP Drops	Ingress Back Pressure (ingress congestion) when the ingress packet buffer is full for an interface.
Total Discards	Total number of ingress dropped packets.

Table 15-40 explain the fields in the command output.

**Table 15-40: outdiscard statistics**

Statistics	Description
Port Block Drops	Packets discarded on an egress interface where port blocking is configured.
VLAN Discards	Packets discarded because an invalid VLAN tag is encountered at an egress interface.
TTL Discards	Packets discarded because the Time-To Live (TTL) of the outgoing packet has passed.

Table 15-40: outdiscard statistics

Statistics	Description
Unknown Discards	Packets discarded for other possible reasons like ACL drop in egress or a policer drop in egress. Discards caused by congestion at queues and drops at queues are not counted under unknown discards.
Unicast Queue Drops	Packets dropped in the unicast queues because of congestion.
Multicast Queue Drops	Packets dropped in the multicast queues because of congestion.
Total Discards	Total number of egress dropped packets.

---

## show interface counters protocol

Use this command to display protocol packets received at the CPU by the control plane.

### Command Syntax

```
show interface (IFNAME|) counters protocol
```

### Parameters

IFNAME                      Interface name.

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

### Example

```
#show interface counters protocol
Interface cel/1
  lacp           : 4
  icmp6          : 5
```

[Table 15-41](#) explain the fields in the command output.

**Table 15-41: show interface counters protocol output details**

Field	Description
Interface	Name of the configured interface.
lacp	Total number of lacp protocol in the interface.
icmp6	Total number of icmp6 protocol in the interface.

# show interface counters queue-drop-stats

Use this command to display dropped packets in the CPU queue and the last increment time.

## Command Syntax

```
show interface cpu counters queue-drop-stats
```

## Parameters

cpu CPU interface.

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
show interface cpu counters queue-drop-stats
+-----+-----+-----+-----+
| Queue Name | Count | Last Increment | Last Increment Time |
+-----+-----+-----+-----+
arp          169735545      9145653      2017 Oct 23 14:33:54
```

[Table 15-42](#) explain the fields in the command output.

Table 15-42: show interface counters queue-drop-stats output details

Field	Description
Queue Name	Name of the protocol.
Count	Number of arp protocols in the interface.
Last Increment	Final increment number in the protocol.
Last Increment time	Time of the last increment in the protocol.

## show interface counters queue-stats

Use this command to display transmitted and dropped packet and byte counts of individual queues.

Note: In Qumran devices, all packets dropped in a queue are counted (even policer drops).

### Command Syntax

```
show interface (IFNAME|) counters queue-stats
show interface cpu counters queue-stats
```

### Parameters

IFNAME	Interface name.
cpu	CPU interface.

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

Note: Default traffic counters are not supported on Qumran AX.

### Example

```
#show interface counters queue-stats
D - Default Queue, U - User-defined Queue
+-----+-----+-----+-----+-----+-----+
|Interface|Queue/Class-map|Q-Size|Output pkts|Output bytes|Dropped pkts|Dropped bytes |
+-----+-----+-----+-----+-----+-----+
xe1/1    q1          (D) 0    12      1368      0          0
xe1/1    mc-q7       (D) 0     1       82        0          0
xe25     q1          (D) 0     6       684        0          0

#show interface xe1/1 counters queue-stats
D - Default Queue, U - User-defined Queue
+-----+-----+-----+-----+-----+-----+
|Queue/Class-map|Q-Size|Tx pkts|Tx bytes |Dropped pkts|Dropped bytes |
+-----+-----+-----+-----+-----+-----+
q0          (D) 0     0       0         0         0
q1          (D) 0    12     1368        0         0
q2          (D) 0     0       0         0         0
q3          (D) 0     0       0         0         0
q4          (D) 0     0       0         0         0
q5          (D) 0     0       0         0         0
q6          (D) 0     0       0         0         0
q7          (D) 0     0       0         0         0
mc-q0       (D) 0     0       0         0         0
mc-q1       (D) 0     0       0         0         0
mc-q2       (D) 0     0       0         0         0
mc-q3       (D) 0     0       0         0         0
mc-q4       (D) 0     0       0         0         0
mc-q5       (D) 0     0       0         0         0
mc-q6       (D) 0     0       0         0         0
mc-q7       (D) 0     1       82        0         0

#show interface cpu counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+-----+-----+-----+-----+-----+-----+
| Queue/Class-map | Q-Size | Tx pkts | Tx bytes | Dropped pkts | Dropped bytes |
+-----+-----+-----+-----+-----+-----+
igmp            (E) 800592 14519      987292    1304163    88683084
```

arp

(E) 1250496 1008785

68597380

0

0

Table 15-43 explain the fields in the command output.

Table 15-43: queue flags detail

Flag	Meaning
D	Default queue of the port.
U	User defined queue of the port.
E	Outgoing hello packet's queue in the port.
I	Incoming hello packet's queue in the port.
Q	Hello packet's queue size in bytes.

Table 15-44 explain the fields in the command output.

Table 15-44: show interface counters queue-stats output details

Field	Description
Interface	A defined physical interface to which the queue is associated.
Queue/Class-map	Queues associated with a QoS class-map.
Q-Size	The size of a specified queue in bytes.
Output pkts	The number of out bound packets residing in the queues.
Output Bytes	The number of bytes in the outbound queue.
Dropped pkts	The number of packets dropped because of queue overflow.
Dropped bytes	The number of bytes dropped because of queue overflow.
Tx pkts	The number of transmit packets contained in the out bound queue.
Tx bytes	The number of transmit bytes contained in the out bound queue.



## show interface counters rate

Use this command to display the average traffic rate over the load interval of the interface.

### Command Syntax

```
show interface (IFNAME|) counters rate (kbps|mbps|gbps|)
show interface cpu counters rate (kbps|mbps|gbps|)
```

### Parameter

IFNAME	Interface name.
kbps	Kilobits per second.
mbps	Megabits per second.
gbps	Gigabits per second.
cpu	CPU interface.

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show interface counters rate
```

Interface	Rx		Tx	
	bps	pps	bps	pps
xe1/1	548439552	1008160	544400	1000

```
#show interface cpu counters rate
```

Load interval: 30 second

CPU Queue(%)		Rx bps	Rx pps	Tx bps	Tx pps
isis	( 0%) -	-	-	742	0
arp	( 0%) -	-	-	6	0

[Table 15-45](#) explain the fields in the command output.

**Table 15-45: show interface counters rate output details**

Field	Description
Interface	The particular interface.
RX	Number of hello packets received from the neighbor.
TX	Number hello packets transmitted to the neighbor.
bps	Bytes per second.
pps	Packets per second.
CPU Queue	CPU Queues used for various functions. In the example the CPU is maintaining queues for ARP and the IS-IS routing facilities.
Load interval	The length of time for which data is used to compute load statistics.
RX bps	Number of hello packets received from the neighbor in bytes per second.
RX pps	Number of hello packets received from the neighbor in packets per second.
TX bps	Number hello packets transmitted to the neighbor in bytes per second.
Tx pps	Number hello packets transmitted to the neighbor in packets per second.

## show interface counters speed

Use this command to display the current average speed on the interface.

### Command Syntax

```
show interface (IFNAME|) counters speed (kbps|mbps|gbps|)
```

### Parameter

IFNAME	Interface name.
kbps	Kilobits per second.
mbps	Megabits per second.
gbps	Gigabits per second.

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced in OcNOS-SP version 1.0.

### Example

```
#show interface counters speed
* indicates monitor is active
+-----+-----+-----+-----+
|speed      |      |      |      |      |      |      |      |      |
| interface | configured |      |      |      |      |      |      |
+-----+-----+-----+-----+-----+-----+-----+
| bps) | % | speed ( bps) | Warning | Recovery | Rx ( bps) | % | Tx (
+-----+-----+-----+-----+-----+-----+-----+
ce45      100000000000 90      80      0      0.00 0
0.00
xe7        10000000000 90      80      0      0.00 0
0.00
xe31       10000000000 90      80      0      0.00 0
0.00
xe33       10000000000 90      80      0      0.00 0
0.00
xe39       10000000000 90      80      0      0.00 0
0.00
xe40       10000000000 90      80      0      0.00 0
0.00
#
```

# show interface counters summary

Use this command to display the summary of traffic counters on a specific interface or all interfaces.

Note: This command is supported for the out-of-band management (OOB) management interface.

## Command Syntax

```
show interface (IFNAME|) counters summary
```

## Parameter

IFNAME                      Interface name.

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

#show interface xe1/1 counters summary

Interface	Rx packets	Rx bytes	Tx packets	Tx bytes
xe1/1	11032977	11032960000	61	3904

#show interface counters summary

Interface	Rx packets	Rx bytes	Tx packets	Tx bytes
eth0	206222	13756391	235123	337010937
po1	809121	72989094	825221	90605534
xe1/1	0	0	1	114
xe3/1	43	4730	21	2298
xe5/1	29	3178	21	2298
xe8	10	1076	14	1532
xe9/1	16	1760	21	2298
xe11/1	0	0	7	766
xe19/1	12426292	1298526692	6	620
xe21/1	13	1386	14	1532
xe28/1	3144	202370	21	2298
xe30/1	3161	202304	7	766
xe32/1	694067	61687838	710274	79315093
xe32/2	115054	11301256	114947	11290441
xe32/3	603759	51208946	620502	68865557
xe32/4	7	766	7	766

Table 15-46 explain the fields in the command output.

**Table 15-46: show interface counters summary output details**

Field	Description
Interface	The particular interface.
RX	Number of hello packets received from the neighbor.
TX	Number hello packets transmitted to the neighbor.
bps	Bytes per second.
pps	Packets per second.
RX bps	Number of hello packets received from the neighbor in bytes per second.
RX pps	Number of hello packets received from the neighbor in packets per second.
TX bps	Number hello packets transmitted to the neighbor in bytes per second.
Tx pps	Number hello packets transmitted to the neighbor in packets per second.

# show interface fec

Use this command to display the FEC (forward error correction) statistics for an interface.

Note: You can only display FEC statistics for physical interfaces and not for management or logical interfaces.

## Command Syntax

```
show interface (IFNAME|) fec
```

## Parameters

IFNAME                      Physical Interface name.

## Default

None

## Command Mode

Exec and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#sh int ce54 fec
+-----+-----+-----+-----+-----+-----+
| Interface | Config | HW Status | Oper Status | Corrected Block Count | Uncorrected Block Count |
+-----+-----+-----+-----+-----+-----+
| ce54      | on      | c191      | c191      | 0                   | 12                      |
+-----+-----+-----+-----+-----+-----+

#sh int ce53 fec
+-----+-----+-----+-----+-----+-----+
| Interface | Config | HW Status | Oper Status | Corrected Block Count | Uncorrected Block Count |
+-----+-----+-----+-----+-----+-----+
| ce53      | auto   | c191      | c191      | 0                   | 0                       |
+-----+-----+-----+-----+-----+-----+

#sh int ce52 fec
+-----+-----+-----+-----+-----+-----+
| Interface | Config | HW Status | Oper Status | Corrected Block Count | Uncorrected Block Count |
+-----+-----+-----+-----+-----+-----+
| ce52      | off    | off       | off       | 0                   | 0                       |
+-----+-----+-----+-----+-----+-----+
```

Table 15-41 explain the fields in the command output.

Table 15-47: show interface fec

Field	Description
Interface	Name of the configured interface.
config	Configured value.
HW Status	FEC currently programmed in HW.
Oper Status	FEC currently operating over the link.

**Table 15-47: show interface fec (Continued)**

Corrected Block Count	Number of the corrected block count.
Uncorrected Block Count	Number of the uncorrected block count.

# show ip forwarding

Use this command to display the IP forwarding status.

## Command Syntax

```
show ip forwarding
```

## Parameters

None

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

The following is a sample output of the `show ip forwarding` command displaying the IP forwarding status.

```
#show ip forwarding
vrf (management) :IP forwarding is on
vrf (default) :IP forwarding is on
#
```

[Table 15-48](#) explain the fields in the command output.

Table 15-48: show ip forwarding

Field	Description
vrf (management)	Management VRF is for management purposes. IP forwarding packet is on.
vrf (default)	The default VRF uses the default routing context for ip forwarding. IP forwarding packet is on.



# show ip interface

Use this command to display brief information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

## Command Syntax

```
show ip interface brief
show ip interface IFNAME brief
```

## Parameters

IFNAME	Interface name.
brief	Brief summary of IP status and configuration.

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

The following is a sample output from the `show ip interface brief` command:

```
#show ip interface brief

'*' - address is assigned by dhcp client

Interface      IP-Address      Admin-Status      Link-Status
eth0            *10.10.26.101    up                 up
lo              127.0.0.1        up                 up
lo.management  127.0.0.1        up                 up
xe1/1           10.1.1.1         up                 up
xe1/2           unassigned       down               down
xe1/3           unassigned       down               down
xe1/4           unassigned       down               down
xe2             unassigned       up                 down
xe3/1           unassigned       up                 up
xe3/2           unassigned       down               down
xe3/3           unassigned       down               down
```

[Table 15-49](#) explain the fields in the command output.

**Table 15-49: show ip interface output details**

Field	Description
Interface	Interface name, also specifies interface type (eth0, lo, xe1/1, and xe1/2).
IP-Address	The IP address assigned to the interface. An asterisks indicates that the IP address was provided by DHCP.

**Table 15-49: show ip interface output details (Continued)**

Field	Description
Admin-Status	Interface is up and functioning or down.
Link-Status	Interface is connected and passing traffic.

---

## show ip prefix-list

Use this command to display the prefix list entries for IPv4 interfaces.

### Syntax Description

```
show ip prefix-list
show ip prefix-list WORD
show ip prefix-list WORD seq <1-4294967295>
show ip prefix-list WORD A.B.C.D/M
show ip prefix-list WORD A.B.C.D/M longer
show ip prefix-list WORD A.B.C.D/M first-match
show ip prefix-list summary
show ip prefix-list summary WORD
show ip prefix-list detail
show ip prefix-list detail WORD
```

### Parameters

WORD	Name of a prefix list.
A.B.C.D/M	IP prefix <network>/<length> (for example, 35.0.0.0/8).
first-match	First matched prefix.
longer	Lookup longer prefix.
<1-4294967295>	Sequence number.
detail	Detail of prefix lists.
summary	Summary of prefix lists.

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

The following is a sample output of the `show ip prefix-list` command showing prefix-list entries.

```
#show ip prefix-list
ip prefix-list myPrefixList: 3 entries
  seq      5 permit 172.1.1.0/16
  seq     10 permit 173.1.1.0/16
  seq     15 permit 174.1.1.0/16
```

---

## show ip route

Use this command to display the IP routing table for a protocol or from a particular table.

When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. All best routes are entered into the FIB and can be viewed using this command. To display all routes (selected and not selected), use the `show ip route database` command.

Use this command to see all subnets of a specified network if they are present in the routing table. Please use this command with mask information.

### Command Syntax

```
show ip route A.B.C.D
show ip route (database|)
show ip route (database|) (bgp|connected|database|isis|fast-
  reroute|interface|isis|kernel|mbgp|mstatic|next-hop|ospf|rip|static)
show ip route summary
show ip route vrf WORD (database|)
show ip route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)
```

### Parameters

A.B.C.D	Network in the IP routing table.
A.B.C.D/M	IP prefix <network>/<length>, for example, 35.0.0.0/8.
bgp	Border Gateway Protocol.
connected	Connected.
database	Routing table database.
fast-reroute	Fast reroute repair paths.
interface	Interface.
isis	IS-IS.
kernel	Kernel.
mbgp	Multiprotocol BGP routes.
mstatic	Multicast static routes.
next-hop	Next hop address.
ospf	Open Shortest Path First.
rip	Routing Information Protocol.
static	Static routes.
summary	Summarize all routes.
WORD	Routes for a Virtual Routing/Forwarding instance.

### Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example: Display FIB Routes

The following shows output for the best routes.

```
#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
```

---

## show ip route A.B.C.D/M longer-prefixes

Use this command to see all subnets of a specified network if they are present in the routing table. Please use this command with mask information.

### Command Syntax

```
show ip route A.B.C.D/M longer-prefixes
```

### Parameters

A.B.C.D/M

### Command Mode

Exec-mode and Privileged exec-mode

### Applicability

This command was introduced from OcNOS 1.3.6

### Example

```
OcNOS#sh 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 10.1.1.0/24 is directly connected, eth1, 00:00:23

C 10.12.41.0/24 is directly connected, eth0, 00:00:23

S 55.0.0.0/8 [1/0] is directly connected, eth1, 00:00:23

S 55.0.0.0/12 [1/0] is directly connected, eth1, 00:00:23

S 55.0.0.0/24 [1/0] is directly connected, eth1, 00:00:23

S 55.1.0.0/16 [1/0] is directly connected, eth1, 00:00:23

S 55.1.1.0/24 [1/0] is directly connected, eth1, 00:00:23

C 127.0.0.0/8 is directly connected, lo, 00:00:23

Gateway of last resort is 10.30.0.11 to network 0.0.0.0

K\* 0.0.0.0/0 via 10.30.0.11, eth0

O 9.9.9.9/32 [110/31] via 10.10.31.16, eth2, 00:18:56

K 10.10.0.0/24 via 10.30.0.11, eth0

C 10.10.31.0/24 is directly connected, eth2

S 10.10.34.0/24 [1/0] via 10.10.31.16, eth2

O 10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:20:54

C 10.30.0.0/24 is directly connected, eth0

```
S      11.22.11.0/24 [1/0] via 10.10.31.16, eth2
O E2   14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:18:56
S      16.16.16.16/32 [1/0] via 10.10.31.16, eth2
O      17.17.17.17/32 [110/31] via 10.10.31.16, eth2, 00:20:54
C      45.45.45.45/32 is directly connected, lo
O      55.55.55.55/32 [110/21] via 10.10.31.16, eth2, 00:20:54
C      127.0.0.0/8 is directly connected, lo
```

```
OcNOS#sh ip route 55.0.0.0/7 longer-prefixes
```

```
Routing entry for 55.0.0.0/8
```

```
Known via "static", distance 1, metric 0, External Route Tag: 0, best
```

```
    directly connected, eth1
```

```
Routing entry for 55.0.0.0/12
```

```
Known via "static", distance 1, metric 0, External Route Tag: 0, best
```

```
    directly connected, eth1
```

```
Routing entry for 55.0.0.0/24
```

```
Known via "static", distance 1, metric 0, External Route Tag: 0, best
```

```
    directly connected, eth1
```

```
Routing entry for 55.1.0.0/16
```

```
Known via "static", distance 1, metric 0, External Route Tag: 0, best
```

```
    directly connected, eth1
```

```
Routing entry for 55.1.1.0/24
```

```
Known via "static", distance 1, metric 0, External Route Tag: 0, best
```

```
    directly connected, eth1
```

```
OcNOS#sh ip route 55.0.0.0/8 longer-prefixes
```

```
Routing entry for 55.0.0.0/8
```

```
Known via "static", distance 1, metric 0, External Route Tag: 0, best
```

```
    directly connected, eth1
```

```
Routing entry for 55.0.0.0/12
```

```
Known via "static", distance 1, metric 0, External Route Tag: 0, best
```

```
    directly connected, eth1
```

```
Routing entry for 55.0.0.0/24
```

```
Known via "static", distance 1, metric 0, External Route Tag: 0, best
```

```
    directly connected, eth1
```

## Interface Commands

---

```
Routing entry for 55.1.0.0/16
Known via "static", distance 1, metric 0, External Route Tag: 0, best

    directly connected, eth1
```

```
Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0, External Route Tag: 0, best

    directly connected, eth1
```

```
OcNOS#
OcNOS#sh ip route 55.0.0.0/11 longer-prefixes
Routing entry for 55.0.0.0/12
Known via "static", distance 1, metric 0, External Route Tag: 0, best

    directly connected, eth1
```

```
Routing entry for 55.0.0.0/24
Known via "static", distance 1, metric 0, External Route Tag: 0, best

    directly connected, eth1
```

```
Routing entry for 55.1.0.0/16
Known via "static", distance 1, metric 0, External Route Tag: 0, best

    directly connected, eth1
```

```
Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0, External Route Tag: 0, best

    directly connected, eth1
```

```
OcNOS#
OcNOS#
OcNOS#
OcNOS#sh ip route 55.0.0.0/16 longer-prefixes
Routing entry for 55.0.0.0/24
Known via "static", distance 1, metric 0, External Route Tag: 0, best

    directly connected, eth1
```

```
OcNOS#sh ip route 55.1.0.0/16 longer-prefixes
Routing entry for 55.1.0.0/16
Known via "static", distance 1, metric 0, External Route Tag: 0, best

    directly connected, eth1
```

```
Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0, External Route Tag: 0, best
```



```
directly connected, eth1
```

```
OcNOS#sh ip route 55.1.0.0/20 longer-prefixes
```

```
Routing entry for 55.1.1.0/24
```

```
Known via "static", distance 1, metric 0, External Route Tag: 0, best
```

```
directly connected, eth1
```

```
OcNOS#sh ip route 55.1.0.0/24 longer-prefixes
```

```
% Network not in table
```

```
OcNOS#
```

```
OcNOS#
```

```
OcNOS#
```

```
OcNOS#sh ip route 55.1.1.0/24 longer-prefixes
```

```
Routing entry for 55.1.1.0/24
```

```
Known via "static", distance 1, metric 0, External Route Tag: 0, best
```

```
directly connected, eth1
```

```
OcNOS#
```

## Header

Each entry in this table has a code preceding it, indicating the source of the routing entry. For example, O indicates OSPF as the origin of the route and K indicates that the route has been learned from the kernel. [Table 15-50](#) shows these codes and modifiers.

[Table 15-50](#) explain the fields in the command output.

**Table 15-50: route codes and modifiers**

Code	Meaning	Description
K	kernel	Routes added through means other than by using the CLI; for example by using the operating system route command. Static routes added using kernel commands and static routes added using OcNOS commands are different. The kernel static routes are not redistributed when you give the <code>redistribute static</code> command in a protocol. However, the kernel static routes can be redistributed using the <code>redistribute kernel</code> command.
C	connected	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from other routing protocols. Routes for connected networks always exist in the kernel routing table but as an exception are not marked as kernel routes because OcNOS always calculates entries for these routes upon learning interface information from the kernel.
S	static	Routes manually configured via CLI which are not updated dynamically by IGPs.
The codes below are for routes received and dynamically learned via IGP neighbors. These networks are not directly connected to this device and were announced by some other device on the network. IGPs update these routes as the network topology changes.		
R	RIP	RIP routing process and enter Router mode.

**Table 15-50: route codes and modifiers**

Code	Meaning	Description
B	BGP	Route is from an Border Gateway Protocol.
O	OSPF	Modifiers for 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	Modifiers for IS-IS: L1 - IS-IS level-1 L2 - IS-IS level-2 ia - IS-IS inter area
Other modifiers:		
v	vrf leaked	The device has two or more VRFs configured and each has at least one interface bound to it. While each VRF will have its own routing table, the VRFs can learn each other's routes.
*	candidate default	Route has been added to the FIB. With equal cost paths to a destination, the router does per-packet or per-destination load sharing. An asterisk ("*") means that the route is being used at that instant for forwarding packets. If you run the same <code>show ip route x.x.x.x</code> command over and over, you might see the * moving between the route entries.
>	selected route	When multiple routes are available for the same prefix, the best route. When multiple entries are available for the same prefix, OcNOS uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. OcNOS populates the FIB with the <i>best</i> route to each destination
p	stale info	A route information that is marked stale due to graceful restart.

After the codes, the header has default gateway information:

```
Gateway of last resort is 10.12.4.1 to network 0.0.0.0
```

The “gateway of last resort”, also called the default gateway, is a static route that routes IP address 0.0.0.0 (all destinations) through a single host (the gateway). The effect of setting a gateway is that if no routing table entry exists for a destination address, packets to that address will be forwarded to the gateway router.

## Route Entry Fields

[Table 15-51](#) explains the each route entry fields.

**Table 15-51: route entry output details**

Field	Description
Codes and modifiers	As explained in <a href="#">Table 15-50</a> .
IP address	IP address of the remote network.

**Table 15-51: route entry output details**

Field	Description
Administrative distance and metric	The administrative distance determines how trustworthy this route is. If there is a similar route but with a smaller administrative distance, it is used instead, because it is more “trustworthy”. The smaller the administrative distance, the more trustworthy the route. Directly connected routes have an administrative distance of 0, which makes them the most trustworthy type of route. The metric varies from protocol to protocol, and for OSPF the metric is cost, which indicates the best quality path to use to forward packets. Other protocols, like RIP, use hop count as a metric. For neighboring routers, the metric value is 1.
Next hop router IP address	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Outgoing interface name	Interface used to get to the next-hop address for this route.
Duration	Length of time that this route has been present in the routing table. This is also the length of time this route has existed without an update. If the route were removed and then re-added (if the cable was disconnected, for instance), this timer would begin again at 00:00:00.

### Route Entry Examples

- O        10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:20:54
  - This route in the network 10.10.37.0/24 was added by OSPF.
  - This route has an administrative distance of 110 and metric/cost of 11.
  - This route is reachable via nexthop 10.10.31.16.
  - The outgoing local interface for this route is eth2.
  - This route was added 20 minutes and 54 seconds ago.
- O E2     14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:18:56
  - This route is the same as the other OSPF route above; the only difference is that it is a Type 2 External OSPF route.
- C        10.10.31.0/24 is directly connected, eth2
  - This route is directly connected.
  - Route entries for network 10.10.31.0/24 are derived from the IP address of local interface eth2.
- K        10.10.0.0/24 via 10.30.0.11, eth0
  - This route in the network 10.10.0.0/24 was learned from the kernel routing table (route was statically added using kernel commands).
  - This route is reachable via nexthop 10.30.0.11.
  - The outgoing local interface for this route is eth0.
- K\*       0.0.0.0/0 via 10.30.0.11, eth0
  - This is a default route that was learned from the kernel (route was statically added using kernel commands).
  - This route is reachable via nexthop 10.30.0.11.
  - The local interface for this route is eth0.

### Example: Display OSPF Routes

The following is the output with the `ospf` parameter:

```
#show ip route ospf
O        1.1.1.0/24 [110/20] via 2.2.2.1, eth2, 00:00:44
```

```
O IA    4.4.4.0/24 [110/21] via 2.2.2.1, eth2, 00:00:44
#
```

### Example: Display Route Summary

The following is the output with the `summary` parameter.

```
#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source      Networks
kernel            1
connected         5
ospf              2
Total             8
FIB               2
```

### Example: Display RIB Routes

The following shows displaying database routes.

```
#show ip route database
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
       > - selected route, * - FIB route, p - stale info

K    *> 0.0.0.0/0 via 10.30.0.11, eth0
O    *> 9.9.9.9/32 [110/31] via 10.10.31.16, eth2, 00:19:21
K    *> 10.10.0.0/24 via 10.30.0.11, eth0
O    10.10.31.0/24 [110/1] is directly connected, eth2, 00:28:20
C    *> 10.10.31.0/24 is directly connected, eth2
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O    10.10.34.0/24 [110/31] via 10.10.31.16, eth2, 00:21:19
O    *> 10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:21:19
K    * 10.30.0.0/24 is directly connected, eth0
C    *> 10.30.0.0/24 is directly connected, eth0
S    *> 11.22.11.0/24 [1/0] via 10.10.31.16, eth2
O E2 *> 14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:19:21
O    16.16.16.16/32 [110/11] via 10.10.31.16, eth2, 00:21:19
S    *> 16.16.16.16/32 [1/0] via 10.10.31.16, eth2
O    *> 17.17.17.17/32 [110/31] via 10.10.31.16, eth2, 00:21:19
C    *> 45.45.45.45/32 is directly connected, lo
O    *> 55.55.55.55/32 [110/21] via 10.10.31.16, eth2, 00:21:19
K    * 127.0.0.0/8 is directly connected, lo
C    *> 127.0.0.0/8 is directly connected, lo
```

The codes and modifier at the start of each route entry are explained in [Table 15-50](#).

Routes in the FIB are marked with a \*. When multiple routes are available for the same prefix, the best route is indicated with the > symbol. Unselected routes have neither the \* nor the > symbol.

## Route Database Entry Examples

This example shows 2 entries in the route database; one learned from the kernel and the other derived from interface information.

```
K    * 10.30.0.0/24 is directly connected, eth0
C    *> 10.30.0.0/24 is directly connected, eth0
```

- Both these routes are in the same network 10.30.0.0/24.
- The first route has originated from the kernel. The \* indicates that it has been added to the FIB.
- The second route is derived from the IP address of local interface eth0. It is marked as a connected route. Since a connected route has the lowest administrative distance, it is the selected route.

```
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O    10.10.34.0/24 [110/31] via 10.10.31.16, eth2, 00:21:19
```

- The same prefix was learned from OSPF and from static route configuration.
- Static routes are preferred over OSPF routes, so the static route is selected and installed in the FIB.

Note: If the static route becomes unavailable, OcNOS automatically selects the OSPF route and installs it in the FIB.

## Example: Display VRF Routes

The following is the output with the `vrf` parameter:

```
#show ip route vrf vrf31
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 "vrf31"
O      2.2.2.2/32 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
O      10.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
O      20.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
C      21.1.1.0/24 is directly connected, vlan1.4, 00:02:54
C      31.31.1.1/32 is directly connected, lo.vrf31, 00:03:02
O      40.40.1.1/32 [110/3] via 21.1.1.2, vlan1.4, 00:00:43
C      127.0.0.0/8 is directly connected, lo.vrf31, 00:03:05

Gateway of last resort is not set
```

The following is the output with the `vrf database` parameter:

```
#show ip route vrf vrf31 database
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
> - selected route, * - FIB route, p - stale info
```

IP Route Table for VRF "vrf31"

```
O    *> 2.2.2.2/32 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
O    *> 10.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
O    *> 20.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
C    *> 21.1.1.0/24 is directly connected, vlan1.4, 00:02:57
O    21.1.1.0/24 [110/1] is directly connected, vlan1.4, 00:02:57
C    *> 31.31.1.1/32 is directly connected, lo.vrf31, 00:03:05
O    31.31.1.1/32 [110/1] is directly connected, lo.vrf31, 00:03:00
O    *> 40.40.1.1/32 [110/3] via 21.1.1.2, vlan1.4, 00:00:46
B    > 50.1.1.0/24 [200/0] via 41.41.41.41, 00:00:18
C    *> 127.0.0.0/8 is directly connected, lo.vrf31, 00:03:08
```

Gateway of last resort is not set

---

## show ip vrf

This command displays routing information about VRFs.

### Command Syntax

```
show ip vrf
show ip vrf WORD
```

### Parameter

WORD                      Virtual Routing and Forwarding name.

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show ip forwarding
vrf (management) :IP forwarding is on
vrf (default) :IP forwarding is on
```

---

## show ipv6 forwarding

Use this command to display the IPv6 forwarding status.

### Command Syntax

```
show ipv6 forwarding
```

### Parameters

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

The following is a sample output of the `show ipv6 forwarding` command displaying the IPv6 forwarding status.

```
#show ipv6 forwarding
vrf (management) :IPv6 forwarding is on
vrf (default) :IPv6 forwarding is on#
```



---

## show ipv6 interface brief

Use this command to display information about interfaces. To display information about a specific interface, include the interface name.

### Command Syntax

```
show ipv6 interface brief
show ipv6 interface IFNAME brief
```

### Parameters

IFNAME                      Name of the interface.

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show ipv6 interface brief
Interface                IPv6-Address                Admin-Status
lo                        ::1                          [up/up]

gre0                      unassigned                  [admin down/down]

eth3                      3ffe:abcd:104::1            [up/up]
                        3ffe:abcd:103::1
                        fe80::2e0:29ff:fe6f:cf0

eth1                      fe80::260:97ff:fe20:f257    [up/up]

eth2                      unassigned                  [admin down/down]

eth3                      unassigned                  [admin down/down]

sit0                      unassigned                  [admin down/down]

tun24                     unassigned                  [admin down/down]

tunl0                     unassigned                  [admin down/down]
```

[Table 15-52](#) explains the each interface brief entry.

**Table 15-52: show interface brief output details**

Field	Description
Interface	Name of the interface.
IPv6-Address	IPv6 address. An asterisk (“*”) means the address was assigned by the DHCPv6 client.
Admin-Status	Status of the interface:  The first part of the field indicates if the interface is up. The second part indicates if the interface is running.

## show ipv6 route

Use this command to display the IP routing table for a protocol or from a particular table, including database entries known by NSM. When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. The best routes in the FIB can be viewed using `show ipv6 route`.

### Command Syntax

```
show ipv6 route vrf WORD (database|)
show ipv6 route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)
show ipv6 route (database)
show ipv6 route (database) (bgp|connected|isis|kernel|ospf|rip|static)
show ipv6 route X:X::X:X
show ipv6 route X:X::X:X/M
show ipv6 route summary
```

### Parameters

X:X::X:X	Network in the IP routing table.
X:X::X:X/M	Prefix <network>/<length>, e.g., 35.0.0.0/8
all	All IPv6 routes
bgp	Border Gateway Protocol.
connected	Connected.
database	IPv6 routing table database.
isis	IS-IS.
IFNAME	Interface name
kernel	Kernel.
ospf	Open Shortest Path First.
rip	Routing Information Protocol.
static	Static routes.
summary	Summarize all routes
WORD	Routes from a Virtual Routing and Forwarding instance

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

See [Table 15-50](#) and [Table 15-51](#) for an explanation of the codes and fields in the output.

```
#show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng, O - OSPFv3,
```

```
      I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info.  
C> * ::1/128 is directly connected, lo  
C> * 3ffe:1::/48 is directly connected, eth1  
C> * 3ffe:2:2::/48 is directly connected, eth2  
#
```

---

## show ipv6 prefix-list

Use this command to display the prefix list entries for IPv6 interfaces.

### Syntax Description

```
show ipv6 prefix-list
show ipv6 prefix-list WORD
show ipv6 prefix-list WORD seq <1-4294967295>
show ipv6 prefix-list WORD X:X::X:X/M
show ipv6 prefix-list WORD X:X::X:X/M longer
show ipv6 prefix-list WORD X:X::X:X/M first-match
show ipv6 prefix-list summary
show ipv6 prefix-list summary WORD
show ipv6 prefix-list detail
show ipv6 prefix-list detail WORD
```

### Parameters

WORD	Name of prefix list.
X:X::X:X/M	IP prefix <network>/<length> (for example, 35.0.0.0/8).
first-match	First matched prefix.
longer	Look up longer prefix.
<1-4294967295>	Sequence number of an entry.
detail	Detail of prefix lists.
summary	Summary of prefix lists.

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

The following is a sample output of the `show ip prefix-list` command showing prefix-list entries.

```
#show ip prefix-list
ip prefix-list myPrefixList: 3 entries
  seq      5 permit 172.1.1.0/16
  seq     10 permit 173.1.1.0/16
  seq     15 permit 174.1.1.0/16
```

# show hosts

Use this command to display the IP domain-name, lookup style and any name server.

## Command Syntax

```
show hosts
```

## Parameters

None

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#show hosts

VRF: management

DNS lookup is enabled
Default domain      : .com
Additional Domain   : .in .ac
Name Servers        : 10.12.3.23

Host                                     Address
----                                     -
test                                    10.12.12.67
test                                    10::23

* - Values assigned by DHCP Client.
```

[Table 15-53](#) explains the output fields.

Table 15-53: show hosts fields

Entry	Description
VRF: management	DNS configuration of specified VRF
DNS lookup is enabled	DNS feature enabled or disabled
Default domain	Default domain name used to complete unqualified host names (names without a dotted decimal domain name).
Additional Domain	A list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.
Name Servers	DNS server addresses that are used to translate hostnames to IP addresses.

**Table 15-53: show hosts fields**

Entry	Description
Host      Address test    10.12.12.67 test    10::23	Static hostname-to-address mappings in DNS.
* - Values assigned by DHCP Client.	* in name-server indicates it has been learned dynamically.

---

## show running-config interface

Use this command to show the running system status and configuration for a specified interface, or a specified interface for a specified protocol.

### Command Syntax

```
show running-config interface IFNAME
show running-config interface IFNAME bridge
show running-config interface IFNAME ip igmp
show running-config interface IFNAME ip multicast
show running-config interface IFNAME ip pim
show running-config interface IFNAME ipv6 ospf
show running-config interface IFNAME ipv6 rip
show running-config interface IFNAME ipv6 pim
show running-config interface IFNAME isis
show running-config interface IFNAME lacp
show running-config interface IFNAME ldp
show running-config interface IFNAME mpls
show running-config interface IFNAME mstp
show running-config interface IFNAME ospf
show running-config interface IFNAME ptp
show running-config interface IFNAME rip
show running-config interface IFNAME rstp
show running-config interface IFNAME rsvp
show running-config interface IFNAME stp
show running-config interface IFNAME synce
```

### Parameters

bridge	Bridge.
ip	IPv4 (see also <a href="#">show running-config interface ip</a> ).
ipv6	IPv6 (see also <a href="#">show running-config interface ipv6</a> ).
isis	Intermediate System to Intermediate System.
lacp	Link Aggregation Control Protocol.
ldp	Label Distribution Protocol.
mpls	Multi-Protocol Label Switching.
mstp	Multiple Spanning Tree Protocol.
ospf	Open Shortest Path First.
ptp	Precision Time Protocol.
rip	Routing Information Protocol.



rstp	Rapid Spanning Tree Protocol.
rsvp	Resource Reservation Protocol.
stp	Spanning Tree Protocol.
synce	Synchronous Ethernet.

## Command Mode

Privileged Exec mode and Config Mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#show running-config interface eth1 bridge
!
interface eth1
  switchport
  bridge-group 1
  switchport mode access
  user-priority 3
  traffic-class-table user-priority 2 num-traffic-classes 3 value 3 traffic-
class-table user-priority 7 num-traffic-classes 1 value 2 traffic-class-table
user-priority 7 num-traffic-classes 2 value 0 traffic-class-table user-
priority 7 num-traffic-classes 3 value 0 traffic-class-table user-priority 7
num-traffic-classes 4 value 0 traffic-class-table user-priority 7 num-traffic-
classes 5 value 0 traffic-class-table user-priority 7 num-traffic-classes 6
```

---

## show running-config interface ip

Use this command to show the running system status and configuration for a specified IP.

### Command Syntax

```
show running-config interface IFNAME ip (igmp|multicast|pim|)
```

### Parameters

IFNAME	Interface name.
igmp	Internet Group Management Protocol.
multicast	Multicast.
pim	Protocol Independent Multicast.

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show running-config interface eth1 ip igmp
!
interface eth1
 switchport
```

---

## show running-config interface ipv6

Use this command to show the running system status and configuration for a specified IPv6 protocol.

### Command Syntax

```
show running-config interface IFNAME ipv6 (mld|multicast|ospf|pim|rip|)
```

### Parameters

IFNAME	Interface name.
mld	Multicast Listener Discovery
multicast	Multicast
ospf	Open Shortest Path First
pim	Protocol Independent Multicast
rip	Routing Information Protocol

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show running-config interface eth1 ipv6 rip
!
interface eth1
  switchport
```

---

## show running-config ip

Use this command to show the running system of IP configurations.

### Command Syntax

```
show running-config ip (dhcp|mroute|route)
```

### Parameters

dhcp	Dynamic Host Configuration Protocol.
mroute	Static IP multicast route.
route	Static IP route.

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
>enable
#show running-config ip route
!
ip route 3.3.3.3/32 eth3
ip route 3.3.3.3/32 eth2
ip route 200.0.0.0/16 lo
!
```

---

## show running-config ipv6

Use this command to show the running system status and configuration for IPv6.

### Command Syntax

```
show running-config ipv6 (access-list|mroute|neighbor|prefix-list|route|)
```

### Parameters

access-list	Access list.
mroute	Static IPv6 Multicast route.
neighbor	Static IPv6 neighbor entry.
prefix-list	IPv6 prefix-list.
route	Static IPv6 route.

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
>enable
#show running-config ipv6 access-list
!
ipv6 access-list abc permit any
!
#show running-config ipv6 prefix-list
!
ipv6 prefix-list sde
seq 5 permit any
!
#show running-config ipv6 route
!
ipv6 route 3e11::/64 lo
ipv6 route 3e11::/64 eth2
ipv6 route fe80::/64 eth2
!
```

---

## show running-config prefix-list

Use this command to display the running system status and configuration details for prefix lists.

### Command Syntax

```
show running-config prefix-list
```

### Parameters

None

### Command Mode

Privileged exec mode, configure mode, router-map mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
>enable
(config)#show running-config prefix-list
!
ip prefix-list abc
 seq 5 permit any
!
ip prefix-list as
 description annai
!
ip prefix-list wer
 seq 45 permit any
!
(config)#
```

---

## shutdown

Use this command to shut down an interface.

Use the `no` form of this command to bring up an interface.

### Command Syntax

```
shutdown
no shutdown
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

The following example shows the use of the `shutdown` command to shut down the interface called `eth3`.

```
#configure terminal
(config)#interface eth3
(config-if)#shutdown
```

## speed

Use this command to set the link speed of the interface.

Use the `no` parameter to set the speed to its default value.

On copper ports, auto-negotiation is enabled by default and force speed is not supported.

On fiber optic ports, auto-negotiation is disabled by default. Auto-negotiation is not supported on fiber optic medium/AOC for speeds 10g and beyond. IP Infusion Inc. does not recommend using auto speed on such transceivers. On DAC cables, both force and auto-negotiation are supported.

IP Infusion Inc. recommends configuring the same speed mode on both peers.

When an interface is configured with the speed auto option, the negotiated parameters are speed, [duplex](#), [flowcontrol](#), and [fec](#), each of which is configured separately. Please see the respective command for details.

Note: For 10g DAC/AOC, setting speed auto negotiates with a maximum of 1G.

Note: Interface speed setting is only supported on physical front-panel ports and not supported on Management interface `eth0`.

[Table 15-54](#) shows the IP Infusion Inc. recommendations regarding front-panel port speed and transceivers.

**Table 15-54: Recommendations**

Supported/ Recommended	Explanation
Not Supported	When front panel port capability is less than the transceiver's capability the behavior is undefined.
Not Recommended	When the transceiver's capability and front panel port capability is the same, reducing the speed is not recommended.
Recommended	When the transceiver's capability is less than the front panel port capability, the behavior is undefined and the link might even come up. So speed needs to be set to match the transceiver's capability.

[Table 15-55](#) show examples with front-panel configurations:

**Table 15-55: Front-panel configurations**

Front Panel Port	Explanation
Front Panel Port 100g	When 40g transceivers are used, make sure to use the command <code>speed 40g</code> . IP Infusion Inc. does not recommend using 40g on 100g speed transceivers.
Front Panel Port 40g	100g transceivers should not be used.
Front Panel Port 25g	<p>When 10g transceivers are used, make sure to use the <code>port-group</code> command to reduce the speed to 10g. IP Infusion Inc. does not recommend to use 10g on 25g speed transceivers. When using 1g transceivers, make sure to set the speed to 1g.</p> <p>Below 25g, port-speed can defer (10g or 1g) for ports under same port-group i.e. 1 port can have 1g &amp; remaining 10g but 1 port 25g &amp; remaining 10g not allowed. When "<code>no speed</code>" command is used at interface level it tries to set speed "25g" to one of the port of port-group while other may be at 10g or 1g speed which is not allowed. Use "<code>no port-group</code>" command in such case.</p>



**Table 15-55: Front-panel configurations (Continued)**

Front Panel Port	Explanation
Front Panel Port 10g	25g transceivers should not be used. When using 1g transceivers, make sure to set the speed to 1g.
Front Panel Port 1g	10g/25g transceivers should not be used.

**Command Syntax**

```
speed (10m | 100m | 1g | 2.5g | 10g | 20g | 25g | 40g | 50g | 100g | auto )
no speed
```

**Parameter**

10m	10 megabits
100m	100 megabits
1g	1 gigabit
2.5g	2.5 gigabits
10g	10 gigabits
20g	20 gigabits
25g	25 gigabits
40g	40 gigabits
50g	50 gigabits
100g	100 gigabits
auto	Negotiate the speed with a connected port

**Default**

No default value is specified

**Command Mode**

Interface mode

**Applicability**

This command was introduced before OcNOS version 1.3.

**Example**

Enable auto-negotiation:

```
#configure terminal
(config)#interface xe0
(config-if)#speed auto
```

---

## 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.

User should be prompted for confirmation, while executing `switchport/no switchport` command. To support this requirement, please refer the command `enable/disable confirmation-dialog`.

Use the `no` form of this command to set the mode to routed.

### Command Syntax

```
switchport
no switchport
```

### Parameters

None

### Default

No default value is specified

### 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

#configure terminal
(config)#enable confirmation-dialog
(config)#interface xe5
(config-if)#switchport
Are you sure? (y/n): y
(config-if)#
(config-if)#exit

(config)#disable confirmation-dialog
(config)#
(config)#interface xe5
(config-if)#switchport
(config-if)#
```

---

## switchport allowed ethertype

Use this command to indicate which types of traffic will be allowed on the switchport.

Note: A maximum of 5 Ethertype values can be assigned on an interface.

### Command Syntax

```
switchport allowed ethertype {arp|ipv4|ipv6|mpls|ETHERTYPE|log}
```

### Parameters

arp	ARP traffic
ipv4	IPv4 traffic
ipv6	IPv6 traffic
mpls	MPLS traffic
ETHERTYPE	Traffic of any Ethertype value (0x600 - 0xFFFF).
log	Log unwanted ethertype packets.

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

### Example

```
(config)#interface xe32/1

(config-if)#switchport
(config-if)#switchport allowed ethertype ipv4
(config-if)#switchport allowed ethertype 0x800
```

---

## switchport protected

Use this command to enable or disable the protected port feature on an interface.

### Command Syntax

```
switchport protected (community | isolated | promiscuous)
no switchport protected
```

### Parameter

community	Community mode
isolated	Isolated mode type
promiscuous	Protected mode type

### Default

Promiscuous

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport protected isolated
(config-if)#no switchport protected

(config)#interface po1
(config-if)#switchport protected promiscuous
(config-if)#no switchport protected
```

## transceiver

Use this command to set the type of Small Form-factor Pluggable (SFP) transceiver inserted in the physical port.

Use the `no` form of this command to remove the setting.

### Command Syntax

```
transceiver (1000base-sx|1000base-lx|1000base-ex|1000base-cx|10gbase-sr|10gbase-
lr|10gbase-er|10gbase-cr|25gbase-sr|25gbase-lr|25gbase-er|25gbase-cr|40gbase-
sr4|40gbase-lr4|40gbase-er4|40gbase-cr4|100gbase-sr4|100gbase-lr4|100gbase-
er4|100gbase-cr4)
no transceiver
```

### Parameters

1000base-cx	SFP 1000base-cx
1000base-ex	SFP 1000base-ex
1000base-lx	SFP 1000base-lx
1000base-sx	SFP 1000base-sx
100gbase-cr4	QSFP28 100gbase-cr4
100gbase-er4	QSFP28 100gbase-er4
100gbase-lr4	QSFP28 100gbase-lr4
100gbase-sr4	QSFP28 100gbase-sr4
10gbase-cr	SFP+ 10gbase-cr
10gbase-er	SFP+ 10gbase-er
10gbase-lr	SFP+ 10gbase-lr
10gbase-sr	SFP+ 10gbase-sr
25gbase-cr	SFP+ 25gbase-cr
25gbase-ers	SFP+ 25gbase-er
25gbase-lr	SFP+ 25gbase-lr
25gbase-sr	SFP+ 25gbase-sr
40gbase-cr4	QSFP 40gbase-cr4
40gbase-er4	QSFP 40gbase-er4
40gbase-lr4	QSFP 40gbase-lr4
40gbase-sr4	QSFP 40gbase-sr4

### Default

No default value is specified

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
(config)#interface ce1/1
(config-if)#transceiver 40gbase-lr4
```

## CHAPTER 16 IP Service Level Agreements Commands

---

IP Service Level Agreements (SLAs) is a diagnostic method which generates and analyses the traffic between an OcNOS device and your network. IP SLA monitors and reports network performance data which helps you to identify the actual root cause of a problem when the performance level drops.

This chapter describes the commands used to manage the IP SLA for ICMP echo.

- [clear ip sla statistics](#)
- [frequency](#)
- [icmp-echo](#)
- [ip sla](#)
- [ip sla schedule](#)
- [show ip sla statistics](#)
- [show ip sla summary](#)
- [show running-config ip sla](#)
- [threshold](#)
- [timeout](#)

---

## clear ip sla statistics

Use this command to clear the IP SLA statistics.

### Command Syntax

```
clear ip sla statistics <1-65535>
```

### Parameters

1-65535	IP SLA identifier
---------	-------------------

### Default

N/A

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#clear ip sla statistics 1
```



---

## frequency

Use this command to configure the frequency/interval to send ICMP echo packets one by one.

Use the `no` form of this command to remove the configured ICMP echo frequency.

### Command Syntax

```
frequency <1-60>
no frequency
```

### Parameters

1-60	Frequency in seconds
------	----------------------

### Default

5 seconds

### Command Mode

IP SLA ICMP Echo mode (config-ip-sla-echo)

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#frequency 3
```

---

## icmp-echo

Use this command to select and configure the ICMP echo SLA operation. ICMP echo packets are constructed in the device and sent to the destination address that you specify. These packets are transferred on a specific interface by setting the `source-interface` parameter.

Use the `no` form of this command to un-configure or remove the configured ICMP echo measurement sessions.

### Command Syntax

```
icmp-echo (ipv4 A.B.C.D|ipv6 X:X::X:X|HOSTNAME) (source-interface IFNAME|)
no icmp-echo (ipv4 A.B.C.D | ipv6 X:X::X:X | HOSTNAME)
```

### Parameters

A.B.C.D	IPv4 address
X:X::X:X	IPv6 address
HOSTNAME	Host name
IFNAME	Source interface name

### Default

N/A

### Command Mode

IP SLA mode (`config-ip-sla`)

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#
```

---

## ip sla

Use this command to create an IP SLA instance. One instance maps to a single SLA operation. You can create multiple SLA operations to perform multiple similar or different SLA operations.

Use the `no` form of this command to remove a configured IP SLA configurations.

### Command Syntax

```
ip sla <1-65535>
no ip sla <1-65535>
```

### Parameters

1-65535	IP SLA identifier
---------	-------------------

### Default

N/A

### Command Mode

Configuration mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#
```

---

## ip sla schedule

Use this command to schedule an IP SLA operation by associating a [time-range](#) object with the IP SLA operation.

Use the `no` form of this command to stop the configured IP SLA measurement.

### Command Syntax

```
ip sla schedule <1-65535> time-range WORD (vrf (NAME) |)
```

### Parameters

<code>&lt;1-65535&gt;</code>	IP SLA identifier.
<code>time-range</code>	Time Range
<code>TR_NAME</code>	Time range name that you set with the <a href="#">time-range</a> command.
<code>vrf</code>	VPN Routing/Forwarding instance
<code>NAME</code>	VPN Routing/Forwarding instance name. Maximum limit 32 characters

### Default

N/A

### Command Mode

Configuration mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#configure terminal
(config)#ip sla schedule 1 time-range t1 vrf v1
```

## show ip sla statistics

Use this command to display the statistics of IP SLA measurement.

### Command Syntax

```
show ip sla statistics (1-65535) detail
```

### Parameters

1-65535                      IP SLA identifier.

### Default

N/A

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#show ip sla statistics 1 detail
=====
                IP SLA Statistics
=====
IP SLA ID           : 1
Start Time           : 2021 Aug 30 17:40:04
Elapsed time(milli sec) : 46015
Packets Sent         : 23
Packets Received     : 23
Packet Loss(%)       : 0.0000
Invalid Tests        : 0
Round Trip Delay(usec)
  Minimum            : 1000
  Maximum            : 1000
  Average            : 1000
```

[Table 16-56](#) explains the output fields.

**Table 16-56: show ip sla statistics fields**

Field	Description
IP SLA ID	IP SLA Identifier (1-65535)
Start Time	Measurement start time
Elapsed time(milli sec)	Time taken to complete the measurement in milliseconds
Packets Sent	Number of packet sent

**Table 16-56: show ip sla statistics fields (Continued)**

Field	Description
Packets Received	Number of packet received
Packet Loss(%)	Packet lost in percentage
Invalid Tests	Received ICMP echo reply packets after configured threshold limit will be marked as invalid tests
Round Trip Delay(usec)	Round trip delay between ICMP echo request and ICMP echo reply: minimum, maximum and average round trip delay in microseconds

---

## show ip sla summary

Use this command to display the summary of all IP SLA measurements.

### Command Syntax

```
show ip sla summary
```

### Parameters

None

### Default

N/A

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive
```

ID	Type	Destination	Stats (usec)	Return Code	Last Run
-----					
^1	icmp-echo	20.2.2.3	0	OK	2021 Aug 23 13:53:37

[Table 16-57](#) explains the output fields.

**Table 16-57: show ip sla summary fields**

Field	Description
ID	IP SLA Identifier (1-65535)
Type	Measurement type
Destination	Destination address
Stats (usec)	Round trip time in microseconds for the measurement
Return Code	Measurement status
Last Run	Measurement last run date and time

---

## show running-config ip sla

Use this command to display the IP SLA running configuration alone.

### Command Syntax

```
show running-config ip sla
```

### Parameters

None

### Default

N/A

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#show running-config ip sla
ip sla 1
  icmp-echo ipv4 20.2.2.3
  frequency 2
  threshold 2000
  timeout 5000
ip sla schedule 1 time-range t1 vrf v1
```



---

## threshold

Use this command to configure the threshold for every ICMP echo packet.

Use the `no` form of this command to remove the configured ICMP echo threshold.

### Command Syntax

```
threshold <1000-60000>
no threshold
```

### Parameters

1000-60000      Threshold in milliseconds.

### Default

10000 milliseconds

### Command Mode

IP SLA ICMP Echo mode (config-ip-sla-echo)

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#threshold 5000
```

---

## timeout

Use this command to configure the timeout for every ICMP echo packet. Any packet arriving beyond this interval is considered to be lost.

Use the `no` form of this command to remove the configured ICMP echo timeout.

### Command Syntax

```
timeout <1000-60000>
no timeout
```

### Parameters

1000-60000	Timeout in milliseconds.
------------	--------------------------

### Default

10000 milliseconds

### Command Mode

IP SLA ICMP Echo mode (config-ip-sla-echo)

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#timeout 5000
```

---

## CHAPTER 17 Linux Shell Commands

---

This chapter is a reference for Linux shell commands that you can run at the OcNOS prompt.

Table 17-58 describes the commands. Note the following:

- You must be in privileged exec mode to run these commands.
- You cannot use the pipe ("|") or redirect (">") operators.

**Table 17-58: Linux shell commands**

Command	Description
<code>cat <i>file</i></code>	Display contents of <i>file</i>
<code>cd</code>	Change to home directory
<code>cd <i>dir</i></code>	Change directory to <i>dir</i>
<code>cp <i>file1 file2</i></code>	Copy <i>file1</i> to <i>file2</i>
<code>cp -r <i>dir1 dir2</i></code>	Copy <i>dir1</i> to <i>dir2</i> ; create <i>dir2</i> if it does not exist
<code>dir</code>	Display contents of current directory
<code>less <i>file</i></code>	Display the contents of <i>file</i>
<code>ls <i>options</i></code>	Display contents of current directory
<code>mkdir <i>dir</i></code>	Create a directory <i>dir</i>
<code>more <i>file</i></code>	Display the contents of <i>file</i>
<code>mv <i>file1 file2</i></code>	Rename <i>file1</i> to <i>file2</i>
<code>mv <i>file dir</i></code>	Move <i>file</i> to directory <i>dir</i>
<code>pwd</code>	Display current directory
<code>rmdir <i>dir</i></code>	Remove a directory <i>dir</i> (only if empty)



---

## CHAPTER 18 Network Time Protocol

---

This chapter is a reference for Network Time Protocol (NTP) commands.

NTP synchronizes clocks between computer systems over packet-switched networks. NTP can synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).

NTP uses a hierarchical, layered system of time sources. Each level of this hierarchy is called a “stratum” and is assigned a number starting with zero at the top. The number represents the distance from the reference clock and is used to prevent cyclical dependencies in the hierarchy.

Note: The default time-to-live value for the unicast packets is 64.

This chapter contains these commands:

- [clear ntp statistics](#)
- [debug ntp](#)
- [feature ntp](#)
- [ntp acl](#)
- [ntp authenticate](#)
- [ntp authentication-key](#)
- [ntp discard](#)
- [ntp enable](#)
- [ntp logging](#)
- [ntp master](#)
- [ntp master stratum](#)
- [ntp peer](#)
- [ntp request-key](#)
- [ntp server](#)
- [ntp source-interface](#)
- [ntp sync-retry](#)
- [ntp trusted-key](#)
- [show ntp authentication-keys](#)
- [show ntp authentication-status](#)
- [show ntp logging-status](#)
- [show ntp peer-status](#)
- [show ntp peers](#)
- [show ntp statistics](#)
- [show ntp trusted-keys](#)
- [show running-config ntp](#)

---

## clear ntp statistics

Use this command to reset NTP statistics.

### Command Syntax

```
clear ntp statistics (all-peers | io | local | memory)
```

### Parameters

all-peers	Counters associated with all peers
io	Counters maintained in the input-output module
local	Counters maintained in the local protocol module
memory	Counters related to memory allocation

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear ntp statistics all-peers
```

---

## debug ntp

Use this command to display NTP debugging messages.

Use the `no` form of this command to stop displaying NTP debugging messages.

### Command Syntax

```
debug ntp
no debug ntp
```

### Parameters

None

### Command Mode

Exec mode and Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#debug ntp

(config)#no debug ntp
```

---

## feature ntp

Use this command to enable to NTP feature.

Use the `no` form of this command to disable NTP feature and delete all the NTP related configurations.

### Command Syntax

```
feature ntp (vrf management|)
no feature ntp (vrf management|)
```

### Parameters

management	Virtual Routing and Forwarding name
------------	-------------------------------------

### Default

By default, feature ntp is enabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#feature ntp vrf management

(config)#no feature ntp vrf management
```



## ntp acl

Use this command to allow particular client to communicate with NTP server.

Use the `no` form of this command to remove the particular client from NTP server.

Note: `ntp discard` option and limited rate flag are required for sending the KOD packet.

### Command Syntax

```
ntp allow (A.B.C.D | X:X::X:X) (mask (A.B.C.D | <1-128>))
({nopeer|noserve|noquery|nomodify|kod|limited|notrap|}) (vrf management|)
no ntp allow (A.B.C.D | X:X::X:X) (mask (A.B.C.D | <1-128>))
({nopeer|noserve|noquery|nomodify|kod|limited|notrap|}) (vrf management|)
```

### Parameters

A.B.C.D	IPv4 address of the client
X:X::X:X	IPv6 address of the client
A.B.C.D	Mask for the IPv4 address
1-128	Mask for the IPv6 address
nopeer	Prevent the client from establishing a peer association
noserve	Prevent the client from performing time queries
noquery	Prevent the client from performing NTPq and NTPdc queries, but not time queries
nomodify	Restrict the client from making any changes to the NTP configurations
kod	Send a kiss-of-death packet if the client limit has exceeded
limited	Deny time service if the packet violates the rate limits established by the discard command
notrap	Prevent the client from configuring control message traps
vrf	Virtual Router and Forwarding
management	Virtual Routing and Forwarding name

### Default

By default, only local host is permitted.

### Command Mode

Configure mode

### Applicability

This command is introduced in OcNOS version 4.2.

### Example

```
#configure terminal
(config)#ntp allow 1.1.1.1 mask 255.255.255.0 nopeer kod notrap noserve vrf
management
```

---

## ntp authenticate

Use this command to enable NTP authentication.

Use the `no` form of this command to disable authentication.

### Command Syntax

```
ntp authenticate (vrf management|)
no ntp authenticate (vrf management|)
```

### Parameters

<code>management</code>	Virtual Routing and Forwarding name
-------------------------	-------------------------------------

### Default

By default, `ntp authenticate` is disabled

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#ntp authenticate vrf management
```

---

## ntp authentication-key

Use this command to set an NTP Message Digest Algorithm 5 (MD5) authentication key.

Use the `no` form of this command to delete an authentication key.

### Command Syntax

```
ntp authentication-key <1-65535> md5 WORD (vrf management|)
ntp authentication-key <1-65535> md5 WORD 7 (vrf management|)
no ntp authentication-key <1-65535> md5 WORD (vrf management|)
```

### Parameters

<1-65535>	Authentication key
WORD	MD5 string (maximum 8 characters)
7	Encrypt using weak algorithm
management	Virtual Routing and Forwarding name

### Default

The default authentication key is 65535.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#ntp authentication-key 535 md5 J@u-b;l2 vrf management
```

---

## ntp discard

Use this command to enable rate limiting access to the NTP service running on a system.

Use the no form of this command to disable rate limiting access to the NTP service running on a system.

This NTP discard option and limited rate flag are required for sending the KOD packet. KOD (Kiss of Death) packets have the leap bits set unsynchronized and stratum set to zero and the reference identifier field set to a four-byte ASCII code. If the noserve or notrust flag of the matching restrict list entry is set, the code is "DENY"; if the limited flag is set and the rate limit is exceeded, the code is "RATE".

### Command Syntax

```
ntp discard minimum <1-65535> (vrf management|)
no ntp discard minimum (vrf management|)
```

### Parameters

minimum	Specify the minimum interpacket spacing <default 2>
<0-65535>	Minimum value

### Default

By default, the minimum value is 2.

### Command Mode

Configure mode

### Applicability

This command is introduced in OcNOS version 4.2.

### Example

```
#configure terminal
(config)#ntp discard minimum 50 vrf management
```

---

## ntp enable

Use this command to enable NTP feature and start the NTP service.

Use the `no` form of this command to stop the NTP service.

### Command Syntax

```
ntp enable (vrf management|)
no ntp enable (vrf management|)
```

### Parameters

management	Virtual Routing and Forwarding name
------------	-------------------------------------

### Default

By default, ntp is enabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#ntp enable vrf management
```

---

## ntp logging

Use this command to log NTP events.

Use the `no` form of this command to disable NTP logging.

### Command Syntax

```
ntp logging (vrf management|)
no ntp logging (vrf management|)
```

### Parameters

management	Virtual Routing and Forwarding name
------------	-------------------------------------

### Default

By default, ntp logging message is disabled

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#ntp logging vrf management
```

---

## ntp master

Use this command to run OcNOS device as NTP server.

Use the `no` command to disable NTP server.

### Command Syntax

```
ntp master (vrf management|)
no ntp master (vrf management|)
```

### Parameters

vrf	Virtual Router and Forwarding
management	Virtual Routing and Forwarding name

### Default

By default, NTP master is disabled

### Command Mode

Configure mode

### Applicability

This command is introduced in OcNOS version 4.2.

### Example

```
#configure terminal
(config)#ntp master vrf management
```

---

## ntp master stratum

Use this command to set stratum value for NTP server.

Use the `no` command to remove stratum value.

The NTP Stratum model is a representation of the hierarchy of time servers in an NTP network, where the Stratum level (0-15) indicates the device's distance to the reference clock.

### Command Syntax

```
ntp master stratum <1-15> (vrf management|)
no ntp master stratum (vrf management|)
```

### Parameters

<1-15>	Stratum value for NTP server
vrf	Virtual Router and Forwarding
management	Virtual Routing and Forwarding name

### Default

By default, NTP startum value is 16.

### Command Mode

Configure mode

### Applicability

This command is introduced in OcNOS version 4.2.

### Example

```
#configure terminal
(config)#ntp master stratum 2 vrf management
```



## ntp peer

Use this command to configure a peer association. In a peer association, this system can synchronize with the other system or the other system can synchronize with this system.

Use the `no` command to remove a peer association.

### Command Syntax

```
ntp peer (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}) (vrf management|)

ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}) (vrf management|)

no ntp peer (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}) (vrf management|)

no ntp peer (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}) (vrf management|)

no ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}) (vrf management|)

no ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key|minpoll|maxpoll}) (vrf management|)
```

### Parameters

A.B.C.D	IPv4 address of peer
HOSTNAME	Host name of peer
X:X::X:X	IPv6 address of peer
prefer	Prefer this peer; preferred peer responses are discarded only if they vary dramatically from other time sources
key	Peer authentication key
<1-65534>	Peer authentication key value
minpoll	Minimum poll interval
<4-16>	Minimum poll interval value in seconds raised to a power of 2 (default 4 = 16 seconds)
maxpoll	Maximum poll interval
<4-16>	Maximum poll interval value in seconds raised to a power of 2 (default 6 = 64 seconds)
management	Virtual Routing and Forwarding name

### Default

By default, value of `minpoll` is 4 and `maxpoll` is 6.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#configure terminal
(config)#ntp peer 10.10.0.23 vrf management
(config)#ntp peer 10.10.0.23 prefer key 12345 vrf management

(config)#no ntp peer 10.10.0.23 vrf management
```

---

## ntp request-key

Use this command to define NTP request-key which is used by the NTPDC utility program. NTP client should be able to modify NTP server configuration by using this request-key. Request key must be a trusted key.

Use `no` form of this command to remove a request key.

### Command Syntax

```
ntp request-key <1-65534> (vrf management|)
no ntp request-key <1-65534> (vrf management|)
```

### Parameter

<1-65534>	Request key number
vrf management	Virtual Routing and Forwarding name

### Default

No default value

### Command Mode

Configure mode

### Applicability

This command is introduced in OcNOS version 5.1 MR.

### Example

```
#configure terminal
(config)#ntp request-key 123 vrf management
```

---

## ntp server

Use this command to configure an NTP server so that this system synchronizes with the server, but not vice versa.

Use the `no` option with this command to remove an NTP server.

### Command Syntax

```
ntp server (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}) (vrf management|)

ntp server (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}) (vrf management|)

no ntp server (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}) (vrf management|)

no ntp server (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}) (vrf management|)

no ntp server (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}) (vrf management|)

no ntp server (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}) (vrf management|)
```

### Parameters

A.B.C.D	IPv4 address of the server
HOSTNAME	Host name of the server
X:X::X:X	IPv6 address of the server
prefer	Prefer this server; preferred server responses are discarded only if they vary dramatically from other time sources
key	Server authentication key
<1-65534>	Server authentication key
minpoll	Minimum poll interval
<4-16>	Minimum poll interval value in seconds raised to a power of 2 (default 4 = 16 seconds)
maxpoll	Maximum poll interval
<4-16>	Maximum poll interval value in seconds raised to a power of 2 (default 6 = 64 seconds)
management	Virtual Routing and Forwarding name

### Default

By default, `minpoll` is 4 and `maxpoll` is 6.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

**Examples**

```
#configure terminal
(config)#ntp server 10.10.0.23 vrf management
(config)#ntp server 10.10.0.23 prefer key 12345 vrf management

(config)#no ntp server 10.10.0.23 vrf management
```

---

## ntp source-interface

Use this command to configure an NTP source-interface. NTP sets the source IP address for all NTP packets based on the address of the interface through which the NTP packet are sent.

Use the `no` option with this command to remove an NTP server.

### Command Syntax

```
ntp source-interface IFNAME
```

### Parameter

IFNAME	Interface name
--------	----------------

### Default

No default value is specified.

### Command Mode

Configure mode

### Applicability

This command was introduced in a version before OcNOS 1.3.

### Examples

```
#configure terminal
(config)#ntp source-interface xe7/1
(config)#no ntp source-interface xe7/1
```

---

## ntp sync-retry

Use this command to retry NTP synchronization with configured servers.

### Command Syntax

```
ntp sync-retry (vrf management|)
```

### Parameters

management	Virtual Routing and Forwarding name
------------	-------------------------------------

### Default

No default value is specified

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#ntp sync-retry vrf management
```

---

## ntp trusted-key

Use this command to define a “trusted” authentication key. If a key is trusted, the device will synchronize with a system that specifies this key in its NTP packets.

Use the `no` option with this command to remove a trusted key.

### Command Syntax

```
ntp trusted-key <1-65534> (vrf management|)
no ntp trusted-key <1-65534> (vrf management|)
```

### Parameter

<1-65534>	Authentication key number
management	Virtual Routing and Forwarding name

### Default

By default, `ntp trusted-key` is disabled

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#ntp trusted-key 234676 vrf management
```



---

# show ntp authentication-keys

Use this command to display authentication keys.

## Command Syntax

```
show ntp authentication-keys
```

## Parameters

None

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#show ntp authentication-keys
-----
Auth Key      MD5 String
-----
123           0xa2cb891442844220
```

[Table 18-59](#) explains the output fields.

**Table 18-59: show ntp authentication-key fields**

Entry	Description
Auth key	Authentication key (password). Use the password to verify the authenticity of packets sent from this interface or peer interface.
MD5 String	One or more MD5 key strings. The MD5 key values can be from 1 through 16 characters long. You can specify more than one key value within the list.

---

## show ntp authentication-status

Use this command to display whether authentication is enabled or disabled.

### Command Syntax

```
show ntp authentication-status
```

### Parameters

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show ntp authentication-status  
Authentication enabled
```

---

## show ntp logging-status

Use this command to display the NTP logging status.

### Command Syntax

```
show ntp logging-status
```

### Parameters

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show ntp logging-status  
NTP logging enabled
```

# show ntp peer-status

Use this command to display the peers for which the server is maintaining state along with a summary of that state.

## Command Syntax

```
show ntp peer-status
```

## Parameters

None

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#show ntp peer-status
Total peers : 1
* - selected for sync, + - peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
      remote      refid      st t when poll reach      delay      offset      jitter
=====
*216.239.35.4      .GOOG.      1 u  24   64  377   38.485      0.149      0.053
```

Table 18-60 explains the output fields.

Table 18-60: show ntp peer-status fields

Entry	Description
Total peers	Number of servers and peers configured.
* - selected for sync, + - peer mode (active), - - peer mode (passive), = - polled in client mode x - source false ticker	Fate of this peer in the clock selection process.
Remote	Address of the remote peer.
refid	Reference ID (0.0.0.0 for an unknown reference ID).
st	The stratum of the remote peer (a stratum of 16 indicated remote peer is unsynchronized).
t	Type of peer (local, unicast, multicast and broadcast).
when	Time the last packet was received.
poll	The polling interval (seconds).

Table 18-60: show ntp peer-status fields

Entry	Description
reach	The reachability register (octal).
delay	Current estimated delay in seconds.
offset	Current estimated offset in seconds.
jitter	Current dispersion of the peer in seconds.

# show ntp peers

Use this command to display NTP peers.

## Command Syntax

```
show ntp peers
```

## Parameters

None

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#show ntp peers

-----
Peer IP Address                               Serv/Peer
-----
216.239.35.4                                   Server (configured)
```

[Table 18-61](#) explains the output fields.

Table 18-61: show ntp peers fields

Entry	Description
Peer IP Address	Address of the neighbor protocol.
Serv/Peer	List of NTP peers and servers configured or dynamically learned.

## show ntp statistics

Use this command to display NTP statistics.

### Command Syntax

```
show ntp statistics (io | local | memory | peer ( ipaddr (A.B.C.D | X:X::X:X ) |
name (HOSTNAME)) )
```

### Parameters

io	Counters maintained in the input-output module
local	Counters maintained in the local protocol module
memory	Counters related to memory allocation
peer	Counters associated with the specified peer
A.B.C.D	Peer IPv4 address
X:X::X:X	Peer IPv6 address
HOSTNAME	Peer host name

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show ntp statistics local
time since restart:      1685
time since reset:       1685
packets received:       4
packets processed:      0
current version:        0
previous version:       0
declined:               0
access denied:          0
bad length or format:   0
bad authentication:     0
rate exceeded:          0
#show ntp statistics memory
time since reset:       1698
total peer memory:     15
free peer memory:      15
calls to findpeer:     0
new peer allocations:  0
peer demobilizations:  0
hash table counts:     0  0  0  0  0  0  0  0
                        0  0  0  0  0  0  0  0
                        0  0  0  0  0  0  0  0
                        0  0  0  0  0  0  0  0
                        0  0  0  0  0  0  0  0
                        0  0  0  0  0  0  0  0
```

Table 18-62 explains the output fields.

**Table 18-62: show ntp statisticsfields**

Entry	Description
Time since restart	Time when the ntp protocols were last started and how long they have been running.
Time since reset	Time when the ntp protocols were last reset and how long they have been running.
Packets received	Number of packets received from the peers.
Packets processed	Number of packets processed to the peers.
Current version	Current version of the protocol that is being used.
Previous version	Previous version of the protocol that has been used.
Declined	Access to the protocol declined
Access denied	Number of attempts denied to access protocol
Bad length or format	Number of messages received with length or format errors so severe that further classification could not occur.
Bad authentication	Number of messages received with incorrect authentication.
Rate exceeded	Exceed the configured rate if additional bandwidth is available from other queues
Total peer memory	Actual memory available to the peer system.
Free peer memory	Free memory available to the peer system.
Calls to find peer	Number of calls to find peer.
New peer allocations	Number of allocations from the free peer list.
Peer demobilizations	Number of structures freed to free peer list.
Hash table counts	Peer hash table's each bucket count.



---

# show ntp trusted-keys

Use this command to display keys that are valid for authentication.

## Command Syntax

```
show ntp trusted-keys
```

## Parameters

None

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#show ntp trusted-keys

Trusted Keys:
333
#
```

[Table 18-63](#) explains the output fields.

**Table 18-63: show ntp trusted-keys fields**

Entry	Description
Trusted Keys	Keys that are valid for authentication.

---

## show running-config ntp

Use this command to display the NTP running configuration.

### Command Syntax

```
show running-config ntp [|all]
```

### Parameters

all	Reserved for future use
-----	-------------------------

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show running-config ntp
feature ntp vrf management
ntp enable vrf management
ntp authenticate vrf management
ntp logging vrf management
ntp authentication-key 123 md5 0xa2cb891442844220 7 vrf management
ntp trusted-key 123 vrf management
ntp server 216.239.35.4 vrf management
```

---

## CHAPTER 19 RADIUS

---

This chapter is a reference for Remote Authentication Dial In User Service (RADIUS) commands. RADIUS provides centralized Authentication, Authorization management for users that connect to and use a network service. RADIUS is specified in RFC 2865.

Note: Only network administrators can execute these commands. For more, see the [username](#) command.

Note: The commands below are supported only on the “management” VRF.

- [clear radius-server](#)
- [debug radius](#)
- [radius-server login host](#)
- [radius-server login host acct-port](#)
- [radius-server login host auth-port](#)
- [radius-server login host key](#)
- [radius-server login key](#)
- [radius-server login timeout](#)
- [show debug radius](#)
- [show radius-server](#)
- [show running-config radius](#)

---

## clear radius-server

Use this command to clear radius-server statistics.

### Command Syntax

```
clear radius-server ((HOSTNAME | X:X::X:X | A.B.C.D)|) counters (vrf (management | all)|)
```

### Parameters

A.B.C.D	IPv4 address of RADIUS server
X:X::X:X	IPv6 address of RADIUS server
HOSTNAME	DNS host name of RADIUS server
vrf management	To clear radius server counters for Virtual Routing and Forwarding management
all	To clear radius server counters for both management and default vrf
counters	To clear radius server counters for default vrf

### Command Mode

Exec mode

### Applicability

This command is introduced in OcNOS version 1.3.7.

### Examples

```
#clear radius-server counters vrf management
```

---

## debug radius

Use this command to display RADIUS debugging information.

Use the `no` form of this command stop displaying RADIUS debugging information.

### Command Syntax

```
debug radius
no debug radius
```

### Parameters

None

### Command Mode

Executive mode and configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#debug radius
```

---

## radius-server login host

Use this command to configure a RADIUS server for both accounting and authentication.

Use the `no` form of this command to remove a RADIUS server.

### Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) seq-num
(<1-8>)

radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) seq-num
(<1-8>) timeout <1-60>

radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) seq-num
(<1-8>) (acct-port <0-65535> |) | timeout <1-60> |)

radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) seq-num
(<1-8>) (| (auth-port <0-65535> (| (acct-port <0-65535> (| (timeout <1-60>))))))

radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) seq-num
(<1-8>) (| (key ((0 WORD) | (7 WORD) ) (| (auth-port <0-65535> (| (acctport <0-65535>
(| (timeout <1-60>))))))))

no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|)

no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|)
timeout
```

### Parameters

<code>login</code>	Remote login
<code>A.B.C.D</code>	IPv4 address of RADIUS server
<code>X:X::X:X</code>	IPv6 address of RADIUS server
<code>HOSTNAME</code>	DNS host name of RADIUS server
<code>seq-num</code>	seq-num Sequence Number / Priority index for radius-servers
<code>&lt;1-8&gt;</code>	sequence number for servers
<code>timeout</code>	How long to wait for a response from the RADIUS server before declaring a timeout failure
<code>&lt;1-60&gt;</code>	Range of time out period in seconds
<code>vrf</code>	Virtual Routing and Forwarding
<code>management</code>	Management VRF

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

**Examples**

```
#configure terminal  
(config)#radius-server login host 203.0.113.15 vrf management seq-num 1
```

---

## radius-server login host acct-port

Use this command to configure a RADIUS server and specify a UDP port to use for RADIUS accounting messages.

Use the `no` form of this command to remove a RADIUS server.

### Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  <1-8>|) acctport <0-65535> |) | timeout <1-60> |)

no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) acct-
  port |) | timeout <1-60> |)
```

### Parameters

<code>login</code>	Remote login
<code>A.B.C.D</code>	IPv4 address of RADIUS server
<code>X:X::X:X</code>	IPv6 address of RADIUS server
<code>HOSTNAME</code>	DNS host name of RADIUS server
<code>acct-port</code>	UDP port to use for RADIUS accounting messages
<code>&lt;0-65535&gt;</code>	Range of UDP port numbers
<code>seq-num</code>	seq-num Sequence Number / Priority index for radius-servers
<code>&lt;1-8&gt;</code>	sequence number for servers
<code>timeout</code>	How long to wait for a response from the RADIUS server before declaring a timeout failure
<code>&lt;1-60&gt;</code>	Range of timeout period in seconds
<code>vrf</code>	Virtual Routing and Forwarding
<code>management</code>	Management VRF

### Default

By default, `radius-server login host acct-port` is 1813

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#radius-server login host 192.168.2.3 vrf management seq-num 2 acct-
port 23255
```



## radius-server login host auth-port

Use this command to configure a RADIUS server and specify a UDP port to use for RADIUS authentication messages.

Use the `no` form of this command to remove a RADIUS server.

### Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|) (|(authport <0-65535> (|(acct-port <0-65535> (|(timeout <1-60>))))))
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|)
  (authport (|(acct-port (|(timeout)))))
```

### Parameters

<code>login</code>	Remote login
<code>A.B.C.D</code>	IPv4 address of RADIUS server
<code>X:X::X:X</code>	IPv6 address of RADIUS server
<code>HOSTNAME</code>	DNS host name of RADIUS server
<code>seq-num</code>	seq-num Sequence Number / Priority index for radius-servers
<code>&lt;1-8&gt;</code>	sequence number for servers
<code>auth-port</code>	UDP port to use for RADIUS accounting messages
<code>&lt;0-65535&gt;</code>	Range of UDP port numbers
<code>acct-port</code>	UDP port to use for RADIUS accounting messages
<code>&lt;0-65535&gt;</code>	Range of UDP port numbers
<code>timeout</code>	How long to wait for a response from the RADIUS server before declaring a timeout failure
<code>&lt;1-60&gt;</code>	Range of timeout period in seconds
<code>vrf</code>	Virtual Routing and Forwarding
<code>management</code>	Management VRF

### Default

By default, `radius-server login host acct-port` is 1812

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management seq-num 1 auth-port
23255
```

## radius-server login host key

Use this command to set per-server shared key ("shared secret") which is a text string shared between the device and RADIUS servers.

Use the no form of this command to remove a server shared key.

### Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>|) |(key ((0 WORD) | (7 WORD) | (WORD)) |(auth-port <0-65535> |(acct-
    port <0-65535>
  |(timeout <1-60>))))))

no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (key
  ((0 WORD) | (7 WORD) | (WORD)) |(auth-port <0-65535> |(acct-port
  |(timeout))))))
```

### Parameters

login	Remote login
A.B.C.D	IPv4 address of RADIUS server
X:X::X:X	IPv6 address of RADIUS server
HOSTNAME	DNS host name of RADIUS server
seq-num	seq-num Sequence Number / Priority index for radius-servers
<1-8>	sequence number for servers
0	Unencrypted (clear text) shared key
WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 63 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
auth-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
acct-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
timeout	How long to wait for a response from the RADIUS server before declaring a timeout failure
<1-60>	Range of timeout period in seconds
vrf	Virtual Routing and Forwarding
management	Management VRF

### Default

No default value is specified

### Command Mode

Configure mode

**Applicability**

This command was introduced before OcNOS version 1.3.

**Examples**

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management seq-num 1 key 0
testing auth-port 23255
```

---

## radius-server login key

Use this command to set a global preshared key ("shared secret") which is a text string shared between the device and RADIUS servers.

Use the `no` form of this command to remove a global preshared key.

### Command Syntax

```
radius-server login key ((0 WORD) | (7 WORD)) (vrf management|)
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
(<1-8>|) (|(key ((0 WORD) | (7 WORD)) (|(auth-port <0-65535> (|(acctport <0-65535>
(|(timeout <1-60>))))))))))
no radius-server login key ((0 WORD) | (7 WORD)) (vrf management|)
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf
management|) (seqnum(<1-8>|) (key ((0 WORD) | (7 WORD)) (|(auth-port <0-65535>
(|(acctport(|(timeout))))))))))
```

### Parameters

login	Remote login
0	Unencrypted (clear text) shared key
WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 63 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
vrf	Virtual Routing and Forwarding
management	Management VRF

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#radius-server login key 7 p2AcxlQA vrf management

#configure terminal
(config)#no radius-server login key 7 p2AcxlQA vrf management
```

---

## radius-server login timeout

Use this command to set the global timeout which is how long the device waits for a response from a RADIUS server before declaring a timeout failure.

Use the `no` form of this command to set the global timeout to its default (1 second).

**Note:** TELNET client session's default timeout is 60 seconds, so configuring timeout of 60 seconds timeout impacts TELNET client applications, because it cannot be fallback to use the other configured server/group. Hence it is recommended to configure 57 seconds or lesser timeout while using TELNET. This timeout doesn't have an impact on SSH connections.

### Command Syntax

```
radius-server login timeout <1-60> (vrf management|)
no radius-server login timeout (vrf management|)
```

### Parameters

<code>login</code>	Remote login
<code>&lt;1-60&gt;</code>	Range of timeout period in seconds
<code>vrf</code>	Virtual Routing and Forwarding
<code>management</code>	Management VRF

**Note:** The system takes minimum 3 secs to timeout even though the configured timeout value is less than 3 seconds. Hence do not configure timeout value less than 3 secs. The timeout range value is mentioned as 1-60 secs for backward compatibility.

### Default

By default, radius-server login timeout is 5 seconds

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#radius-server login timeout 15 vrf management

#configure terminal
(config)#no radius-server login timeout 15 vrf management
```

---

## show debug radius

Use this command to display debugging information.

### Command Syntax

```
show debug radius
```

### Parameters

None

### Command Mode

Executive mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show debug radius  
RADIUS client debugging is on
```

---

# show radius-server

Use this command to display the RADIUS server configuration.

## Command Syntax

```
show radius-server (|vrf(management|all)) ((WORD) |(groups (GROUP|)|)|sorted
```

## Parameters

WORD	DNS host name or IP address
groups	RADIUS server group
GROUP	Group name; if this parameter is not specified, display all groups
sorted	Sort by RADIUS server name
vrf	management or all VRFs

## Command Mode

Executive mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show radius-server vrf management
    VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:
Radius Server      : 10.12.12.39
  Sequence Number  : 1
  available for authentication on port : 1812
  available for accounting on port    : 1813
  RADIUS shared secret : *****
  Failed Authentication count      : 0
  Successful Authentication count   : 0
  Failed Connection Request       : 0
  Last Successful authentication   :

Radius Server      : 1.1.1.1
  Sequence Number  : 2
  available for authentication on port : 1234
  available for accounting on port    : 1234
  timeout          : 5
  Failed Authentication count      : 0
  Successful Authentication count   : 0
  Failed Connection Request       : 0
  Last Successful authentication   :
```

[Table 19-64](#) explains the output fields.

**Table 19-64: show radius-server fields**

Entry	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Timeout Value	Period the local router waits to receive a response from a RADIUS accounting server before retransmitting the message
Total number of servers	Number of authentication requests received by the authentication server.



---

## show running-config radius

Use this command to display RADIUS configuration settings in the running configuration.

### Command Syntax

```
show running-config radius
```

### Parameters

None

### Command Mode

Executive mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show running-config radius
radius-server login key 7 0x67efdb4ad9d771c3ed8312b2bc74cedb vrf management
radius-server login host 10.12.12.39 vrf management seq-num 1 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb
```



---

## CHAPTER 20 Secure Shell

---

This chapter describes Secure Shell (SSH) commands.

SSH is a cryptographic protocol for secure data communication, remote login, remote command execution, and other secure network services between two networked computers.

Note: In OcNOS, the default Linux terminal type is "export TERM=xterm"

Note: The commands below are supported only on the "management" VRF.

This chapter contains these commands:

- [clear ssh host-key](#)
- [clear ssh hosts](#)
- [debug ssh server](#)
- [feature ssh](#)
- [show debug ssh-server](#)
- [show running-config ssh server](#)
- [show ssh host-key](#)
- [show ssh server](#)
- [show username](#)
- [ssh](#)
- [ssh6](#)
- [ssh server algorithm encryption](#)
- [ssh keygen host](#)
- [ssh login-attempts](#)
- [ssh server port](#)
- [ssh server session-limit](#)
- [username sshkey](#)
- [username keypair](#)

---

## clear ssh host-key

Use these commands to remove SSH server host key.

### Command syntax

```
clear ssh host-key ((dsa|rsa|ecdsa|ed25519)|) (vrf management|)
```

### Parameters

dsa	dsa keys
rsa	rsa keys
ecdsa	ecdsa keys
ed25519	ed25519 keys
management	Management VRF

### Default

If no keys are specified, all the host keys will be removed

### Command Mode

Privilege exec mode

### Applicability

This command was introduced in OcNOS version 5.0

### Examples

```
OcNOS#clear ssh host-key vrf management
OcNOS#
OcNOS#clear ssh host-key rsa
OcNOS#
```

---

## clear ssh hosts

Use this command to clear the `known_hosts` file.

This command clears all trusted relationships established with SSH servers during previous connections. When a client downloads a file from an external server the first time, the client stores the server keys in the `known_hosts` file. After that, other connections to the same server will use the server keys stored in the `known_hosts` file. In other words, a trusted relationship is created when a client accepts the server keys the first time.

An example of when you need to clear a trusted relationship is when SSH server keys are changed.

### Command Syntax

```
clear ssh hosts
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#clear ssh hosts
```

---

## debug ssh server

Use this command to display SSH server debugging information.

Use the `no` form of this command to stop displaying SSH server debugging information.

### Command Syntax

```
debug ssh server
no debug ssh server
```

### Parameters

None

### Default

By default, disabled.

### Command Mode

Executive mode and configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#debug ssh server
```

---

## feature ssh

Use this command to enable the SSH server.

Use the `no` form of this command to disable the SSH server.

### Command Syntax

```
feature ssh (vrf management|)
no feature ssh (vrf management|)
```

### Parameters

management	Virtual Routing and Forwarding name
------------	-------------------------------------

### Default

By default, feature ssh is enabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)feature ssh
```

---

## show debug ssh-server

Use this command to display whether SSH debugging is enabled.

### Command Syntax

```
show debug ssh-server
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show debug ssh-server  
ssh server debugging is on
```



---

## show running-config ssh server

Use this command to display SSH settings in the running configuration.

### Command Syntax

```
show running-config ssh server
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show running-config ssh server
feature ssh vrf management
ssh server port 1024 vrf management
ssh login-attempts 2 vrf management
ssh server algorithm encryption 3des-cbc
```

---

## show ssh host-key

Use this command to display the SSH server key.

By default, ssh feature is enabled in "management" vrf. Until and unless the same feature is explicitly enabled in "default" vrf, respective show command output will be empty.

### Command syntax

```
show ssh host-key ((dsa|rsa|ecdsa|ed25519)|) (vrf management|)
```

### Parameters

dsa	dsa keys
rsa	rsa keys
ecdsa	ecdsa keys
ed25519	ed25519 keys
management	Management VRF

### Default

If no keys are specified, all host keys will be displayed

### Command Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 5.0

### Examples

```
#sh ssh host-key
*****
dsa public key :

ssh-dss AAAAB3NzaC1kc3MAAACBANgq+TZPkmKOn7ot7PBO9TOCV/
+GPyHCz9Wq39+6veigQ2CWmLNo
uqZb1B05LfeU2MuRz4rtO6mcX81nAygqDLNZaRsirYdWTsJ40HAOZYr9765w+M8TAcKmBYbuWSIkqn
YQ
J1h5bj6UrJ7dW4LgaSxmVmrkXoYrr5gnxfEVgw8HAAAAFQC//
BVHnTWh8Iizbk0mvOyNzqtfMwAAAIBQ
Ca9X0qbL66Js0ul+7LMmLvWkC4Fy1Y/3igZORZ+NsnP4CJIJ1JCLwj7nj/NeUfUuyG1/
dnDVdki4FngL
LjbVa5XrK5VbsEj4sZBfebklVZKd8h880FqNhfc3iZjCGqdYrWWlRYdNqNvq7zVa6YC7Vvo0sEC5/
rDm
aNygbx0iCAAAAIEAoZHk+5cqaYptqYBPGPMRynpWyWJPJQjoiy+p1BRNk7E/kwInQaqmtFQuM/
YaTOoN
nz5skwQ1dJmdJGq+h7bfmab0atzaaVjkcTjz0rtSBO3JID2G6KqG55yhr03bc8BY+A6g9Qm8TuWZU6
8D
NIZGj28GZSbkIpQgqSD9VUAxEHs=

dsa fingerprint :
```

---

1024 SHA256:Qzd8n4RjsxeW9+AnUP+zc59oPRTl2FBwdwDfVBq0DdQ

\*\*\*\*\*

\*\*\*\*\*

rsa public key :

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC706mz0GQvdEaqK/2zUUtCOh/  
kEUkZpQ7d8gie4jfl

yV4nV2glu7oIbdnoBBI0a5bIwbUGDHPUvfTpoJntpryY7G/

QIWuBJVDiu6QteoB4u5byNVbSqA3fljbF

MISYfLxK3i3S07htadDfUIpYTyx/

D5PCf8DDxmdf7UkhOM4Quj8GgGW3PacE2YyJASBq5x7MaWEUiStu

NgtemWqR/DTw+OO8l3gZzHhWBcmHLzo3jdkH/

8ffLGEWqEb78wR4lxckVlja4suFB0GEa7vFLucYO3Tp

GzZARf7iY5A0bB0fi7ZilyQ3RN7+di28lSNWsFCzZm8vWS7GyLUFn1xttlqJ

rsa fingerprint :

2048 SHA256:YVX+zlrDk8bqzF+HPKpFW0BttbLoiQ5IBDVI/VMYhbs

\*\*\*\*\*

\*\*\*\*\*

ecdsa public key :

ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBCN/  
XoG

uZGwNfKCE+cuQOULrSHomRSmkDp0u6MsoNIVLhtRe9+r8Ak7G8taE55D7NgugnEDzdLKBmeCZWcww6  
4=

ecdsa fingerprint :

256 SHA256:T7KOgXyrU/38EvO6z/apgYDANf+q9YhqCiYoocD5Ajj

\*\*\*\*\*

\*\*\*\*\*

ed25519 public key :

ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAII/jNFIYKbUk/ePbp4wu/  
AjhP5gERqn6F+4tH39idbh7

ed25519 fingerprint :

256 SHA256:1MU6iy03eEQBj099GERLjkMCPDoUwkdCwGh8bgYZbeo

\*\*\*\*\*

#

---

## show ssh server

Use this command to display the SSH server status.

### Command Syntax

```
show ssh server
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show ssh server
VRF MANAGEMENT:
ssh server enabled port: 22
authentication-retries 3
VRF DEFAULT:
ssh server enabled port: 22
authentication-retries 3
#
```

---

## show username

Use this command to display the RSA or DSA key pair for a user.

### Command Syntax

```
show username USERNAME keypair
```

### Parameters

USERNAME	User identifier
----------	-----------------

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3

### Examples

```
#show username kedar keypair
*****RSA KEY*****
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDCnWo/3Y7LlVkw/Z43dbVIm+I3o25JlgUTmwa9l1
T35+2gNvDbIPfYAqUKYgrmXKDC9vg7f4SAsmXS+4ZwrrQSTTsHk8PNLA+4lEcufFNl3jpfXTuhphN9
N9
i+uFHGYIIviWZksiRqpMZmDlALyzAIOzyCfG44hlRm3/
pYfhBNhHruvxYVhbp4wHsmrWfcFb+HZCWQGM
CJupxu8bouGd2UW5/B1Vy1yuYNIhdo2NHjUI+ameETV+Wroki8+OLVA6eXp5/
KY3Bj9x2+AxOCiKcpU0
axwFSoCbP3+29wrp4JJhl4ssSqM+19+VbUtpuXAM0cR7VQ7mJ0JDZ9tBvK4l8/
bitcount: 2048 fingerprint: 2b:ac:17:a4:ef:1d:79:4e:2d:17:af:72:4c:c7:e4:2f
*****
*****DSA KEY*****
ssh-dss AAAAB3NzaC1kc3MAAACBAP0npAm+Pw8t7OpO+KQ0Vx3ayXavHHVPPAKOo8RTmquE8zUSjn
/XiZ+vP2343RpXu9/
jLwAcCUMfNBZyE8NbmGKxMMk2PqMz10VtfvDon5LSNurXL4lypZLG2hR2PNva4w
6b4Adpd+ElfEoUncIgOun2i4S08N5TCMYVyusKjYzDAAAFQCWeAzeahZeoIzBlnSo87madxfL3QAA
AI
EA4b86l/
nHoWobRoYBrkeOGtjyWLRKk1P2T+rGH+j0rqqJiD0sh2PVfppylliNvqLtYSmXyMCxzEEeFd
HH1cVXgrgQjtUOeCPhF+2We2ummm1Cwg4v71Z358FRjsi9VgJ/vQUpOq1hRDhwjJHtEHSA+NkX/
ccW9J
ww8Y0oNhCI7DcAAACANuYiP6tKGSU9LeClF1F65Tq1blVHfLp3TSeZYPldqonDoZ1qo3NNvOOH5KN8
Lj
MRtTCNlGaXow1QccS941XFy3efuWXxC00HZ64FhmjCyOYYv2Wsvn4UGCAG3ikiu6M1xjOLl6b53H4m
B3
w7O6bkcyjHlGnytwrgR0D/nlsZ/9fs=
bitcount: 1024 fingerprint: c1:0a:e5:e1:a1:78:ae:c2:4a:07:4a:50:07:4b:d5:84
*****
```

---

## ssh

Use this command to open an ssh session to a IPv4 address or host name resolved to an IPv4 address.

### Command Syntax

```
ssh WORD (vrf (NAME | management))
ssh WORD <1-65535> (vrf (NAME | management))
ssh (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | aes192-cbc |
aes256-cbc | 3des-cbc)) WORD (vrf (NAME | management))
ssh (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | aes192-cbc |
aes256-cbc | 3des-cbc)) WORD <1-65535> (vrf (NAME | management))
```

### Parameters

WORD	User and destination host name to resolve into IPv4 address to open a SSH session as user@ipv4-address/hostname
1-65535	Destination Port to open a SSH session. Default is 22.
cipher	Specify algorithm to encrypt SSH session
aes128-ctr	Advanced Encryption Standard 128 bit Counter Mode
aes192-ctr	Advanced Encryption Standard 192 bit Counter Mode
aes256-ctr	Advanced Encryption Standard 256 bit Counter Mode
aes128-cbc	Advanced Encryption 128 bit Standard Cipher Block Chaining
aes192-cbc	Advanced Encryption Standard 192 bit Cipher Block Chaining
aes256-cbc	Advanced Encryption Standard 256 bit Cipher Block Chaining
3des-cbc	Triple Data Encryption Standard Cipher Block Chaining
vrf	VPN routing/forwarding instance.
NAME	Name of the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance.

### Default

The default destination port is 22.

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#ssh cipher aes128-ctr 10.12.16.17 22 vrf management
The authenticity of host '10.12.16.17 (10.12.16.17)' can't be established.
RSA key fingerprint is 93:82:98:ce:b7:20:1a:85:a5:9a:2e:93:13:84:ea:9e.
Are you sure you want to continue connecting (yes/no)?
```

---

## ssh6

Use this command to open an ssh session to an IPv6 address or host name resolved to an IPv6 address.

### Command Syntax

```
ssh6 (X:X::X:X | HOSTNAME) (vrf (NAME | management))
ssh6 (X:X::X:X | HOSTNAME) <1-65535> (vrf (NAME | management))
ssh6 (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | aes192-cbc |
aes256-cbc | 3des-cbc)) (X:X::X:X | HOSTNAME) (vrf (NAME | management))
ssh6 (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | aes192-cbc |
aes256-cbc | 3des-cbc)) (X:X::X:X | HOSTNAME) <1-65535> (vrf (NAME |
management))
```

### Parameters

X:XX::X:X	User and destination IPv6 address to open an SSH session as user@ipv6-address
HOSTNAME	User and destination host name to resolve into IPv6 address to open an SSH session as user@ipv4-address/hostname
1-65535	Destination Port to open a SSH session. Default is 22.
cipher	Algorithm to encrypt SSH session
aes128-ctr	Advanced Encryption Standard 128 bit Counter Mode
aes192-ctr	Advanced Encryption Standard 192 bit Counter Mode
aes256-ctr	Advanced Encryption Standard 256 bit Counter Mode
aes128-cbc	Advanced Encryption 128 bit Standard Cipher Block Chaining
aes192-cbc	Advanced Encryption Standard 192 bit Cipher Block Chaining
aes256-cbc	Advanced Encryption Standard 256 bit Cipher Block Chaining
3des-cbc	Triple Data Encryption Standard Cipher Block Chaining
vrf	VPN routing/forwarding instance.
NAME	Name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance.

### Default

The default destination port is 22.

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#ssh6 cipher aes128-ctr 2:2::2:2 22 vrf management
The authenticity of host '2:2::2:2 (2:2::2:2)' can't be established.
RSA key fingerprint is 93:82:98:ce:b7:20:1a:85:a5:9a:2e:93:13:84:ea:9e.
```

Are you sure you want to continue connecting (yes/no)?



---

## ssh server algorithm encryption

Use this command to set an encryption algorithm for SSH sessions.

An SSH server authorizes connection of only those algorithms from the list below. If a client tries to establish a connection to the server with the algorithm encryption not in the list, the connection fails.

SSH supports these encryption algorithms:

- Advanced Encryption Standard Counter:
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - aes128-cbc
- Advanced Encryption Standard Cipher Block Chaining:
  - aes192-cbc
  - aes256-cbc
- Triple Data Encryption Standard Cipher Block Chaining:
  - 3des-cbc

Use the `no` form of this command to not encrypt SSH sessions.

### Command Syntax:

```
ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc  
| aes192-cbc | aes256-cbc | 3des-cbc} (vrf management|)  
no ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-  
cbc | aes192-cbc | aes256-cbc | 3des-cbc} (vrf management|)
```

### Parameters

aes18-ctr	AES 128 bit Counter Mode
aes192-ctr	AES 192 bit Counter Mode
aes256-ctr	AES 256 bit Counter Mode
aes128-cbc	AES 128 bit Cipher block chaining
aes192-cbc	AES 192 bit Cipher block chaining
aes256-cbc	AES 256 bit Cipher block chaining
3des-cbc	Triple DES Cipher block chaining
vrf management	Management VPN routing/forwarding instance.

### Default

No encryption.

By default, all the ciphers are supported for a new SSH client to connect to the SSH server.

### Command Mode

Configure mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#configure terminal
(config)#ssh server algorithm encryption aes128-ctr
```

## ssh keygen host

Use these commands to create SSH server host, and public keys. These host keys are added in the SSH clients known\_hosts file after user's acceptance.

Once entry is added in known\_hosts, for the subsequent attempt login to the server will be validated against the host key and if there is key mismatch user will be prompted about the change in server identity.

### Command syntax

```
ssh keygen host dsa (vrf management|) (force|)
ssh keygen host rsa (length <1024-4096>|) (vrf management|) (force|)
ssh keygen host ecdsa (length (256|384|521)|) (vrf management|) (force|)
ssh keygen host ed25519 (vrf management|) (force|)
```

### Parameters

dsa	dsa keys
rsa	rsa keys
ecdsa	ecdsa keys
ed25519	ed25519 keys
management	Management VRF
force	Replace the old host-key with newly generated host-key
<1024-4096>	Number of bits to use when creating the SSH server key; this parameter is only valid for RSA keys (DSA keys have a default length of 1024)

### Default

DSA key has length of 1024 bits

RSA key has default length of 2048 bits

ECDSA key has default length of 521 bits

ED25519 key has length of 256 bits

### Command Mode

Privilege exec mode

### Applicability

This command was introduced in OcNOS version 5.0

### Examples

```
OcNOS#ssh keygen host rsa vrf management
OcNOS#
OcNOS#ssh keygen host ecdsa vrf management
OcNOS#
OcNOS#ssh keygen host ecdsa
%% ssh host key exists, use force option to overwrite
OcNOS#
OcNOS#ssh keygen host ecdsa force
```

---

## ssh login-attempts

Use this command to set the number of times that a user can try to log in to a SSH session.

Use the `no` form of this command to set the number of login attempts to its default (3).

Enable the [feature ssh](#) command to configure this command on default vrf port.

You can only give this command when the SSH server is enabled for default vrf. See the [feature ssh](#) command.

### Command Syntax

```
ssh login-attempts RETRIES (vrf management|)
no ssh login-attempts (vrf management|)
```

### Parameters

RETRIES	Number of retries <1-3>
management	Management VPN routing/forwarding instance.

### Default

By default, the device attempts to negotiate a connection with the connecting host three times.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ssh login-attempts 3
```

---

## ssh server port

Use this command to set the port number on which the SSH server listens for connections. The default port on which the SSH server listens is 22.

Use the `no` form of this command to set the default port number (22).

### Command Syntax

```
ssh server port <1024-65535> (vrf management|)
no ssh server port (vrf management|)
```

### Parameters

<1024-65535>	Port number
management	Management VPN routing/forwarding instance.

### Default

By default, the SSH server port is 22.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#ssh server port 1720
```

---

## ssh server session-limit

Use this command to limit number of SSH sessions. Only 40 sessions allowed including Telnet and SSH.

Use `no` form of this command to set to default value.

Note: Few Terminal application (Ex: MobaXterm) where user run SSH Client has limits to use this SSH session limit option.

### Command Syntax

```
ssh server session-limit <1-40> (vrf management|)
no ssh server session-limit (vrf management|)
```

### Parameters

<1-40>	Number of sessions
management	Virtual Routing and Forwarding name

### Default

By default, 40 sessions are allowed.

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS-SP version 4.2

### Examples

```
#configure terminal
(config)#ssh server session-limit 4 vrf management
```

## username sshkey

Use this command to create a user account.

### Command Syntax

```
username USERNAME sshkey LINE
```

### Parameters

USERNAME	User identifier
LINE	Digital System Algorithm (DSA) key or Rivest, Shamir, and Adelman (RSA) key in OpenSSH format; this key is written to the <code>authorized_keys</code> file

### Default

By default, SSHKEY is 1024.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#username fred sshkey ssh-rsa
AAAAB3NzaC1kc3MAAAEBAIirweZzCdyITqbMWB8Wly9ivGxY1JBVnWTVtcWKi6uc
CPZyw3I6J6/+69LEkPUSAYo+SK8zj0NF2f25FFc2YDMh1KKHi5gK7iXF3/ran54j
nP2byyLeo8rnuVqfEDLaBilqQaWBcdQvsZc14t5SEJfsOQSfr03PDqPYAisrZRvM
5pWfzo486Rh33J3+17OuARQtZFDp4wA5zZoFxl4U3RK42JzKNUiYBDrH3lSgfkv
XLWLXz9WcxY6zuKvXFWUpOA9PRXwUsKQqWuyyWZQLNavENqFyoQ8oZnNKLcYE0h8
QnUe62NGxb3jQXKLf1OL04JFNiii9sACG1Y/ut4ANysAAAAVAJbM7Z4chRgiVahN
iwXFJNkBmWGZAAABAAuF1FlI6xy0L/pBaIlFw34uUL/mh4SR2Di2X52eK70VNj+m
y5eQdRC6cxpaVqpS3Q4xTN+W/kaBbIlX40xJP5lcmVfn/nqiuIeEodmVIJMWxOD
fh3eGeGuSW6l4Vzd1RGrxpYInIOygmULRcxhmbX+rPliuUIvhg36iH0UR7XBln6h
uyKFvEmaL7bGlRvELjqaj0y6iiCfPlyGBc5vavH5X+jOWqdsJHsCgcIzPF5D1Ybp
w0nZmGsqO+P55mjMuj002uI7Ns1sxyirbnGhd+ZZ1u03QDy6MBcUspai8U5CIe6X
WqvXY+yJjpuvlW9GTHowCcGd6Z/e9IC6VE/kNEAAAAEAFIe6kLGTALR0F3AfapYY
/M+bvkmkKhOJUzVdLiwMjcvTJb9fQpPxqXElS3ZvUNIEELUPS/V7KgSsj8eg3FKN
iUGICkTwHIK7RTLC8k4IE6U3V3866JtxW+Znv1DB7uwnbZgoIZuVt3r1+h8O0ah8
UKwDUMJT0fwu9cuuS3G8Ss/gKilHgByrcXoK51/r4Bc4QmR2VQ8sXOREv/SHJeY
JGbEX3OxjRgXC7Glprdpil8zs0dPiZ0ovAswsBOYlKYhd7JvfCcvWRjgP5h55aw
GNSmNs3STKufbIqYGeDAISYNY4F2JzR593KIBnWgyhokyYybyEBh8NwTTO4J5rT
ZA==
```

---

## username keypair

Use this command to generate the key for users.

### Command Syntax

```
username USERNAME keypair rsa
username USERNAME keypair dsa
username USERNAME keypair rsa length <1024-4096>
username USERNAME keypair rsa length <1024-4096> force
username USERNAME keypair rsa force
username USERNAME keypair dsa force
```

### Parameters

USERNAME	User identifier
rsa	Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key
dsa	Digital System Algorithm (DSA) SSH key
<1024-4096>	Number of bits to use when creating the SSH server key; this parameter is only valid for RSA keys (DSA keys have a default length of 1024)
force	Forces the replacement of an SSH key

### Default

DSA keys have a default value of 1024.

RSA keys have a minimum key length of 1024 bits and the default length is 4096.

By default the system has RSA/DSA public/private key pair placed in /etc/ssh/. The force option is used if the user wants to regenerate the ssh rsa keys. The same thing applies for dsa also.

### Command Mode

Execute mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#username fred keypair rsa
```



---

## CHAPTER 21 sFlow Commands

---

This chapter describes the Sampled Flow (sFlow) commands.

- [clear sflow statistics](#)
- [debug sflow](#)
- [feature sflow](#)
- [sflow agent-ip](#)
- [sflow collector](#)
- [sflow poll-interval](#)
- [sflow sampling enable](#)
- [sflow sampling-rate](#)
- [show sflow](#)
- [show sflow interface](#)
- [show sflow statistics](#)

---

## clear sflow statistics

Use this command to clear sFlow sampling-related counters such as the number of packets sampled and the number of counters sampled.

### Command Syntax

```
clear sflow statistics (interface IFNAME|)
```

### Parameters

IFNAME	Interface name
--------	----------------

### Default

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear sflow statistics
```

---

## debug sflow

Use this command to display sFlow debugging messages.

### Command Syntax

```
debug sflow (all|agent|sampling|polling|)
```

### Parameters

all	Debug all (agent,sampling,polling)
agent	Debug sFlow agent
sampling	Debug sFlow sampling
polling	Debug sFlow polling

### Default

By default, debug command is disabled.

### Command Mode

Exec mode and Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#debug sflow all
#debug sflow agent

#configure terminal
(config)#debug sflow agent
```

---

## feature sflow

Use this command to enable the sFlow feature.

Use the no form to disable the sFlow feature.

### Command Syntax

```
feature sflow
no feature sflow
```

### Parameters

None

### Default

By default, sFlow feature is disabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
(config)#feature sflow
```

---

## sflow agent-ip

Use this command to manually configure the agent IP address when there the eth0 IP address is down. The sflow is enabled only when the eth0 ip address available. The switch sends th sflow packets to the sflow collector via agent IP address.

### Command Syntax

```
sflow agent-ip A.B.C.D
no sflow agent-ip
```

### Parameters

agent-ip	sFlow Agent
A.B.C.D	Ipv4 address type

### Default

By default, disabled.

### Command Mode

Exec mode and Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.9

### Example

```
OcNOS(config)#sflow agent-ip 10.10.10.1
OcNOS(config)#no sflow agent-ip
```

---

## sflow collector

Use this command to configure the collector details such as the collector IPv4 address, port number, receiver time-out and datagram size.

Use the `no` form of this command to disable the sFlow collector.

### Command Syntax

```
sflow collector A.B.C.D port <1024-65535> receiver-time-out <0-2147483647>
max-datagram-size <200-9000>

no sflow collector (A.B.C.D port <1024-65535>|)
```

### Parameter

A.B.C.D	Collector IPv4 address. This address must be reachable via the management VRF.
<1024-65535>	Collector UDP Port number. The standard sFlow UDP Port : 6343
<0-2147483647>	Receiver time out value in seconds. Zero means no timeout. Upon timeout, value collector information is removed, stopping any ongoing sampling.
<200-9000>	Maximum datagram size in bytes that can be sent Collector

### Default

By default, sFlow collector is disabled. Default port number is 6343.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#sflow collector 2.2.2.2 port 1111 receiver time-out 30 max-datagram-
size 500

(config)#no sflow collector
```

---

## sflow poll-interval

Use this command to configure the sFlow counter polling interval. Any change in the polling interval restarts ongoing polling of existing data source interfaces, if any.

Use the `no` form of this command to disable the sFlow counter polling interval.

### Command Syntax

```
sflow poll-interval <5-60>
no sflow poll-interval
```

### Parameters

<5-60>	Interface counter. Polling interval in seconds
--------	--

### Default

By default, sFlow counter polling interval is disabled.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#interface xel
(config-if)#sflow poll-interval 25
(config-if)#no sflow poll-interval
```

---

## sflow sampling enable

Use this command to enable or disable sampling on an interface after giving the [sflow sampling-rate](#) command on the same interface.

Note: sFlow egress sampling for multicast, broadcast, or unknown unicast packets is not supported.

### Command Syntax

```
sflow enable
no sflow enable
```

### Default

By default, sFlow sampling is disabled.

### Command Mode

Interface mode

### Parameters

None

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
(config)#interface xel
(config-if)#sflow sampling-rate 1024 direction ingress max-datagram-size 200
(config-if)#sflow enable
(config-if)#no sflow enable
```



---

## sflow sampling-rate

Use this command to set the sampling rate on an interface. Any change in the sampling rate restarts the ongoing sampling of existing data-source interfaces, if any.

Use the `no` form of this command to disable the sFlow sampling rate.

**Note:** Packets to CPU is rate limited. In case of unknown unicast, rate limit is applied to such packets as well as sampled data packets.

### Command Syntax

```
sflow sampling-rate <1024-16777215> direction (ingress | egress) max-header-size
<128-256>

no sflow sampling-rate direction (ingress | egress)
```

### Parameters

<1024-16777215>	Sampling rate
direction	The direction of sampling an interface:
ingress	Ingress traffic
egress	Egress traffic
<128-256>	Maximum header size in bytes

### Default

By default, sFlow sampling rate is disabled.

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#interface xel
(config-if)#sflow sampling-rate 1024 direction ingress max-header-size 200
(config-if)#no sflow sampling-rate direction ingress
```

# show sflow

Use this command to display sFlow agent configuration along with statistics for all interfaces.

## Command Syntax

```
show sflow (brief | detail)
```

## Parameters

- `brief` Display configuration parameters on interfaces along with sampling rate and poll interval.
- `detail` Same as `brief` along with configured and default attributes and values of sFlow agent, sFlow collector, and sampling information.

## Default

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#show sflow
sFlow Feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent      IP: 10.12.16.38
Collector IP: 10.12.16.17      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)         : 0

sFlow Port Detailed Information:
Interface  Packet-Sampling      Packet-Sampling      Counter-Polling      Maximum Header
           Rate        Count        Interval      Count        Size(bytes)
           Ingress    Egress    Ingress    Egress    (sec)
-----
xe1         1024         0         0         0         6         3         128         0

#
#show sflow brief
sFlow Feature: Enabled
Collector IP: 10.12.16.17      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)         : 0

sFlow Port Configuration:
Interface  Status      Sample Rate      Counter-Polling
           Ingress    Egress    Ingress    Egress    Interval (sec)
-----
xe1         Enabled    Disabled    1024         0         6
```

**Table 21-65: Show sflow output**

Entry	Description
sFlow feature	Shows whether sFlow is enabled or disabled.
sFlow Version	Displays the sFlow version. Version 5 is the current global standard.
sFlow Global Information	Global Information consists of the Agent IP address, Collector IP, Port number, Maximum Datagram Size, and the Receiver timeout.
Agent IP	IPv4 address of this switch/router.
Collector IP	IPv4 address of the sFlow collector server.
Port	Port number on the sFlow collector server. Standard is port 6343.
Maximum Datagram Size	The maximum size of the datagrams sent by the agent
Receiver timeout	The number of seconds between each sampling – zero means sample continuously.
sFlow Port Interface	The interface of this switch/router on which sFlow is running (e.g. xe1/1).
Packet-Sampling Rate	the number of packets received or transmitted before a sample is taken.
Packet-Sampling Count	The number of sample packets that have been sampled on both the ingress and egress of the interface.
Counter-Polling	Shows the amount of time between polling samples and the count of the total number of polling samples taken.
Maximum Header Size	The maximum header size for both the ingress and egress of the interface.

# show sflow interface

Use this command to display the sFlow configuration for the input interface.

## Command Syntax

```
show sflow interface IFNAME
```

## Parameters

IFNAME	Interface name
--------	----------------

## Default

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

Note: For information about the output of this command, see the [show sflow](#) command.

```
#show sflow interface xel
sFlow feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent      IP: 10.10.26.104
Collector IP: 10.12.16.18      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)         : 0
```

sFlow Port Detailed Information:					
Interface	Packet-Sampling		Counter-Polling		Maximum Header
	Rate	Count	Interval(sec)	Count	Size(bytes)
-----	-----	-----	-----	-----	-----
xel	1024	0	6	41	128

---

## show sflow statistics

Use this command to display sFlow counter information.

### Command Syntax

```
show sflow statistics (interface IFNAME|)
```

### Parameters

IFNAME                      Interface name.

### Default

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

Note: For information about the output of this command, see the [show sflow](#) command.

```
#show sflow statistics
```

```
sFlow Port Statistics:
Interface  Packet-Sampling  Counter-Polling
          Count    Count
-----
xe1                0                19
```



---

## CHAPTER 22 Simple Network Management Protocol

---

This chapter is a reference for Simple Network Management Protocol (SNMP) commands.

SNMP provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- An SNMP manager: The system used to control and monitor the activities of network devices. This is sometimes called a Network Management System (NMS).
- An SNMP agent: The component within a managed device that maintains the data for the device and reports these data SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables which describe the system configuration. These variables can be queried by SNMP managers.

In SNMP, administration groups are known as *communities*. SNMP communities consist of one agent and one or more SNMP managers. You can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The security levels are:

- noAuthNoPriv: No authentication or encryption
- authNoPriv: Authentication but no encryption
- authPriv: Both authentication and encryption.

SNMP is defined in RFCs 3411-3418.

Note: The commands below are supported on the “management” and default VRF.

This chapter contains these commands:

- `debug snmp-server`
- `show running-config snmp`
- `show snmp`
- `show snmp community`
- `show snmp context`
- `show snmp engine-id`
- `show snmp group`
- `show snmp host`
- `show snmp user`
- `show snmp view`
- `snmp context`
- `snmp-server community`
- `snmp-server community-map`
- `snmp-server contact`

- [snmp-server context](#)
- [snmp-server disable default](#)
- [snmp-server enable snmp](#)
- [snmp-server enable traps](#)
- [snmp-server engineID](#)
- [snmp-server group](#)
- [snmp-server host](#)
- [snmp-server location](#)
- [snmp-server smux-port-disable](#)
- [snmp-server tcp-session](#)
- [snmp-server user](#)
- [snmp-server view](#)



---

## debug snmp-server

Use this command to display SNMP debugging information.

Use the `no` form of this command to stop displaying SNMP debugging information.

### Command Syntax

```
debug snmp-server
no debug snmp-server
```

### Parameters

None

### Default

By default, disabled.

### Command Mode

Exec and configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#debug snmp-server
```

---

## show running-config snmp

Use this command to display the SNMP running configuration.

### Command Syntax

```
show running-config snmp
```

### Parameters

None

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show running-config snmp
snmp-server view all .1 included
snmp-server community abc group network-admin
snmp-server enable snmp
```

---

# show snmp

Use this command to display the SNMP configuration, including session status, system contact, system location, statistics, communities, and users.

## Command Syntax

```
show snmp
```

## Parameters

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show snmp
SNMP Protocol:Enabled
sys Contact:
sys Location:

-----
Community Group/Access Context acl_filter
-----
public network-admin

-----
                                SNMP USERS
-----
User Auth Priv(enforce) Groups
-----

SNMP Tcp-session :Disabled
```

# show snmp community

Use this command to display SNMP communities.

## Command Syntax

```
show snmp community
```

## Parameters

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show snmp community
```

```
-----  
-----  
Community          Group/Access      view-name  
version  
-----  
-----  
test                network-operator  
testing             network-operator    ipi  
2c
```

[Table 22-66](#) explains the output fields.

Table 22-66: show snmp community fields

Entry	Description
Community	SNMP Community string.
Group/Access	Community group name.
View-name	Community view name.
Version	Community version.

---

# show snmp context

Use this command to display SNMP server contexts and associated groups.

## Command syntax

```
show snmp context
```

## Parameters

None

## Command Mode

Exec mode

## Applicability

This command is introduced in OcNOS-SP version 5.1 MR

## Example

```
OcNOS#show snmp context
-----
context                                groups
-----
ctx1                                   grp1,grp2
ctx2                                   grp3
```

# show snmp engine-id

Use this command to exhibit the SNMP engine identifier.

The SNMP engine identifier is a distinctive string employed to recognize the device for administrative purposes. The default engine-id is formulated using the MAC address, but an option for user-configured engine-id is also provided. The `show` command should be employed to retrieve information about the presently configured SNMP engine-id on the device.

## Command Syntax

```
show snmp engine-id
```

## Parameters

None

## Command Mode

Exec mode

## Applicability

This command was introduced prior to OcNOS version 1.3 and its display in the `show` output was enhanced in OcNOS version 6.3.2.

## Examples

Default SNMP engine-id:

```
#show snmp engine-id
SNMP ENGINE-ID Type: MAC address
SNMP ENGINE-ID : 80 00 1f 88 03 e8 c5 7a 1a 02 1c
```

User-Configured engine-id:

```
#show snmp engine-id
SNMP ENGINE-ID Type: User configured Text
SNMP ENGINE-ID Text: ipinfusion
SNMP ENGINE-ID : 80 00 1f 88 04 69 70 69 6e 66 75 73 69 6f 6e
```

[Table 22-67](#) explains the output fields.

Table 22-67: show snmp engine-ip fields

Entry	Description
SNMP ENGINE-ID: 80 00 1f 88 04 69 70 69 6e 66 75 73 69 6f 6e	The SNMP engine identifier is a distinct string utilized to uniquely recognize the device for administrative purposes.

# show snmp group

Use this command to display SNMP server groups and associated views.

## Command Syntax

```
show snmp group
```

## Parameters

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show snmp group
-----
community/user      group          version  Read-View  Write-view  Notify-view
-----
test                network-operator  2c/1    all        all        all
kedar               network-operator  3       all        none       all
tamil               network-operator  3       all        none       all
```

Table 22-68 explains the output fields.

Table 22-68: show snmp group output

Entry	Description
Community/User	Displays the access type of the user for which the notification is generated.
Group	The name of the SNMP group, or collection of users that have a common access policy.
Version	SNMP version number.
Read-View	A string identifying the read view of the group.  For further information on the SNMP views, use the show snmp view command.
Write-View	A string identifying the write view of the group.
Notify-View	A string identifying the notify view of the group.  The notify view indicates the group for SNMP notifications, and corresponds to the setting of the snmp-server group group-name version notify notify-view command.

# show snmp host

Use this command to display the SNMP trap hosts.

## Command Syntax

```
show snmp host
```

## Parameters

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show snmp host
-----
Host          Port    Version  Level    Type    SecName
-----
10.10.26.123  162    2c       noauth   trap    test
```

[Table 22-69](#) explains the output fields.

Table 22-69: Show snmp host output

Entry	Description
Host	The IP address of the SNMP host server.
Port	The port being used for SNMP traffic.
Version	SNMP version number.
Level	The security level being used.
Type	The type of SNMP object being sent.
SecName	Secure Name for this SNMP session.



---

# show snmp user

Use this command to display SNMP users and associated authentication, encryption, and group.

## Command Syntax

```
show snmp user
```

## Parameters

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show snmp user
```

```
SNMP USERS
```

User	Auth	Priv(enforce)	Groups
ntwadmin	MD5	AES	network-admin

```
#
```

[Table 22-70](#) explains the output fields.

Table 22-70: Show snmp user output

Entry	Description
User	The person attempting to use the SMNMP agent.
Auth	The secure encryption scheme being used.
Priv(enforce)	What enforcement privilege is being used (in this case, it is the Advance Encryption Standard).
Group	The group to which the user belongs.

---

## show snmp view

Use this command to display SNMP views.

### Command Syntax

```
show snmp view
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show snmp view
```

```
View : all  
OID : .1  
View-type : included
```

---

## snmp context

Use this command to associate the SNMP context with the VRF.

Use the `no` form of this command to remove the SNMP context association from VRF.

### Command Syntax

```
snmp context-name WORD
no snmp context-name
```

### Parameters

WORD	SNMP context name (Maximum 32 alphanumeric characters)
------	--

### Default

No default value is specified.

### Command Mode

Configure VRF mode

### Applicability

This command was introduced before OcNOS version 6.1.0.

### Examples

```
OcNOS#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
OcNOS(config)#ip vrf red
OcNOS(config-vrf)#snmp context-name context1
```

---

## snmp-server community

Use this command to create an SNMP community string and access privileges.

Use the `no` form of this command to remove an SNMP community string.

### Command Syntax

```
snmp-server community WORD (| (view VIEW-NAME version (v1 | v2c ) ( ro)) |  
(group (network-admin|network-operator)) |( ro) | (use-acl WORD) ) (vrf  
management|)  
  
no snmp-server community COMMUNITY-NAME (vrf management|)
```

### Parameters

WORD	Name of the community (Maximum 32 alphanumeric characters)
VIEW-NAME	Name of the snmp view (Maximum 32 alphanumeric characters)
version	Set community string and access privileges
v1	SNMP v1
v2c	SNMP v2c
ro	Read-only access
group	Community group
network-admin	System configured group for read-only
network-operator	System configured group for read-only(default)
ro	Read-only access
use-acl	Access control list (ACL) to filter SNMP requests
WORD	ACL name; maximum length 32 characters
management	Virtual Routing and Forwarding name

### Default

No default value specified.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal  
(config)#snmp-server community MyComm view MyView1 version v2c ro vrf  
management
```

---

## snmp-server community-map

Use this command to map the community name with context and SNMPv2 user.

Use `no` form of this command to remove the community mapping.

Note: Community can be mapped with one context and user.

### Command Syntax

```
snmp-server community-map WORD context WORD user WORD (vrf management|)
no snmp-server community-map WORD context WORD user WORD (vrf management|)
```

### Parameters

WORD	SNMP community name
context	SNMP context name
WORD	Context string
user	SNMP user name
WORD	User string
management	Virtual Routing and Forwarding name

### Command Mode

Configure mode

### Applicability

This command is introduced in OcNOS-SP version 5.1 MR.

### Examples

```
OcNOS(config)#snmp-server community-map test context ctx2 user testing vrf
management
```

---

## snmp-server contact

Use this command to set the system contact information for the device (`sysContact` object).

Use the `no` form of this command to remove the system contact information.

### Command Syntax

```
snmp-server contact (vrf management|) (TEXT|)
no snmp-server contact (vrf management|) (TEXT|)
```

### Parameters

<code>management</code>	Virtual Routing and Forwarding name
<code>TEXT</code>	System contact information; maximum length 1024 characters without spaces

### Default

No default value specified.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#snmp-server contact vrf management Irving@555-0150
```

---

## snmp-server context

Use this command to create SNMP context.

Use `no` form of this command to remove the context.

### Command Syntax

```
snmp-server context WORD (vrf management|)
no snmp-server context WORD (vrf management|)
```

### Parameters

context	SNMP context name
WORD	Context string (Maximum 32 alphanumeric characters)
management	Virtual Routing and Forwarding name

### Command Mode

Configure mode

### Applicability

This command is introduced in OcNOS version 5.1MR.

### Examples

```
OcNOS(config)#snmp-server context ctx1 vrf management
```

---

## snmp-server disable default

Use this command to disable default instance which is running on OcNOS device. After configuring this command user should not be able to enable default snmp instance. Use no form of this command to unset this after that only user should be able to configure default instance.

### Command Syntax

```
snmp-server disable-default
```

### Parameters

None

### Default

No default value specified.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 6.1.0.

### Examples

```
#configure terminal
(config)#snmp-server disable-default
```



---

## snmp-server enable snmp

Use this command to start the SNMP agent daemon over UDP.

Use the `no` form of this command to stop the SNMP agent daemon over UDP.

### Command Syntax

```
snmp-server enable snmp (vrf management|)
no snmp-server enable snmp (vrf management|)
```

### Parameters

management	Virtual Routing and Forwarding name
------------	-------------------------------------

### Default

No default value specified.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#snmp-server enable snmp vrf management
```

---

## snmp-server enable traps

Use this command to enable or disable SNMP traps and inform requests.

Note: For CMMD, Critical logs in the console are equivalent to Alert traps & Alert logs on the console is equivalent to critical trap in SNMP.

### Command Syntax

```
snmp-server enable traps (link(|linkDown|linkUp|include-interface-  
name)|snmp(|authentication)| mpls|pw|pwdelete|ospf|bgp|isis|vxlan|vrrp|ospf6)  
no snmp-server enable traps (link(|linkDown|linkUp|include-interface-  
name)|snmp(|authentication)| mpls|pw|pwdelete|ospf|bgp|isis|vxlan|vrrp|ospf6)
```

### Parameters

bgp	bgp notification trap
isis	isis notification trap
link	Module notifications enable
linkDown	IETF Link state down notification
linkUp	IETF Link state up notification
snmp	Enable RFC 1157 notifications
authentication	Send SNMP authentication failure notifications
mpls	mpls notification trap
mplsl3vpn	mpls-l3vpn notification trap
ospf	ospf notification trap
ospf6	ospf6 notification trap
pw	pw notification trap
pwdelete	pwdelete notification trap
rib	rib notification trap
rsvp	rsvp notification trap
vrrp	vrrp notification trap
vxlan	vxlan notification trap
linkDown	IETF link state down notification
linkup	IETF link state up notification
include-interface-name	Enable this option to include interface name in the Linkup/Linkdown trap's varbind

### Default

By default, SNMP server traps are enabled.

### Command Mode

Configure mode

## Applicability

This command was introduced before OcNOS version 1.3 and was updated in OcNOS version 4.0.

## Examples

```
(config)#snmp-server enable traps snmp
(config)#snmp-server enable traps mpls
(config)#snmp-server enable traps mpls13vpn
(config)#snmp-server enable traps rsvp
(config)#snmp-server enable traps ospf
(config)#snmp-server enable traps ospf6
(config)#snmp-server enable traps vrrp
(config)#snmp-server enable traps vxlan
(config)#snmp-server enable traps snmp authentication
```

---

## snmp-server engineID

Use this command to establish the SNMPv3 engine ID.

Use the no form of this command to remove the SNMPv3 engine ID.

### Command Syntax

```
snmp-server engineID ENGINE_ID_STR
no snmp-server engineID
```

### Parameters

ENGINE\_ID\_STR String of characters that uniquely identifies the SNMP engine ID.

### Default

By Default the SNMP Server Engine ID value is automatically generated using the MAC address.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 6.3.2.

### Examples

```
#configure terminal
(config)#snmp-server engineID ipinfusion
```

## snmp-server group

Use this command to create a SNMP group.

Use the `no` form of this command to remove the groups.

### Command syntax

```
snmp-server group WORD version (1|2c) (context (all|WORD)) (vrf management|)
snmp-server group WORD version 3 (auth|noauth|priv) (context (all|WORD)) (vrf
management|)
no snmp-server group WORD (context (all|WORD)) (vrf management|)
```

### Parameters

<code>WORD</code>	Specify the snmp group name (Maximum 32 alphanumeric characters)
<code>version</code>	SNMP Version
<code>1</code>	SNMP v1
<code>2c</code>	SNMP v2c
<code>3</code>	SNMP v3 security level
<code>noauth</code>	No authentication and no privacy (noAuthNoPriv) security model: messages transmitted as clear text providing backwards compatibility with earlier versions of SNMP
<code>auth</code>	Authentication and no privacy (authNoPriv) security model: use message digest algorithm (MD5) or Secure Hash Algorithm (SHA) for packet authentication; messages transmitted in clear text
<code>priv</code>	Authentication and privacy (authPriv) security model: use authNoPriv packet authentication with Data Encryption Standard (DES) Advanced Encryption Standard (AES) for packet encryption
<code>context</code>	SNMP context name
<code>WORD</code>	SNMP context string (Maximum 32 alphanumeric characters)
<code>all</code>	All context name's allowed for this group.
<code>management</code>	Virtual Routing and Forwarding (VRF) name

### Default

None

### Command Mode

Configure mode

### Applicability

This command is introduced in OcNOS-SP version 5.1 MR.

### Examples

```
OcNOS#con t
OcNOS(config)#snmp-server context ctx1 vrf management
OcNOS(config)#snmp-server group grp1 version 3 auth context ctx1 vrf
management
```

```
OcNOS(config)#snmp-server group grp3 version 2c context ctx2 vrf management
```

## snmp-server host

Use this command to configure an SNMP trap host. An SNMP trap host is usually a network management station (NMS) or an SNMP manager.

Use the `no` form of this command to remove an SNMP trap host.

Note: The maximum number of SNMP trap hosts is limited to 8.

### Command Syntax

```
snmp-server host (A.B.C.D | X:X::X:X | HOSTNAME) ((traps version(( (1 | 2c) WORD ) | (3 (noauth | auth | priv) WORD))) | (informs version ((2c WORD ) | (3 (noauth | auth | priv) WORD)))) (udp-port <1-65535>) (vrf management|)

snmp-server host (A.B.C.D | X:X::X:X | HOSTNAME) WORD (udp-port <1-65535>) (vrf management|)

snmp-server host (A.B.C.D | X:X::X:X | HOSTNAME) (version(( (1 | 2c) WORD ) | (3 (noauth | auth | priv) WORD))) (udp-port <1-65535>) (vrf management|)

no snmp-server host (A.B.C.D|X:X::X:X|HOSTNAME) (vrf management|)
```

### Parameters

A.B.C.D	IPv4 address
X:X::X:X	IPv6 address
HOSTNAME	DNS host name
WORD	SNMP community string or SNMPv3 user name (Maximum 32 alphanumeric characters)
informs	Send notifications as informs
version	SNMP Version. Default notification is traps
<1-65535>	Host UDP port number; the default is 162
management	Virtual Routing and Forwarding name
traps	Send notifications as traps
version	Version
1	SNMP v1
2c	SNMP v2c
WORD	SNMP community string (Maximum 32 alphanumeric characters)
3	SNMP v3 security level
noauth	No authentication and no privacy (noAuthNoPriv) security model: messages transmitted as clear text providing backwards compatibility with earlier versions of SNMP
auth	Authentication and no privacy (authNoPriv) security model: use message digest algorithm 5 (MD5) or Secure Hash Algorithm (SHA) for packet authentication; messages transmitted in clear text
priv	Authentication and privacy (authPriv) security model: use authNoPriv packet authentication with Data Encryption Standard (DES) Advanced Encryption Standard (AES) for packet encryption
WORD	SNMPv3 user name

## Default

The default SNMP version is v2c and the default UDP port is 162.Simple Network Management Protocol.

## Command Mode

Configure mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#configure terminal
(config)#snmp-server host 10.10.10.10 traps version 3 auth MyUser udp-port 512
vrf management
```



---

## snmp-server location

Use this command to set the physical location information of the device (`sysLocation` object).

Use the `no` form of this command to remove the system location information.

### Command Syntax

```
snmp-server location (vrf management|) (TEXT|)
no snmp-server location (vrf management|) (TEXT|)
```

### Parameters

management	Virtual Routing and Forwarding name
TEXT	Physical location information; maximum length 1024 characters

### Default

No system location string is set.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#snmp-server location vrf management Bldg. 5, 3rd floor, northeast
```

---

## snmp-server smux-port-disable

Use this CLI to disable the SMUX open port.

### Command Syntax

```
snmp-server smux-port-disable
```

### Parameters

None

### Default

None

### Command Mode

Configure mode

### Applicability

This command is introduced in OcNOS version 5.1 release.

### Examples

```
#configure terminal
#snmp-server smux-port-disable
```

---

## snmp-server tcp-session

Use this command to start the SNMP agent daemon over TCP.

Use the `no` form of this command to close the SNMP agent daemon over TCP.

### Command Syntax

```
snmp-server tcp-session (vrf management|)
no snmp-server tcp-session (vrf management|)
```

### Parameters

management	Virtual Routing and Forwarding name
------------	-------------------------------------

### Default

By default, snmp server tcp session is disabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#snmp-server tcp-session vrf management
```

---

## snmp-server user

Use this command to create an SNMP server user.

Use the `no` form of this command to remove an SNMP server user.

### Command Syntax

```
snmp-server user WORD ((network-operator|network-admin| WORD|) ((auth (md5 | sha
) (encrypt|) AUTH-PASSWORD) ((priv (des | aes) PRIV-PASSWORD) |) |) (vrf
management|)

no snmp-server user USER-NAME (vrf management|)
```

### Parameters

WORD	Specify the snmp user name (Min 5 to Max 32 alphanumeric characters)
network-operator network-admin	Name of the group to which the user belongs.
WORD	User defined group-name
auth	Packet authentication type
md5	Message Digest Algorithm 5 (MD5)
sha	Secure Hash Algorithm (SHA)
AUTH-PASSWORD	Authentication password; length 8-32 characters
priv	Packet encryption type ("privacy")
des	Data Encryption Standard (DES)
aes	Advanced Encryption Standard (AES)
PRIV-PASSWORD	Encryption password; length 8-33 characters
management	Virtual Routing and Forwarding name
encrypt	Specify authentication-password and/or privilege-password in encrypted form. This option is provided for reconfiguring a password using an earlier encrypted password that was available in running configuration display or get-config payload. Users are advised not to use this option for entering passwords generated in any other method.

### Default

By default, snmp server user word is disabled

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

**Examples**

```
#configure terminal
(config)#snmp-server user Fred auth md5 J@u-b;l2e`n,9p_ priv des
t41VVb99i8He{Jt vrf management
```

---

## snmp-server view

Use this command to create or update a view entry

Use the `no` form of this command to remove a view entry.

**Note:** OIDs to be excluded or included need to be specifically mentioned while configuring the SNMP view. Only when the OIDs are included will they be displayed in SNMP-Walk. When an OID is excluded, other OIDs must be explicitly included for the system to function.

### Command Syntax

```
snmp-server view VIEW-NAME OID-TREE (included | excluded) (vrf management|)
no snmp-server view VIEW-NAME (vrf management|)
```

### Parameters

VIEW-NAME	Name of the snmp view (Maximum 32 alphanumeric characters)
OID-TREE	Object identifier of a subtree to include or exclude from the view; specify a text string consisting of numbers and periods, such as 1.3.6.2.4
included	Include <code>OID-TREE</code> in the SNMP view
excluded	Exclude <code>OID-TREE</code> from the SNMP view
management	Virtual Routing and Forwarding name

### Default

By default, `snmp-server view VIEW-NAME OID-TREE` is disabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

The following example creates a view named `myView3` that excludes the `snmpCommunityMIB` object (1.3.6.1.6.3.18).

```
#configure terminal
(config)#snmp-server view myView3 1.3.6.1.6.3.18 excluded vrf management
```

## CHAPTER 23 Software Monitoring and Reporting

---

This document describes software watchdog and reporting related commands.

- [clear cores](#)
- [copy core](#)
- [copy techsupport](#)
- [feature software-watchdog](#)
- [show bootup-parameters](#)
- [show cores](#)
- [show running-config watchdog](#)
- [show software-watchdog status](#)
- [show system log](#)
- [show system login](#)
- [show system reboot-history](#)
- [show system resources](#)
- [show system uptime](#)
- [show techsupport](#)
- [show techsupport status](#)
- [software-watchdog](#)
- [software-watchdog keep-alive-time](#)

---

## clear cores

Use this clear command to delete the core files present in /var/log/crash/cores

### Syntax

```
clear cores (|WORD)
```

### Parameters

WORD	Core file name
------	----------------

### Default

NA

### Command Mode

Executive Mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show cores
Core location :/var/log/crash/cores
Core-File-Name
-----
core_hostpd.9581_20190324_222313_signal_11.gz
#clear cores core_hostpd.9581_20190324_222313_signal_11.gz
#show cores
Core location :/var/log/crash/cores
Core-File-Name
-----
#
```



# copy core

Use this command to copy the core file to another file.

The core filename is in the form: core\_PROCESSNAME.PROCID\_YYMMDD\_HHMMSS\_signal\_SIGNALNUM.gz

## Syntax

```
copy core FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL) (vrf
(NAME|management) |)
```

## Parameters

core	Copy Crash core files to remote location. Core file location: /var/log/crash/cores/
FILE	Source file name
TFTP-URL	Destination: tftp: [//server[:port]] [/path]
FTP-URL	Destination: ftp: [//server] [/path]
SCP-URL	Destination: scp: [//server] [/path]
SFTP-URL	Destination: sftp: [//server] [/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

## Default

NA

## Command Mode

Privileged EXEC

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
# copy core core_hostpd.9581_20190324_222313_signal_11.gz scp scp://10.12.16.17/home/
core core_hostpd.9581_20190324_222313_signal_11.gz vrf management
Enter Username:root
Enter Password:
  % Total      % Received % Xferd  Average Speed   Time    Time       Time  Current
                             Dload  Upload  Total  Spent  Left  Speed
100 681k    0      0    0 681k      0 3588k  --:--:--  --:--:--  --:--:-- 3588k
100 681k    0      0    0 681k      0 3588k  --:--:--  --:--:--  --:--:-- 3588k
Copy Success
```

---

## copy techsupport

Use this command to copy the contents of a compressed techsupport file (tar.gz) to another file.

The default filename is in the form: tech\_support\_YYYY\_MMM\_DD\_HH\_MM\_SS.tar.gz.

### Syntax

```
copy (log|techsupport) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL)
(vrf (NAME|management) |)
```

### Parameters

log	Log file storage; on Linux this refers to /var/log/
techsupport	Tech support file storage; on Linux this refers to /var/log/
FILE	Source file name
TFTP-URL	Destination: tftp: [//server[:port]] [/path]
FTP-URL	Destination: ftp: [//server] [/path]
SCP-URL	Destination: scp: [//server] [/path]
SFTP-URL	Destination: sftp: [//server] [/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

### Default

NA

### Command Mode

Privileged EXEC

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#copy techsupport tech_support_23_Feb_2019_18_27_00.tar.gz scp scp://10.12.16.17/home/
tech_support_23_Feb_2019_18_27_00.tar.gz vrf management
```

```
Enter Username:root
Enter Password:
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 72368 0 0 0 72368 0 147k --:-- --:-- --:-- 147k
100 72368 0 0 0 72368 0 147k --:-- --:-- --:-- 147k
Copy Success
#
```

---

## feature software-watchdog

Use this command to enable software watchdog functionality for all OcNOS modules. This feature is enabled by default.

Use the `no` form of this command to disable software watchdog functionality.

### Command Syntax

```
feature software-watchdog
no feature software-watchdog
```

### Parameter

None

### Default

By default, software watchdog is enabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
#(config)feature software-watchdog
```

---

## show bootup-parameters

Use this command to show OcNOS kernel bootup parameters.

### Command Syntax

```
show bootup-parameters
```

### Parameter

None

### Command Mode

Execution mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show bootup-parameters
BOOT_IMAGE=/boot/vmlinuz-3.16.7-g490411a-ec-as7712-32x root=UUID=317567fc-
b69e-4
5d9-ab4e-fa1d9e57b
703 console=ttyS1,115200n8 ro
```

# show cores

Use this command to list core files in the system or to display information about a given core file.

When cmlsh logged in via non-root user crashes, core files will not get generated. User can further debug the issue based on CLI-history and logs from /var/log/messages.

## Command Syntax

```
show cores (|WORD details)
```

## Parameter

WORD	Core file name
------	----------------

## Command Mode

Execution mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#sh cores
Core location :/var/log/crash/cores
Core-File-Name
-----
core_nsm.683_20191110_103611_signal_5.gz
core_nsm.712_20191107_171803_signal_11.gz
core_nsm.684_20191112_054937_signal_5.gz
core_yangcli.5695_20191107_171715_signal_11.gz
#
```

Table 23-71 explains the output fields.

Table 23-71: show cores fields

Entry	Description
Core-File-Name	Core dump file name.

---

## show running-config watchdog

Use this command to display watchdog configurations.

### Command Syntax

```
show running-config watchdog
```

### Parameters

None

### Command Mode

Privileged EXEC

### Applicability

This command is introduced in OcNOS-SP version 5.0.

### Example

```
OcNOS#sh running-config watchdog
software-watchdog keep-alive-time 300
```

---

## show software-watchdog status

Use this command to display the software watchdog status for each OcNOS module.

### Command Syntax

```
show software-watchdog status
show software-watchdog status detail
```

### Parameter

None

### Command Mode

Execution mode

### Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.4.

### Examples

```
#show software-watchdog status
Software Watchdog timeout in seconds : 60
Process name          Watchdog status
=====
nsm                    Enabled
ripd                   Enabled
ripngd                 Enabled
ospfd                  Enabled
ospf6d                 Enabled
isis                   Enabled
hostpd                 Enabled
ldpd                   Enabled
rsvpd                  Enabled
mribd                  Enabled
pimd                   Enabled
authd                  Enabled
mstpd                  Enabled
imi                    Enabled
onmd                   Enabled
HSL                    Enabled
oamd                   Enabled
vlogd                  Enabled
vrrpd                  Enabled
ndd                    Enabled
ribd                   Enabled
bgpd                   Enabled
l2mribd                Enabled
lagd                   Enabled
sflow                  Enabled
```

```
cmld          Enabled
cmmd          Enabled
```

```
#show software-watchdog status detail
Software Watchdog timeout in seconds : 60
```

Process Name	Watchdog Status	Process Status	Disconnect Count	Connect Count	Last Restart Reason
nsm	Enabled	Running	0	1	Fresh bootup
ripd	Enabled	Running	0	1	Fresh bootup
ripngd	Enabled	Running	0	1	Fresh bootup
ospfd	Enabled	Running	0	1	Fresh bootup
ospf6d	Enabled	Running	0	1	Fresh bootup
isisd	Enabled	Running	0	1	Fresh bootup
hostpd	Enabled	Running	0	1	Fresh bootup
ldpd	Enabled	Running	0	1	Fresh bootup
rsvpd	Enabled	Running	0	1	Fresh bootup
mribd	Enabled	Running	0	1	Fresh bootup
pimd	Enabled	Running	0	1	Fresh bootup
authd	Enabled	Running	0	1	Fresh bootup
mstpd	Enabled	Running	0	1	Fresh bootup
imi	Enabled	Running	0	1	Fresh bootup
onmd	Enabled	Running	0	1	Fresh bootup
HSL	Enabled	Running	0	1	Fresh bootup
oamd	Enabled	Running	0	1	Fresh bootup
vlogd	Enabled	Running	0	1	Fresh bootup
vrripd	Enabled	Running	0	1	Fresh bootup
ndd	Enabled	Running	0	1	Fresh bootup
ribd	Enabled	Running	0	1	Fresh bootup
bgpd	Enabled	Running	0	1	Fresh bootup
l2mribd	Enabled	Running	0	1	Fresh bootup
lagd	Enabled	Running	0	1	Fresh bootup
sflow	Enabled	Running	0	1	Fresh bootup
cmld	Enabled	Running	0	1	Fresh bootup
cmmd	Enabled	Running	0	1	Fresh bootup

Table 23-72 explains the output fields.

Table 23-72: show software-watchdog status output fields

Field	Description
Process Name	The name of a protocol module.
Watchdog Status	Status of a protocol module (Enabled or Disabled).
Process Status	Status of the protocol module Running/Not-running).
Disconnect Count	Number of times the protocol module disconnected from monitoring module.



Table 23-72: show software-watchdog status output fields (Continued)

Field	Description
Connect Count	Number of times the protocol module connected to monitoring module.
Last Restart Reason	Reason why a module disconnected from monitoring module.

---

## show system log

Use this command to display the system's log file.

### Command Syntax

```
show system log
```

### Parameters

None

### Command Mode

Execution mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show system log
Syslog           : enabled      File Name      : /var/log/messages
Oct 18 18:10:18 localhost rsyslogd: [origin software="rsyslogd"
swVersion="8.4.2
" x-pid="541" x-info="http://www.rsyslog.com"] start
Oct 18 18:10:18 localhost systemd[1]: Started Apply Kernel Variables.
Oct 18 18:10:18 localhost systemd[1]: Started Create Static Device Nodes in /
dev
.
Oct 18 18:10:18 localhost systemd[1]: Starting udev Kernel Device Manager...
Oct 18 18:10:18 localhost systemd[1]: Started udev Kernel Device Manager.
Oct 18 18:10:18 localhost systemd[1]: Starting Copy rules generated while the
ro
ot was ro...
Oct 18 18:10:18 localhost systemd[1]: Starting LSB: Set preliminary keymap...
Oct 18 18:10:18 localhost systemd[1]: Started Copy rules generated while the
roo
t was ro.
Oct 18 18:10:18 localhost nfs-common[163]: Starting NFS common utilities:.
Oct 18 18:10:18 localhost systemd[1]: Found device /dev/ttyS0.
Oct 18 18:10:18 localhost systemd[1]: Found device 16GB_SATA_Flash_Drive
OcNOS-CONFIG.
Oct 18 18:10:18 localhost systemd[1]: Starting File System Check on /dev/disk/
by
-label/OcNOS-CONFIG...
Oct 18 18:10:18 localhost systemd[1]: Starting system-ifup.slice.
Oct 18 18:10:18 localhost systemd-fsck[217]: OcNOS-CONFIG: clean, 85/128016
file
s, 27057/512000 blocks
Oct 18 18:10:18 localhost systemd[1]: Created slice system-ifup.slice.
--More--
```

[Table 23-73](#) explains the output fields.

**Table 23-73: show system log fields**

Entry	Description
Syslog	Status of the protocol (enabled or disabled).
File Name	Specifies the name of the system log files that you configured.

---

## show system login

Use this command to display the system's login history.

### Command Syntax

```
show system login
```

### Parameters

None

### Command Mode

Execution mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show system login
eric      ttyS0      Wed Oct 19 18:31      still logged in
takayuki  ttyS0      Wed Oct 19 18:14 - 18:25  (00:10)
girish    ttyS0      Wed Oct 19 16:46 - 17:01  (00:14)
```

```
wtmp begins Wed Oct 19 16:46:18 2016
```

# show system reboot-history

Use this command to show the OcNOS reboot history.

## Command Syntax

```
show system reboot-history
```

## Parameters

None

## Command Mode

Execution mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show system reboot-history
#) On Thu Jun 6 06:16:03 2013
Reason: Reset Requested by Active User
Service: NONE
#) On Thu Jun 6 06:21:30 2015
Reason: Reset Requested due to Process Crash
Service: nsm
#
```

[Table 23-73](#) explains the output fields.

Table 23-74: show system reboot-history fields

Entry	Description
Reason	Displays the reason, why the fields are reset.
Service	Name of the service in this protocol.

# show system resources

Use this command to display the system’s current resources.

## Command Syntax

```
show system resources (iteration <1-5>|)
```

## Parameters

<1-5>                      The number of times to check the resources before they are displayed.

## Command Mode

Execution mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
DELL-6K3#show system resources
load average: 0.11, 0.08, 0.05
Tasks: 113 total,   1 running, 112 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.1 us,  0.4 sy,  0.0 ni, 98.5 id,   0.0 wa,   0.0 hi,   0.0 si,   0.0
st
KiB Mem:   8181040 total,   736124 used,  7444916 free,   133012 buffers

#show system resources iteration 5
load average: 0.03, 0.06, 0.05
Tasks: 112 total,   3 running, 109 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.0 us,  0.6 sy,  0.0 ni, 98.4 id,   0.0 wa,   0.0 hi,   0.0 si,   0.0
st
KiB Mem:   8181040 total,   736608 used,  7444432 free,   132976 buffers
KiB Swap:         0 total,         0 used,         0 free.  252416 cached Mem
```

[Table 23-75](#) explains the output fields.

**Table 23-75: show system resource fields**

Entry	Description
Load Average	Number of processes that are running. The average reflects the system load the past 1, 5, and 15 minutes.
Tasks	Number of processes in the system and how many processes are actually running when the command is issued.
CPU	Displays the CPU utilization information for processes on the device.

Table 23-75: show system resource fields

Entry	Description
KiB Mem	<p>The memory field (Mem) shows the virtual memory used by processes. The value in the memory field is in KB and MB, and is broken down as follows:</p> <p>Total: The total amount of available virtual memory, in kibibytes (KiBs).</p> <p>Used:The total amount of used virtual memory, in kibibytes (KiBs).</p> <p>Free: The total amount of free virtual memory, in kibibytes (KiBs)</p> <p>Buffers: The size of the memory buffer used to hold data recently called from disk.</p>
KiB Swap	<p>The Swap field shows the total swap space available and how much is unused and is broken down as follows:</p> <p>Total: The total amount of available swap memory, in kibibytes (KiBs).</p> <p>Used: The total amount of used swap memory, in kibibytes (KiBs).</p> <p>Free: The total amount of free swap memory, in kibibytes (KiBs).</p> <p>Cache Memory: Memory that is not associated with any program and does not need to be swapped before being reused.</p>

# show system uptime

Use this command to display how lone the system has been up and running.

## Command Syntax

```
show system uptime
```

## Parameters

None

## Command Mode

Execution mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
DELL-6K3#show system uptime
19:10:22 up 1 day, 1:01, 1 user, load average: 0.08, 0.05, 0.05
```

[Table 23-76](#) explains the output fields.

Table 23-76: show system uptime fields

Entry	Description
Time and up	Current time, in the local time zone, and how long the router or switch has been operational.
Users	Number of users logged in to the router or switch.
Load Average	Number of processes that are running. The average reflects the system load the past 1, 5, and 15 minutes.



---

## show techsupport

Use this command to collect system data for technical support to save support information in a compressed (.gz) file.

The default file path is `/var/log/` and the filename is `tech_support_YYYY_MMM_DD_HH_MM_SS.tar.gz`.

The filename given can be the same as another file; to distinguish them, each of the filenames are appended with a date and timestamp.

If a `show techsupport` command execution is in progress, any newly issued `show techsupport` commands are ignored.

If a `show techsupport` command is executing, and the `show running-config` command is given, the displayed information is copied from the `show techsupport` command.

### Command Syntax

```
show techsupport
({all|authd|bgp|cmmd|hostpd|hsl|imi|isis|l2mribd|lag|ldp|mribd|mstp|nd|nsm|oam|onm|ospf|ospf6|pcep|pim|ptp|rib|rip|ripng|rsvp|sflow|synce|vrrp})
```

### Parameters:

all	ALL Related Information
authd	AUTHD Related Information
bgp	BGP Related Information
cmmd	CMMD Related Information
hostpd	HOSTP Related Information
hsl	HSL Related Information
imi	IMI Related Information
isis	ISIS Related Information
l2mribd	L2MRIB Related Information
lag	LAG/LACP Related Information
ldp	LDP Related Information
mribd	MRIB Related Information
mstp	MSTP Related Information
nd	NDD Related Information
nsm	NSM Related Information
oam	BFD Related Information
onm	ONM/LLDP Related Information
ospf	OSPF Related Information
ospf6	OSPF6 Related Information
pcep	PCEP Related Information
pim	PIM Related Information
ptp	PTP Related Information
rib	RIB Related Information

rip	RIP Related Information
ripng	RIPNG Related Information
rsvp	RSVP Related Information
sflow	SFLOW Related Information
synce	SYNCE Related Information
vrrp	VRRP Related Information

### Default

The default file path for show techsupport is /var/log/.

### Command Mode

Privileged EXEC

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show techsupport all
#show techsupport bgp
#show techsupport bgp isis
```

---

## show techsupport status

Use this cli to view the status of `show techsupport` CLI to generate techsupport archive.

### Command Syntax

```
show techsupport status
```

### Parameters

None

### Command Mode

Privileged EXEC

### Applicability

This command was introduced before OcNOS-SP version 4.2.

### Example

```
#show techsupport status
Tech Support Command Execution Is Complete
##Generated Tech Support File-list
/var/log/OcNOS_tech_support_18_Jun_2021_10_01_38.tar.gz
Tar File is generated at /var/log and file name begins with
'OcNOS_tech_support'
```

---

## software-watchdog

Use this command to enable the software watchdog feature for an OcNOS module.

Use the `no` form of this command to disable the software watchdog feature.

### Command Syntax

```
software-watchdog (nsm|authd|bgpd|cmld|hostpd|imi|isisd|lagd|l2mribd|  
mstpd|mribd|ndd|oamd|onmd|ospfd|ospf6d|pimd|ribd|ripd|ripngd|sflow|vlogd|vrrpd|  
ldpd|rsvpd|hs1|cmmd)  
  
no software-watchdog (nsm|authd|bgpd|cmld|hostpd|imi|isisd|lagd|l2mribd|  
mstpd|mribd|ndd|oamd|onmd|ospfd|ospf6d|pimd|ribd|ripd|ripngd|sflow|vlogd|vrrpd|  
ldpd|rsvpd|hs1|cmmd)
```

### Parameters

nsm	NSM module
authd	AUTH module
bgpd	BGP module
cmld	CML module
hostpd	HOSTP module
imi	IMI module
isisd	ISIS module
lagd	LAG module
l2mribd	L2MRIB module
mstpd	MSTP module
mribd	MRIB module
ndd	NDD module
oamd	OAM module
onmd	ONM module
ospfd	OSPF module
ospf6d	OSPF6 module
pimd	PIM module
ribd	RIB module
ripd	RIP module
ripngd	RIPNG module
sflow	SFLOW module
vlogd	VLOG module
vrrpd	VRRP module
ldpd	LDP module
rsvpd	RSVP module
hs1	HSL module

cmmnd

CMM module

**Default**

By default, software watchdog is enabled.

**Command Mode**

Configure mode

**Applicability**

This command was introduced before OcNOS version 1.3.

**Examples**

```
#configure terminal
#(config)no software-watchdog imi
#(config)software-watchdog nsm
```

---

## software-watchdog keep-alive-time

Use this command to set the software watchdog keep-alive time interval in seconds. The default keep-alive time interval is 60 seconds.

Use the `no` form of this command to set default keep-alive time interval.

### Command Syntax

```
software-watchdog keep-alive-time <30-1800>
no software-watchdog keep-alive-time
```

### Parameters

<30-1800>	Keep-alive time interval in seconds
-----------	-------------------------------------

### Default

By default, software watchdog is enabled and the keep-alive time interval is 60 seconds.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
#(config)software-watchdog keep-alive-time 100
```

## CHAPTER 24 Syslog

---

This chapter is a reference for the `syslog` commands.

Linux applications use the `syslog` utility to collect, identify, time-stamp, filter, store, alert, and forward logging data. The `syslog` utility can track and log all manner of system messages from informational to extremely critical. Each system message sent to a `syslog` server has two descriptive labels associated with it:

- The function (facility) of the application that generated it. For example, an application such as `mail` and `cron` generates messages with a facility names “mail” and “cron”.
- Eight degrees of severity (numbered 0-7) of the message which are explained in [Table 24-77](#).

This chapter contains these commands:

- [clear logging logfile](#)
- [feature rsyslog](#)
- [log syslog](#)
- [logging console](#)
- [logging level](#)
- [logging logfile](#)
- [logging monitor](#)
- [logging remote facility](#)
- [logging remote server](#)
- [logging timestamp](#)
- [show logging](#)
- [show logging last](#)
- [show logging logfile](#)
- [show logging logfile last-index](#)
- [show logging logfile start-seqn end-seqn](#)
- [show logging logfile start-time end-time](#)
- [show running-config logging](#)

## Syslog Severities

In the example log entries in [Table 24-77](#), the prefixes are removed. For example, this is a complete log entry with the prefix:

```
2020 Apr 12 11:20:27.612 : 17U-18U : PSERV : MERG : !!! hsl Module crashed, System
reboot halted as it rebooted continuously 2 times
```

This is the same log entry without the prefix:

```
hsl Module crashed, System reboot halted as it rebooted continuously 2 times
```

Table 24-77: Syslog severities (Sheet 1 of 2)

Severity Level	Keyword	Description
0	emergency	<p>The whole system is unusable and needs operator intervention to recover. If only a particular port or component is unusable, but the system as a whole is still usable it is not categorized at an emergency level.</p> <p>Examples of this type of message:</p> <pre>Output Power of PSU XX (psu_no) XX Watt] has exceeded Maximum Output Power Limit[XX Watt] OSPF Initialization failed.</pre>
1	alert	<p>The operator needs to act immediately or the system might go into emergency state. The system or one of its component's functionality might be critically affected.</p> <p>Examples of this type of message:</p> <pre>Temperature of sensor is (curr_temp)C. It is nearing Emergency Condition. OSPF has exceed lsdb limit OSPF Detected router with duplicate router ID [ID]</pre>
2	critical	<p>A critical system event happened which requires the operator's attention. The event might not require immediate action, but this event can affect functionality or behavior of a system component.</p> <p>Examples of this type of message:</p> <pre>OSPF Neighbor session went down. Interface %s changed state to down</pre>
3	error	<p>An error event happened which does not require immediate attention. This log message provides details about error conditions in the system or its components which you can use to troubleshoot problems.</p> <p>These events are not logged directly even if the logging level is set to include this level. You also need to enable the protocol debug filters (such as <code>debug ospf all</code>).</p> <p>Examples of this type of message:</p> <pre>Device i2c bus open error.!!! [DECODE] Attr ASPATH: Invalid AS Path value. OSPF MD5 authentication error</pre>



**Table 24-77: Syslog severities (Sheet 2 of 2)**

Severity Level	Keyword	Description
4	notification	<p>Notifications about important system and protocol events to assure the operator that the system is running properly. If a critical/alert condition has happened and has been corrected, that is also logged at this level.</p> <p>Examples of this type of message:</p> <pre>OSPF Received link up for interface: xe1 OSPF neighbour [10.1.1.1] Status change Exstart -&gt; Exchange Interface %s changed state to UP</pre>
5	informational	<p>Detailed informational events happening across the system and protocol modules. These events are not necessarily important and are useful only to find details about the functionality being executed in the system and its components. Some of these events might be periodic events like hello or keep alive messages along with packet dumps. Also, this level includes logs for control packets that are ignored and do not impact the protocol states.</p> <p>IP Infusion Inc. recommends to use proper debug filters to log only relevant events and switch off other events; otherwise the logs can get verbose. For example:</p> <pre>debug ospf all no debug ospf packet hello</pre> <p>The above enables all OSPF debugging, but disables the periodic hello messages.</p> <p>Examples of this type of message:</p> <pre>Successfully added dynamic neighbour [DECODE] KAlive: Received! [FSM] Ignoring Unsupported event &lt;EVENT&gt; in state &lt;STATE&gt; Unknown ICMP packet type" OSPF RECV[%s]: From %r via %s: Version number mismatch OSPF RECV[%s]: From %r via %s: Network address mismatch</pre>
6	debug informational	Developer notification events that might not be readable by an operator. However these logs are useful for debugging by a developer and if required, this level needs to be enabled and provided to technical support for analysis.
7	debug detailed	Developer notification events that might not be readable by an operator. However these logs are useful for debugging by a developer and if required, this level needs to be enabled and provided to technical support for analysis.

## Log File Rotation

Log rotation is important to maintain the stability of the device, because the larger log files are difficult to manipulate and file system would run out of space. The solution to this common problem is log file rotation.

Log rotation is scheduled to happen for every 5 minutes, here the log file size is used as the condition to perform rotation.

Log rotate operation creates a backup of the current log file, and clears the current log file content. Also these rotated log files are compressed to save disk space. Excluding the current log file, four backup files are maintained in the system, and the older logs are removed as part of the rotation operation.

Default log file `/var/log/messages` rotated, if the size is greater than 100 MB. The following are the rotated log files generated in the path `/var/log`

```
root@host:/var/log# ls messages*
messages  messages.1  messages.2.gz  messages.3.gz  messages.4.gz
```

Manually configured log file `/log/LOG1` gets rotated, if its size is greater than configured size. Here `LOG1` is the manually configured using the command `logging logfile <filename>` and the log file size in bytes can be configured using the command `logging logfile LOG1 <severity> size <4096-419430400>`

```
(config)#logging logfile LOG1 7 size 4096
```

Here configured logging file `/log/LOG1` is rotated if the size is greater than 4096 bytes. The following are the rotated log files generated in the path `/log`

```
root@host:/log# ls LOG*
LOG1  LOG1.1  LOG1.2.gz  LOG1.3.gz  LOG1.4.gz
```

---

## clear logging logfile

Use this command to clear the existing contents of the configured logging logfile.

**Note:** If the name of the configured logging log file is “mylogfile”, this command clears only the log file mylogfile. But the other rotated or compressed log files are untouched.

### Command Syntax

```
clear logging logfile
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Executive mode

### Applicability

This command was introduced before OcNOS-SP version 3.0.

### Example

```
#clear logging logfile
```

---

## feature rsyslog

Use this command to enable the rsyslog server.

Use the `no` form of this command to disable the rsyslog server.

### Command Syntax

```
feature rsyslog vrf (management|)
no feaature rsyslog vrf (management|)
```

### Parameters

<code>management</code>	Virtual Routing and Forwarding name
-------------------------	-------------------------------------

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#feature rsyslog vrf management
```

---

## log syslog

Use this command to begin logging to the system log and set the level to debug.

Syslog enables centrally logging and analyzing of configuration events and system error messages. This helps monitor interface status, security alerts, and CPU process overloads. It also allows real-time capturing of client debug sessions. The command instructs the `VLOGD` daemon to forward all PVR debug output from all active `terminal monitor` sessions to the syslog file.

Use the `no` parameter to disable logging to the system log.

### Command Syntax

```
log syslog
no log syslog
```

### Parameters

None

### Default

No default value is specified

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#log syslog
```

---

## logging console

Use this command to set the severity level that a message must reach before the messages is sent to the console. The severity levels are from 0 to 7 as shown in [Table 24-77](#).

Use the command `logging console disable` to disable logging console messages.

Use the `no` form of this command to remove logging console configuration and return to the default severity level.

Note: Below message will be displayed if console severity is set to 6 or 7:

% Warning : If debug volume is huge it can degrade system performance and makes console to be non-responsive

Note: For CMMD, Critical logs in the console are equivalent to Alert traps & Alert logs on the console is equivalent to critical trap in SNMP.

### Command Syntax

```
logging console (<0-7>|)
logging console disable
no logging console
```

### Parameters

<0-7>                      Maximum logging level for console messages as shown in [Table 24-77](#).

Note: Setting the level above 5 might affect performance and is not recommended in a production network.

disable                    Disables logging console

### Default

If not specified, the default logging level is 2 (Critical).

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3 and the command `logging console disable` was introduced in the OcNOS-SP version 5.1.

### Example

```
#configure terminal
(config)#logging console 6
(config)#commit
(config)#logging console disable
(config)#commit
```

## logging level

Use this command to set the severity level that a message for a specific process must reach before the messages is logged. The severity levels are from 0 to 7 as shown in [Table 24-77](#). Logging happens for the messages less than or equal to the configured severity level.

Use the `no` form of this command to disable logging messages.

Note: Default log level is 2 to report Emergency-0, Alert-1 and Critical-2 level events.

### Command Syntax

```
logging level (all|auth|bgp|dvmp|hostp|hsl|isis|l2mrib|lcp|lagd|ldp|mrib|
mstp|ndd|nsm|onm|ospf|ospf6|pim|pon|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow
|vrrp) <0-7>

no logging level (all|auth|bgp|dvmp|hostp|hsl|isis|l2mrib|lcp|lagd|ldp|mrib|
mstp|ndd|nsm|onm|ospf|ospf6|pim|pon|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow
|vrrp)
```

### Parameters

all	All messages
auth	Auth messages
bgp	BGP messages
dvmp	DVMRP messages
hostp	Hostp messages
hsl	HSL messages
isis	ISIS messages
l2mrib	L2MRIB messages
lcp	LACP messages
lagd	LAGD messages
ldp	LDP messages
mrib	MRIB messages
mstp	MSTP messages
ndd	NDD messages
nsm	NSM messages
oam	OAM messages
onm	ONM messages
ospf	OSPF messages
ospf6	OSPF6 messages
pim	PIM messages
pon	PON messages
pservd	PSERVD messages
ptp	PTP messages
rib	RIB messages

rip	RIP messages
ripng	RIPNG messages
rmon	RMON messages
rsvp	RSVP messages
sflow	Sflow messages
vrrp	VRRP messages
<0-7>	Severity level as shown in <a href="#">Table 24-77</a> .

### Default

By default, the logging level is 2 (critical).

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#logging level all 5

#configure terminal
(config)#logging level bgp 6

(config)#no logging monitor
```



---

## logging logfile

Use this command to specify the log file controls and where to save the logs in a configuration file. This command enables writing debug output and command history to the disk file in the directory `/log/`.

When logging logfile is enabled, OcnOS log information is stored in user configured logging file which is present in `/log` directory. The log is spread across four files total of these files size is the user configured size.

For example, if the name of the logging log file is "mylogFile" and logging file size configured is 4 MB then each file will be maximum size of 1MB. The logging file names will be "mylogFile", "mylogfile.0", "mylogfile.1" and "mylogfile.2".

"mylogFile" will have the latest log information. As soon as it's size becomes 1 MB this file is renamed as mylogFile.0 and newlog information is written to new "mylogFile". As a result oldest log information stored in mylogfile.2 and is lost in order to accommodate new set of logs in mylogFile.

Use option `no` to cancel writing to a specific log file.

Note: Changing logfile parameters (name/size/severity) will be taken into effect for the next OcnOS session.

### Command Syntax

```
logging logfile LOGFILENAME <0-7> ((size <4096-419430400>)|)
no logging logfile
```

### Parameter

LOGFILENAME	Enter the logfile name (Maximum 200 alphanumeric characters)
<0-7>	Severity level as shown in <a href="#">Table 24-77</a> .
<4096-419430400>	Log file size in bytes.

### Default

By default, log file size is 419430400 bytes.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcnOS version 1.3.

### Examples

This command is used to log the debug messages of a particular protocol daemon to the specified file.

```
#configure terminal
(config)#logging logfile test123 7
```

---

## logging monitor

Use this command to set the severity level that a message must reach before a monitor message is logged. The severity levels are shown in [Table 24-77](#).

Use the command `logging monitor disable` to disable the logging monitor messages.

Use the `no` form of this command to remove logging monitor config and return to the default severity level.

### Command Syntax

```
logging monitor (<0-7>|)
logging monitor disable
no logging monitor
```

### Parameters

<0-7>                      Maximum logging level for monitor messages as shown in [Table 24-77](#).

Note:    Setting the level above 5 might affect performance and is not recommended in a production network.

disable                    Disables logging monitor

### Default

If not specified, the default logging level is 7 (debug-details).

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3 and the command `logging monitor disable` was introduced in the OcNOS-SP version 5.1.

### Example

```
#configure terminal
(config)#logging monitor 6
(config)#commit
(config)#logging monitor disable
(config)#commit
```

---

## logging remote facility

Use this command to set a syslog servers facility.

OcNOS supports logging messages to one or more remote syslog servers. but the same facility is used for all the servers.

Use the `no` form of this command to use the default facility value, which is `local7`.

Note: Only one facility is supported for all protocol modules across all the configured logging servers.

### Command Syntax

```
logging remote facility
(local0|local1|local2|local3|local4|local5|local6|local7|user)
no logging remote facility
```

### Parameters

facility	Entity logging the message (user defined); if not specified, the default is local7
local0	Local0 entity
local1	Local1 entity
local2	Local2 entity
local3	Local3 entity
local4	Local4 entity
local5	Local5 entity
local6	Local6 entity
local7	Local7 entity (default)
user	User entity

### Default

If not specified, the default `facility` is `local7`.

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS-SP version 4.1.

### Examples

```
#configure terminal
(config)#logging remote facility local 6
(config)#no logging remote facility
```

---

## logging remote server

Use this command to set a syslog server.

OcNOS supports logging messages to a syslog server in addition to logging to a file or the console (local or SSH/telnet console). OcNOS messages can be logged to a local syslog server (the machine on which OcNOS executes) as well as to one or more remote syslog servers.

Use the `no` form of this command to remove a syslog server.

Note: Maximum 8 remote log servers can be configured.

### Command Syntax

```
logging remote server (A.B.C.D|X:X::X:X|HOSTNAME) ((0|1|2|3|4|5|6|7)|) (port <1024-65535>|) (vrf management|)
no logging remote server (A.B.C.D|X:X::X:X|HOSTNAME) ((0|1|2|3|4|5|6|7)|)
(port|) (vrf management|)
```

### Parameters

A.B.C.D	IPv4 address
X:X::X:X	IPv6 address
HOSTNAME	Host name; specify <code>localhost</code> to log locally
0	Emergency
1	Alert
2	Critical
3	Error
4	Notification
5	Informational
6	Debug informational
7	Debug detailed
<1024-65535>	Port number Default port is 514
vrf management	Virtual Routing and Forwarding name

Note: Severity at which messages are logged as shown in [Table 24-77](#). If not specified, the default is 7.

### Default

If not specified, the default severity at which messages are logged is 7 (debug detailed).

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS Version 6.3.3.

### Examples

```
#configure terminal
```

```
(config)#logging remote server MyLogHost vrf management
(config)#no feature rsyslog vrf management
(config)# (config)#feature rsyslog
(config)#logging remote server 10.10.10.10 7
```

**Note:** In the latter configuration, the default VRF does not need not to be specified in the command.

---

## logging timestamp

Use this command to set the logging timestamp granularity.

Use the `no` form of this command to reset the logging timestamp granularity to its default (milliseconds).

**Note:** Any change in timestamp configurations will result in timestamp configured for event logged by protocol modules except for CLI history for the current and active sessions. The timestamp configuration is reflected in CLI history for new CLI sessions.

Changing logging timestamp will be taken into effect for the next OcNOS session.

### Command Syntax

```
logging timestamp (microseconds|milliseconds|seconds|none)
no logging timestamp
```

### Parameters

<code>microseconds</code>	Microseconds granularity
<code>milliseconds</code>	Milliseconds granularity
<code>seconds</code>	Seconds granularity
<code>none</code>	no timestamp in log message

### Default

By default, logging time stamp granularity is milliseconds.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#logging timestamp milliseconds
```

---

## show logging

Use this command to display the logging configuration.

### Command Syntax

```
show logging (info|level|server|console|timestamp|monitor)
```

### Parameters

info	Show server logging configuration
level	Show facility logging configuration
server	Syslog server configuration
console	Console configuration
timestamp	Timestamp configuration
monitor	Monitor configuration

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show logging console
```

```
Console logging      : enabled Severity: Operator (critical) Level : 2
```

```
#show logging monitor
```

```
Logging monitor     : enabled Severity: Operator (debugging) Level: 7
```

```
#show logging server
```

```
Remote Servers:
    1.1.1.1
    severity: Operator (informational)
    facility: local7
    VRF : management
```

```
#sh logging info
```

```
Remote Servers:
    1.1.1.1
    severity: Operator (informational)
    facility: local7
    VRF : management
```

```
Logging console     : enabled Severity: operator (critical) Level : 2
```

```
Logging monitor     : enabled Severity: Operator (debugging) Level : 7
```

```
Logging timestamp   : seconds
```

```
File logging        : enabled File Name   : /log/abc Severity   : Operator (de
```

## Syslog

---

bugging) Level : 7 Size : 4194304  
Cli logging : enabled

Facility	Default Severity	Current Session Severity
nsm	2	2
ripd	2	2
ripngd	2	2
ospfd	2	2
ospf6d	2	2
isisd	2	2
hostpd	2	2
mribd	2	2
pimd	2	2
authd	2	2
mstpd	2	2
onmd	2	2
HSL	2	2
oamd	2	2
vlogd	2	2
vrrpd	2	2
ndd	2	2
ribd	2	2
bgpd	2	2
l2mribd	2	2
hslrasmgr	2	2
lagd	2	2
pservd	2	2
cmmd	2	2



---

## show logging last

Use this command to display lines from the end of the log file.

### Command Syntax

```
show logging last (<1-9999>)
```

### Parameters

<1-9999>                      Number of lines to display from end of the log file

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show logging last 100
2016 Mar 03 00:02:32 x86_64-debian NSM-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian OSPF-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian OSPFv3-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian IS-IS-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian BGP-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian RIP-3: AgentX: failed to send open message:
Connection refused
```

---

## show logging logfile

Use this command to display whether logging is enabled, the log file name, and the logging severity.

### Command Syntax

```
show logging logfile
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#sh logging logfile
File logging      : enabled  File Name    : /log/abc  Severity   : (7)
2017 Sep 25 17:18:14 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
logging remote server 1.1.1.1 5 vrf management '
```

```
2017 Sep 25 17:18:14 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
ex'
```

```
2017 Sep 25 17:18:17 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging info '
```

```
2017 Sep 25 17:19:15 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging console '
```

```
2017 Sep 25 17:19:20 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging monitor '
```

```
2017 Sep 25 17:19:32 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging logfile '
```

```
2017 Sep 25 17:19:44 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging server '
```

```
2017 Sep 25 17:28:26 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging info '
```

```
2017 Sep 25 17:29:02 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging console
```

---

# show logging logfile last-index

Use this command to display the number of line in the log file.

## Command Syntax

```
show logging logfile last-index
```

## Parameters

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show logging logfile last-index
logfile last-index : 10
```

[Table 24-78](#) explains the output fields.

**Table 24-78: show logging logfile last-index fields**

Entry	Description
logfile last-index	Number of line in the logfile.

# show logging logfile start-seqn end-seqn

Use this command to display a range of lines in the log file.

## Command Syntax

```
show logging logfile start-seqn (<0-2147483647>) (| (end-seqn <0-2147483647>))
```

## Parameters

start-seqn	Starting line number
end-seqn	Ending line number

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show logging logfile start-seqn 2 end-seqn 7
2
3 2019 Jan 04 06:20:49.611 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : sh logging logfile
4
5 2019 Jan 04 06:21:08.512 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
6
7 2019 Jan 04 06:21:16.246 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
NE4-router#
```

[Table 24-79](#) explains the output fields.

Table 24-79: show logging logfile start-seqn end-seqn fields

Entry	Description
start-seqn	Starting line number
end-seqn	Ending line number

---

## show logging logfile start-time end-time

Use this command to display lines from the log file within a given date-time range.

### Command Syntax

```
show logging logfile start-time (<2000-2030> WORD <1-31> WORD) (| (end-time <2000-2030> WORD <1-31> WORD))
```

### Parameters

start-time	Starting date and time:
<2000-2030>	Year in YYYY format
WORD	Month as jan, feb, mar,..., oct, nov, or dec (maximum length 3 characters)
<1-31>	Day of month in DD format
WORD	Hour, minutes, seconds in HH:MM:SS format (maximum length 8 characters); range <0-23>:<0-59>:<0-59>
end-time	Ending date and time:
<2000-2030>	Year in YYYY format
WORD	Month as jan, feb, mar,..., oct, nov, or dec (maximum length 3 characters)
<1-31>	Day of month in DD format
WORD	Hour, minutes, seconds in HH:MM:SS format (maximum length 8 characters); range <0-23>:<0-59>:<0-59>

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#sh logging logfile start-time 2019 Jan 04 06:20:49 end-time 2019 Jan 04
06:21:16
2019 Jan 04 06:20:49.611 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : sh logging logfile

2019 Jan 04 06:21:08.512 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index

2019 Jan 04 06:21:16.246 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
#
```

---

## show running-config logging

Use this command to display the logging configuration.

### Command Syntax

```
show running-config logging
```

### Parameters

None

### Command Mode

Exec mode and Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show running-config logging
no Logging console
no Logging monitor
logging timestamp milliseconds
```

## CHAPTER 25 System Configure Mode Commands

---

This chapter provides a reference for system-level configure mode commands.

- [delay-profile interfaces](#)
- [delay-profile interfaces subcommands](#)
- [forwarding custom-profile](#)
- [forwarding profile](#)
- [hardware-profile filter \(XGS\)](#)
- [hardware-profile filter \(Qumran\)](#)
- [hardware-profile flowcontrol \(Qumran\)](#)
- [hardware-profile statistics \(Qumran\)](#)
- [load-balance rtag7](#)
- [load-balance rtag7 hash](#)
- [load-balance rtag7 macro-flow](#)
- [show forwarding profile limit](#)
- [show hardware-profile filters](#)
- [snmp restart](#)

---

## delay-profile interfaces

Use this command to go into the delay-profile mode to edit the parameters of the "interfaces" profile. In this mode, the user is able to edit the delay measurement profile parameters.

### Command Syntax

```
delay-profile interfaces
```

### Parameters

None

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS-SP version 5.1.

### Examples

```
#configure terminal
OcNOS(config)#delay-profile interfaces
OcNOS(config-dp-intf)#
```



---

## delay-profile interfaces subcommands

The following commands are to edit the delay-profile parameters.

### Command Syntax

```
mode <two-way>
burst-interval <1000-15000>
burst-count <1-30>
interval < 30-3600>
sender-port <VALUE>
advertisement periodic
advertisement periodic threshold <1-100>
advertisement periodic minimum-change <0-10000>
no advertisement periodic
advertisement accelerated
advertisement accelerated threshold <1-100>
advertisement accelerated minimum-change <0-10000>
no advertisement accelerated
```

### Parameters

two-way	Sets the mode of the measurement. Only "two-way" is supported for now.
<1000-15000>	Set the burst interval in milliseconds. The default value is 3000 milliseconds and the range is 1000-15000 milliseconds
<1-30>	Set the number of packets to be sent at each burst interval. The default value is 10 and the range is 1-30
<30-3600>	Set the computation interval in seconds. The default computation interval is 30 seconds. The range is 30-3600 seconds. This will be used also as the periodic advertisement interval.
<1-100>	Set the advertisement threshold percentage in the range of 1-100 (for periodic, default=10% and for accelerated, default=20%)
<1025-65535>	Set the TWAMP sender port value in the range 1025-65535. If not specified, the default value is 862.
<0-10000>	Set the advertisement minimum change in microseconds in the range 0-10000 (for periodic, default=1000 and for accelerated, default=2000)

### Command Mode

delay-profile interfaces mode

### Applicability

This command was introduced in OcNOS-SP version 5.1.

### Examples

```
#configure terminal
```

```
OcNOS(config)#delay-profile interfaces
OcNOS(config-dp-intf)#mode two-way
OcNOS(config-dp-intf)#burst-count 30
OcNOS(config-dp-intf)#burst-interval 3000
OcNOS(config-dp-intf)#interval 30
OcNOS(config-dp-intf)#sender-port 862
OcNOS(config-dp-intf)#advertisement periodic threshold 10
OcNOS(config-dp-intf)#advertisement periodic minimum-change 1000
OcNOS(config-dp-intf)#advertisement accelerated
OcNOS(config-dp-intf)#advertisement accelerated threshold 20
OcNOS(config-dp-intf)#advertisement accelerated minimum-change 2000
OcNOS(config-dp-intf)#no advertisement periodic
OcNOS(config-dp-intf)#commit
OcNOS(config-dp-intf)#exit
OcNOS(config)#
```

## forwarding custom-profile

Use this command to configure forwarding table sizes.

**Note:** You must reboot after any profile change, except a change to the default profile. The configuration is applied only after a reboot.

Use `show-running configuration` or [show forwarding profile limit](#) to verify the selected profile.

Use the `forwarding custom-profile default` command (with no parameters) to set the forwarding table size to its default.

### Command Syntax

Tomahawk platform:

```
forwarding custom-profile {l2-banks <1-4>|l3-banks <1-4>|lpm-banks 2}
```

Helix4 platform:

```
forwarding custom-profile {l2-banks <1-24>|l3-banks <1-23>|vlan-xlate-banks <1-23>|ep-vlan-xlate-banks <1-23>}
```

Tomahawk and Helix4 platforms:

```
forwarding custom-profile default
```

### Parameters

<code>l2-banks</code>	L2 banks. Unspecified banks are used as L2 banks.
<code>&lt;1-4&gt;</code>	Number of L2 banks. Each bank size is 32k entries and each entry is 105 bits.
<code>&lt;1-24&gt;</code>	Number of L2 banks. Each bank size is 1k entries and each entry is 420 bits.
<code>l3-banks</code>	L3 banks. Unspecified banks are used as L2 banks.
<code>&lt;1-4&gt;</code>	Number of L3 banks. Each bank size is 32k entries and each entry is 105 bits.
<code>&lt;1-23&gt;</code>	Number of L3 banks. Each bank size is 1k entries and each entry is 420 bits.
<code>lpm-banks</code>	Longest-prefix match banks. Unspecified banks are used as L2 banks.
<code>2</code>	Two LPM banks per entry. The remaining banks can be used by any.
<code>vlan-xlate-banks</code>	VLAN translate banks. Unspecified banks are used as L2 banks.
<code>&lt;1-23&gt;</code>	Number of VLAN translate banks. Each bank size is 1k entries and each entry is 420 bits.
<code>ep-vlan-xlate-banks</code>	Egress VLAN translate banks. Unspecified banks are used as L2 banks.
<code>&lt;1-23&gt;</code>	Number of EP VLAN translate banks. Each bank size is 1k entries and each entry is 420 bits.
<code>default</code>	Use L2 profile Three; the size of the l2 table (MAC address table) and l3 table (host table) is almost equal.

### Default

By default, the forwarding table size is L2 profile three: the sizes of the L2 table (MAC address table) and L3 table (host table) are almost equal.

## **Command Mode**

Configure mode

## **Applicability**

This command was introduced before OcNOS version 1.3.

This command only applies to Tomahawk and Helix4 platforms.

## **Examples**

```
#configure terminal
(config)#forwarding custom-profile l3-banks 4
```

---

## forwarding profile

Use this command to configure forwarding table sizes.

Note: You must reboot after any profile change, except a change to the default profile. The configuration is applied only after a reboot.

Note: The use of **k** for “kilo” (as in 1k) does not equal 1,000. In all cases, **k** equals the Boolean value: 1,024.

Use `show-running configuration` or [show forwarding profile limit](#) to verify the selected profile.

Use this `no` command to set the forwarding table size to the default.

### Command Syntax

```
forwarding profile (l2-profile-one | l2-profile-two | l2-profile-three | l3-profile
| l3-128bit-profile | lpm-profile | lpm-128bit-profile)
no forwarding profile
```

### Parameters

For details about these profiles, see [show forwarding profile limit](#).

l2-profile-one	L2 profile One
l2-profile-two	L2 profile Two
l2-profile-three	L2 profile Three (default); the sizes of the L2 table (MAC address table) and L3 table (host table) are almost equal
l3-profile	L3 profile
l3-128bit-profile	L3 profile with IPv6 prefix >64 support
lpm-profile	Longest-prefix match profile
lpm-128bit-profile	LPM profile with IPv6 prefix >64 support

### Default

The default forwarding table size is `l2-profile-three`.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#forwarding profile l2-profile-one
```

---

## hardware-profile filter (XGS)

Use this command to enable or disable ingress IPv4 or IPv6 and egress IPv6 filter groups. Disabling filter groups increases the configurable filter entries.

Use the `no` command to remove explicit enable/disable config for the filter group and switch to default behavior for that filter group.

### Command Syntax

```
hardware-profile filter port-isolation (ingress-ipv4|ingress-ipv6|egress-ipv6|ingress-arp|bfd-group) (enable|disable)
no hardware-profile filter (ingress-ipv4|ingress-ipv6|egress-ipv6|bfd-group)
```

Note: 'no' command is provided only for ingress-ipv4, ingress-ipv6 and egress-ipv6. By default, group is enabled. To increase scalability for other groups, disable the group.

Note: During multiple add/delete entry operation execution in TCAM, entry movement is possible which may lead to delay in completion of operation in hardware resulting into higher cpu utilization.

Note: Bfd-group filter is applicable only for Trident-3 devices. Only after enabling the bfd-group filter bfd sessions will be up in Trident-3.

### Parameter

<code>ingress-ipv4</code>	IPv4 filter ingress group.
<code>ingress-ipv6</code>	IPv6 filter ingress group.
<code>egress-ipv6</code>	IPv6 filter egress group.
<code>enable</code>	Enable filter group.
<code>disable</code>	Disable filter group.
<code>ingress-arp</code>	ARP filter ingress group
<code>bfd-group</code>	BFD filter group
<code>port-isolation</code>	The filter must be enabled before configuring port isolation. Since default filter groups are full, some unused filter needs be disabled in order to enable port-isolation filter.
<code>no</code>	Reset the group to as it was during init

### Default

By default, all filter groups are enabled except the `ingress-arp`, `bfd-group`, `port-isolation` filter group.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

The `no` command is introduced in OcNOS version 4.2.

This form of the `hardware-profile filter` command is *not* available on Qumran platforms. See [hardware-profile filter \(Qumran\)](#).

**Examples**

```
#configure terminal
(config)#hardware-profile filter ingress-ipv4 disable
(config)#hardware-profile filter ingress-ipv4 enable
(config)#no hardware-profile filter ingress-ipv4
(config)#hardware-profile filter ingress-ipv6 disable
(config)#hardware-profile filter port-isolation enable
```

---

## hardware-profile filter (Qumran)

Use this command to enable or disable ingress and egress filter groups. Disabling filter groups increases the configurable filter entries.

### Command Syntax

```
hardware-profile filter (ingress-l2-group|ingress-ipv4|qos-group|egress-  
ipv4|egress-ipv6|egress-l2-group) (enable|disable)
```

### Parameter

ingress-l2-group	Layer 2 (MAC) filter ingress group.
ingress-ipv4	IPv4 filter ingress group.
qos-group	QoS filter group.
egress-ipv4	IPv4 filter egress group.
egress-ipv6	IPv6 filter egress group.
egress-l2-group	Layer 2 (MAC) filter egress group.
enable	Enable filter group.
disable	Disable filter group.

### Default

By default, all filter groups are enabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

This command is only available on Qumran platforms. For other platforms, see [hardware-profile filter \(XGS\)](#).

### Examples

```
#configure terminal  
(config)#hardware-profile filter ingress-ipv4 disable  
(config)#hardware-profile filter ingress-ipv4 enable
```



---

## hardware-profile flowcontrol (Qumran)

Use this command to globally enable or disable hardware-based flow control.

### Syntax

```
hardware-profile flowcontrol (disable|enable)
```

### Parameters

disable	Disable flow control globally
enable	Enable flow control globally

### Default

By default flow control is disabled on Qumran platforms.

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS-SP version 1.0.

This command is only available on Qumran platforms.

### Examples

```
#configure terminal
(config)#hardware-profile flowcontrol enable
```

---

## hardware-profile statistics (Qumran)

Use this command to enable or disable filter statistics in hardware.

Note: You must reboot the switch after giving this command for the changes to take effect.

### Command Syntax

```
hardware-profile statistics (ingress-acl|mpls-ac|mpls-lsp|mpls-pwe)
(enable|disable)
```

### Parameter

ingress-acl	Ingress ACL statistics.
mpls-ac	Attachment circuit statistics.
mpls-lsp	LSP statistics.
mpls-pwe	Pseudowire logical interfaces statistics.
enable	Enable statistics.
disable	Disable statistics.

### Default

By default, filter statistics are disabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

This command is only available on Qumran platforms.

### Examples

```
#configure terminal
(config)#hardware-profile statistics mpls-lsp enable
```

---

## load-balance enable

Use this command to enable load-balancing configurations in hardware.

Use the no option to reset the load balancing to default settings.

**Note:** When the command "load-balance enable" is issued, the default load-balance settings are unset. User then has to configure the new load-balancing parameters.

### Command Syntax

This form unsets load balancing globally:

```
load-balance enable
```

This form resets load balancing globally to default settings:

```
no load-balance enable
```

By default, load balancing is enabled for ECMP and LAG.

This form sets hashing based on IPv4 fields:

```
load-balance (ipv4 {src-ipv4 | dest-ipv4 | src14-port | dest14-port | protocol-id})
no load-balance (ipv4 {src-ipv4 | dest-ipv4 | src14-port | dest14-port | protocol-id})
```

This form sets hashing based on IPv6 fields:

```
load-balance (ipv6 {src-ipv6 | dest-ipv6 | src14-port | dest14-port | protocol-id})
no load-balance (ipv6 {src-ipv6 | dest-ipv6 | src14-port | dest14-port | protocol-id})
```

This form sets hashing based on L2 fields:

```
load-balance (l2 {src-dest-mac|non-symmetrice|ether-type|vlan})
no load-balance (l2 {src-dest-mac|non-symmetrice|ether-type|vlan})
```

This form sets hashing on an MPLS fields:

```
load-balance (mpls {labels})
no load-balance (mpls {labels})
```

**Note:** The configured load balancing parameters are global and will be applicable to all LAG & ECMP created in the hardware.

### Parameters

ipv4	Load balance IPv4 packets
src-ipv4	Source IPv4 based load balancing
dest-ipv4	Destination IPv4 based load balancing

<code>src14-port</code>	Source L4 port based load balancing
<code>dest14-port</code>	Destination L4 port based load balancing
<code>protocol-id</code>	Protocol ID based load balancing
<code>ipv6</code>	Load balance IPv6 packets
<code>src-ipv6</code>	Source IPV6 based load balancing
<code>dest-ipv6</code>	Destination IPv6 based load balancing
<code>src14-port</code>	Source L4 port based load balancing
<code>dest14-port</code>	Destination L4 port based load balancing
<code>l2</code>	Load balance L2 packets
<code>src-dest-mac</code>	Source Destination based load balancing
<code>non-symmetric</code>	Non symmetrical based load balancing
<code>ether-type</code>	Ether-type based load balancing
<code>Vlan</code>	VLAN-based load balancing
<code>mpls</code>	Load balance MPLS packets
<code>labels</code>	label stack based load balancing.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS-SP version 1.0.

### Examples

```
(config)#load-balance enable
(config)#load-balance ipv4 src-ipv4
```

## load-balance rtag7

Use this command to configure rtag7 load balancing.

Use the `no` option to disable the rtag7 load balancing.

### Command Syntax

This form enables or disables rtag7 load balancing globally:

```
load-balance rtag7
no load-balance rtag7
```

By default, load balancing is enabled for ECMP, and LAG.

This form sets rtag7 hashing for ECMP and L3 LAG based on IPv4 fields:

```
load-balance rtag7 (ipv4 {src-ipv4|dest-ipv4|src-l4-port|dest-l4-port|protocol-id})
no load-balance rtag7 (ipv4 {src-ipv4|dest-ipv4|src-l4-port|dest-l4-port|protocol-id})
```

By default, IPv4 ECMP is configured with the fields `src-ipv4`, `dest-ipv4`, `src-l4-port`, and `dest-l4port`.

By default, L3 LAG is configured with the fields `src-ipv4` and `dest-ipv4`.

This form sets rtag7 hashing for ECMP based on IPv6 fields:

```
load-balance rtag7 (ipv6 {src-ipv6|dest-ipv6|src-l4-port|dest-l4-port|next-hdr})
no load-balance rtag7 (ipv6 {src-ipv6|dest-ipv6|src-l4-port|dest-l4-port|next-hdr})
```

By default, IPv6 ECMP is configured with the fields `src-ipv6`, `dest-ipv6`, `src-l4-port`, and `dest-l4port`.

This form sets rtag7 hashing for L2 LAG based on L2 fields:

```
load-balance rtag7 (l2 {dest-mac|src-mac|ether-type|vlan})
no load-balance rtag7 (l2 {dest-mac|src-mac|ether-type|vlan})
```

By default, L2 LAG is configured with the fields `src-mac` and `dest-mac`.

This form sets rtag7 hashing on an MPLS egress LER node based on L2/L3 fields:

```
load-balance rtag7 (mpls-ler ((inner-l2 ({dest-mac|src-mac|ether-type|vlan})) |
(inner-l3 ({src-ip|dest-ip|src-l4-port|dest-l4-port|protocol-id}))))
no load-balance rtag7 (mpls-ler ((inner-l2 ({dest-mac|src-mac|ether-type|vlan})) |
(inner-l3 ({src-ip|dest-ip|src-l4-port|dest-l4-port|protocol-id}))))
```

Please note the following:

- For ingress LER nodes, hashing is done on L2 fields, L3 fields (outer IPx), or inner IP fields (only for IPx-over-IPx or IPx-over-GRE-IPx).
- For egress LER nodes, hashing is done based on only L2 and L3 fields immediately after the MPLS header which is popped. Any other fields are not supported.

This form sets rtag7 hashing based on the outer IP address:

```
load-balance rtag7 (tunnel outer-l3-header)
no load-balance rtag7 (tunnel outer-l3-header)
```

**Parameters**

ipv4	Load balance IPv4 packets
src-ipv4	Source IPv4 based load balancing
dest-ipv4	Destination IPv4 based load balancing
src-l4-port	Source L4 port based load balancing
dest-l4-port	Destination L4 port based load balancing
protocol-id	Protocol ID based load balancing
ipv6	Load balance IPv6 packets
src-ipv6	Source IPV6 based load balancing
dest-ipv6	Destination IPv6 based load balancing
src-l4-port	Source L4 port based load balancing
dest-l4-port	Destination L4 port based load balancing
next-hdr	Next header field for IPv6
l2	Load balance L2 packets
dest-mac	Destination MAC address based load balancing
src-mac	Source MAC address based load balancing
ether-type	Ether-type based load balancing
vlan	VLAN-based load balancing
tunnel	Load balance tunneled packets based on outer header (default uses the inner-header)
outer-l3-header	Use outer header for hashing (ip-over-ip, ipv6-over-ip, ip-over-gre-ip, ipv6-over-gre-ip, ipv6-over-ipv6, ip-over-ipv6, ip-over-gre-ipv6, ipv6-over-gre-ipv6)
mpls-ler	Load balance LER packets
inner-l2	Load balance Inner I2 header
dest-mac	Destination MAC address load balancing
src-mac	Source MAC address
ether-type	Ether-type based load balancing
vlan	VLAN tag id
inner-l3	Inner I3 header
dest-ip	Destination IP address
src-ip	Source IP address
src-l4-port	Source L4 port based load balancing
protocol	ID Protocol (IPv4), next-hdr (IPv6)

**Command Mode**

Configure mode

**Applicability**

This command was introduced before OcNOS version 1.3.

**Examples**

```
(config)#load-balance rtag7  
(config)#load-balance rtag7 ipv4 src-ipv4
```

---

## load-balance rtag7 hash

Use this command to set the rtag7 hash computation method.

Use the `no` parameter to set the rtag7 hash computation method to its default.

### Command Syntax

```
load-balance rtag7 hash (crc16-bisync|crc16-ccitt|crc32-lo|crc32-hi)
no load-balance rtag7 hash
```

### Parameters

<code>crc16-bisync</code>	16-bit CRC16 using the binary synchronous polynomial.
<code>crc16-ccitt</code>	16-bit CRC16 using the CCITT polynomial.
<code>crc16-hi</code>	16 most significant bits of computed CRC32.
<code>crc16-lo</code>	16 least significant bits of computed CRC32

### Default

The default rtag7 hash computation method is 16-bit CRC16 using the binary synchronous polynomial (`crc16-bisync`).

### Command Mode

Configure mode

### Default settings

```
load-balance rtag7 hash crc16-bisync
```

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#load-balance rtag7
(config)#load-balance rtag7 hash crc16-ccitt
(config)#show running-config | inc rtag7
!
load-balance rtag7
load-balance rtag7 hash crc16-ccitt
!
(config)#no load-balance rtag7 hash
(config)#
```



---

## load-balance rtag7 macro-flow

Use this command to enable rtag7 macro-flow based hashing.

When macro-flow is enabled, a hash function is chosen dynamically based on corresponding macro flow. It is useful when hash polarization is observed in the topology.

**Note:** In case of topology having multiple level of split paths, macro-flow improves the distribution but can still have variation in traffic distribution. It is observed that when 2 level of hashing is present in topology (LAG after ECMP split traffic to half), 6% of variation was observed.

Use the `no` parameter to disable rtag7 macro-flow based hashing.

### Command Syntax

```
load-balance rtag7 macro-flow
no load-balance rtag7 macro-flow
```

### Parameters

None

### Default

By default, rtag7 macro-flow based hashing is disabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#load-balance rtag7
(config)#load-balance rtag7 macro-flow
(config)#show running-config | inc rtag7
!
load-balance rtag7
load-balance rtag7 macro-flow
!
(config)#no load-balance rtag7 macro-flow
```

# show forwarding profile limit

Use this command to show all the forwarding table sizes.

Note: The use of k for “kilo” (as in 1k) does not equal 1,000. In all cases, k equals 2 ^10: 1,024.

## Command Syntax

```
show forwarding profile limit
```

## Parameters

None

## Default

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show forwarding profile limit
```

```
Configured profile : custom-profile
Forwarding profile : custom-profile(Active in hardware)
```

Forwarding Profile Table Size							
Profile Name	MAC ADDR	Host-Table	Prefix-Table	Vlan-xlate	Egress-Vlan-xlate		
		Table (UC)	Table (UC)	Table	Table		
		IPV4	IPV6	IPV4	IPV6		
l2-profile-one	96k	0k	0k	8k	4k	0k	0k
l2-profile-two	64k	8k	4k	8k	4k	8k	8k
l2-profile-three	32k	16k	8k	8k	4k	16k	16k
l3-profile	4k	92k	46k	8k	4k	0k	0k
custom-profile	576k	60k	30k	8k	4k	0k	0k#

Table 25-80 explains the show command output fields.

**Table 25-80: show forwarding profile limit output**

Field	Description
Profile Name	Names of the forwarding profiles
MAC ADDR Table	MAC address table sizes
Host-Table (UC) IPv4	IPv4 unicast host table sizes
Host-Table (UC) IPv6	IPv6 unicast host table sizes
Prefix-Table (UC) IPv4	IPv4 unicast prefix table sizes
Prefix-Table (UC) IPv6	IPv6 unicast prefix table sizes
Vlan-xlate-Table	Number of VLAN translate banks
Egress-Vlan-xlate-Table	Number of egress VLAN translate banks

## show hardware-profile filters

Use this command to check the status of hardware filter groups. Status is not shown for filter groups which are disabled.

### Command Syntax

```
show hardware-profile filters
```

### Parameters

None

### Default

None

### Command Mode

Exec and privileged exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

This command is *not* available on Qumran platforms.

### Examples

```
#show hardware-profile filters
```

INGRESS:							
	Free	Used		Total Entries			
TCAMS	Entries						
		%	Entries	Total	Dedicated	shared	
QOS	244	5	12	256	256	0	
L2-ACL	253	1	3	256	256	0	
IPV4-ACL	256	0	0	256	256	0	
ARP-ACL	242	5	14	256	256	0	
EGRESS:							
	Free	Used		Total Entries			
TCAMS	Entries						
		%	Entries	Total	Dedicated	shared	
L2-ACL/IPV4-ACL/QOS	512	0	0	512	256	256	

[Table 25-81](#) explains the output fields.

**Table 25-81: show hardware-profile filters**

Field	Description
EGRESS	Egress filtering is a process in which outbound data is monitored or restricted, usually by means of a firewall that blocks packets that fail to meet certain security requirements.
INGRESS	Ingress filtering is a method used to prevent suspicious traffic from entering a network.
TCAMS	Number of ternary content addressable memory (TCAM) entries a particular firewall filter.
Free Entries	Number of TCAM filter entries available for use by the filter group.
Used Entries	Number of TCAM filter entries used by the filter group.
Total Entries	Number of TCAM total filter entries to the filter group.
Dedicated Entries	Number of TCAM filter entries dedicated to the filter group.
Shared Entries	Number of TCAM filter entries shared to the filter group.

---

## snmp restart

Use this command to restart SNMP for a given process.

### Command Syntax

```
snmp restart (auth | bfd | bgp | cfm | efm | isis | ldp | lldp | mrib | mstp | nsm  
| ospf | ospf6 | pim | rib | rmon | rsvp | vrrp)
```

### Parameters

None

### Default

By default, SNMP resart is disabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal  
(config)#snmp restart nsm
```

---

## CHAPTER 26 TACACS+

---

Terminal Access Controller Access-Control System Plus (TACACS+, usually pronounced like tack-axe) is an access control network protocol for network devices.

The differences between RADIUS and TACACS+ can be summarized as follows:

- RADIUS combines authentication and authorization in a user profile, while TACACS+ provides separate authentication.
- RADIUS encrypts only the password in the access-request packet sent from the client to the server. The remainder of the packet is unencrypted. TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.
- RADIUS uses UDP, while TACACS+ uses TCP.
- RADIUS is based on an open standard (RFC 2865). TACACS+ is proprietary to Cisco, although it is an open, publicly documented protocol (there is no RFC protocol specification for TACACS+).

Note: Only network administrators can execute these commands. For more, see the [username](#) command.

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

- [add policy](#)
- [clear tacacs-server counters](#)
- [debug tacacs+](#)
- [default](#)
- [deny](#)
- [feature dynamic-rbac](#)
- [feature tacacs+](#)
- [permit](#)
- [policy](#)
- [role](#)
- [show debug tacacs+](#)
- [show rbac-policy](#)
- [show rbac-role](#)
- [show running-config tacacs+](#)
- [show tacacs-server](#)
- [tacacs-server login host](#)
- [tacacs-server login key](#)
- [tacacs-server login timeout](#)

---

## add policy

Use this command to add a policy to a TACACS+ role-based authorization (RBAC) role.

Use the `no` form of this command to remove a policy from an RBAC role.

### Command Syntax

```
add policy POLICY-NAME
no add policy POLICY-NAME
```

### Parameters

POLICY-NAME	Name of the policy
-------------	--------------------

### Default

None

### Command Mode

RBAC role mode

### Applicability

This command was introduced in OcNOS version 1.3.5.

### Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#no add policy myPolicy2
```



---

## clear tacacs-server counters

Use this command to clear the counter on a specified TACACS server.

### Syntax

```
clear tacacs-server ((HOSTNAME | X:X::X:X | A.B.C.D)|) counters (vrf (management | all)|)
```

### Parameters

HOSTNAME	The name of the server
X:X::X:X	IPv6 address of the server
A.B.C.D	IPv4 address of the server
vrf	VRF of the sever
management	The management VRF
all	All VRFs

### Default

NA

### Command Mode

Executive mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear tacacs-server 10.1.1.1 counters
```

---

## debug tacacs+

Use this command to display TACACS+ debugging information.

Use the `no` form of this command stop displaying TACACS+ debugging information.

### Command Syntax

```
debug tacacs+
no debug tacacs+
```

### Parameters

None

### Default

Disabled

### Command Mode

Executive mode and configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#debug tacacs+
```

---

## default

Use this command to set the default rule for a TACACS+ role-based authorization (RBAC) role.

Use the `no` parameter with this command to remove the default rule for a TACACS+ role-based authorization (RBAC) role.

### Command Syntax

```
default (permit-all | deny-all)
no default
```

### Parameters

<code>permit-all</code>	Permit all commands
<code>deny-all</code>	Deny all commands

### Default

Unless you explicitly give this command, the default rule for a role is `deny-all`.

### Command Mode

RBAC role mode

### Applicability

This command was introduced in OcNOS version 1.3.5.

### Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#add policy myPolicy2
```

---

## deny

Use this command to add a deny rule to a TACACS+ role-based authorization (RBAC) policy.

Use the `no` form of this command to remove a deny rule from an RBAC policy.

### Command Syntax

```
deny RULE-STRING (mode MODE-NAME | )  
no deny RULE-STRING (mode MODE-NAME | )
```

### Parameters

RULE-STRING	Command string
MODE-NAME	Command prompt string such as “config-router” or “config-if”. Deny access to the command only in this mode.

### Default

None

### Command Mode

RBAC policy mode

### Applicability

This command was introduced in OcNOS version 1.3.5.

### Examples

```
#configure terminal  
(config)#policy myPolicy  
(config-policy)#deny "ip address" mode config-if
```

---

## feature dynamic-rbac

Use this command to enable the TACACS+ role-based authorization (RBAC) feature.

Use the `no` form of this command to disable the RBAC feature.

### Command Syntax

```
feature dynamic-rbac
no feature dynamic-rbac
```

### Parameters

None

### Default

By default, feature TACACS+ RBAC is disabled

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 1.3.5.

### Examples

```
#configure terminal
(config)#feature dynamic-rbac
```

---

## feature tacacs+

Use this command to enable the TACACS+ feature.

Use the `no` form of this command to disable the TACACS+ feature.

### Command Syntax

```
feature tacacs+ (vrf management|)
no feature tacacs+ (vrf management|)
```

### Parameters

<code>vrf</code>	Virtual Routing and Forwarding
<code>management</code>	Management VRF

### Default

By default, feature tacacs+ is disabled

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#feature tacacs+ vrf management
```

---

## permit

Use this command to add a permit rule to a TACACS+ role-based authorization (RBAC) policy.

Use the `no` form of this command to remove a permit rule in an RBAC policy.

### Command Syntax

```
permit RULE-STRING (mode MODE-NAME |)
no permit RULE-STRING (mode MODE-NAME |)
```

### Parameters

RULE-STRING	Command string
MODE-NAME	Command prompt string such as “config-router” or “config-if”. Permit access to the command only in this mode.

### Default

None

### Command Mode

RBAC policy mode

### Applicability

This command was introduced in OcNOS version 1.3.5.

### Examples

```
#configure terminal
(config)#policy myPolicy
(config-policy)#permit "ip address" mode config-if
```

---

## policy

Use this command to create a TACACS+ role-based authorization (RBAC) policy and enter RBAC policy mode.

Use the `no` form of this command to remove an RBAC policy.

### Command Syntax

```
policy POLICY-NAME
no policy POLICY-NAME
```

### Parameters

POLICY-NAME	Policy name
-------------	-------------

### Default

None

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 1.3.5.

### Examples

```
#configure terminal
(config)#policy myPolicy
(config-policy)#permit "ip address" mode config-if
```



---

## role

Use this command to create a TACACS+ role-based authorization (RBAC) role and enter RBAC role mode.

Use the `no` form of this command to remove an RBAC role.

### Command Syntax

```
role ROLE-NAME
no role ROLE-NAME
```

### Parameters

ROLE-NAME	Role name. You <i>cannot</i> specify one of these roles already defined in OcNOS:  network-admin network-user network-operator network-engineer  For more about these built-in roles, see <a href="#">username</a> .
-----------	--

### Default

None

### Command Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 1.3.5.

### Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#add policy myPolicy2
```

---

## show debug tacacs+

Use this command to display whether TACACS+ debugging is enabled.

### Command Syntax

```
show debug tacacs+
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show debug tacacs+
TACACS client debugging is on
```

---

## show rbac-policy

Use this command to display TACACS+ role-based authorization (RBAC) policies.

### Command Syntax

```
show rbac-policy (POLICY-NAME |)
```

### Parameters

POLICY-NAME	Policy name
-------------	-------------

### Default

None

### Command Mode

Exec and privileged exec mode

### Applicability

This command was introduced in OcNOS version 1.3.5.

### Examples

```
#show rbac-policy myPolicy
-----
Policy Name      : myPolicy
permit "ip address" mode config-if
```

# show rbac-role

Use this command to display information about TACACS+ role-based authorization (RBAC) roles.

## Command Syntax

```
show rbac-role (ROLE-NAME |)
```

## Parameters

ROLE-NAME	Role name
-----------	-----------

## Default

None

## Command Mode

Exec and privileged exec mode

## Applicability

This command was introduced in OcNOS version 1.3.5.

## Examples

```
#show rbac-role myRole
-----
Role Name           : myRole
Default rule        : permit-all
Attached Policies    : myPolicy1
                    : myPolicy2
-----
```

[Table 26-82](#) explains the output fields.

Table 26-82: show rbac-role fields

Entry	Description
Role Name	Role name
Default rule	permit-all or deny-all
Attached Policies	Name of policies attached to this role

---

# show running-config tacacs+

Use this command to display TACACS+ settings in the running configuration.

## Command Syntax

```
show running-config tacacs+
```

## Parameters

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show running-config tacacs+
feature tacacs+ vrf management
tacacs-server login host 10.16.19.2 vrf management seq-num 1 key 7
0x9f4a8983e0216052
```

[Table 26-83](#) explains the output fields.

**Table 26-83: show running-config fields**

Entry	Description
TACAS server host	TACACS+ server Domain Name Server (DNS) name.
Seq-num	Sequence number of user authentication attempt with the TACACS+ server.
VRF Management	The management traffic using VPN Routing and Forwarding (VRFs).

# show tacacs-server

Use this command to display the TACACS+ server configuration.

## Command Syntax

```
show tacacs-server (|vrf (management|all)) ((WORD) | (groups (GROUP|) |) | (sorted)
```

## Parameters

WORD	DNS host name or IP address
groups	TACACS+ server group
GROUP	Group name; if this parameter is not specified, display all groups
sorted	Sort by TACACS+ server name
vrf	management or all VRFs

## Command Mode

Executive mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Examples

```
#show tacacs-server
total number of servers:1

Tacacs+ Server          : 192.168.10.215/49(*)
    Sequence Number     : 1
    Failed Auth Attempts : 0
    Success Auth Attempts : 14
    Failed Connect Attempts : 0
    Last Successful authentication: 2017 December 18, 12:27:13

(*) indicates last active.
```

Table 26-84 explains the output fields.

Table 26-84: show tacacs-server output fields

Field	Description
Sequence Number	Sequence number of user authentication attempt with the TACACS+ server.
Failed Auth Attempts	Number of times user authentication failed with the TACACS+ server. Increments for server key mismatches and password mismatches or wrong password for the user.
Success Auth Attempts	Number of times user authenticated with TACACS+ server. Increments for each successful login.

**Table 26-84: show tacacs-server output fields**

Field	Description
Failed Connect Attempts	Number of failed TCP socket connections to the TACACS+ server. Increments for server connection failure cases such as server not-reachable, server port mismatches.
Last Successful authentication	Timestamp when user successfully authenticated with the TACACS+ server.

# tacacs-server login host

Use this command to set the TACACS+ server host name or IP address.

Use the `no` form of this command to remove an TACACS+ server (if only a host name or IP address is specified as parameter) or to remove all of a TACACS+ server's configuration settings (if any other parameters are also specified).

## Command Syntax

```
tacacs-server login host (HOSTNAME | X:X::X:X | A.B.C.D) (vrf management|) (seq-num
<1-8> |) (key ((0 WORD) | (7 WORD) | (WORD))) (port <1025-65535> |) (timeout <1-
60> |)

no tacacs-server login host (HOSTNAME | A.B.C.D | X:X::X:X) (vrf management|)

no tacacs-server login host (HOSTNAME | X:X::X:X | A.B.C.D) (vrf management|) (key
((0 WORD) | (7 WORD) | (WORD))) (port <1025-65535> |) (timeout <1-60> |)
```

## Parameters

HOSTNAME	Host name
X:X::X:X	IPv6 address
A.B.C.D	IPv4 address
vrf	Virtual Routing and Forwarding
management	Management VRF
seq-num	Sequence Number / Priority index for tacacs-servers
key	Authentication and encryption key ("shared secret")
0	Unencrypted (clear text) shared key
WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 512 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
port	TACACS+ server port
<1205-65535>	TACACS+ server port number; the default is 49
timeout	TACACS+ server timeout
<1-60>	Timeout value in seconds; default is 5 seconds

## Default

Enable authentication for TACACS+ server configured. Authorization is also enabled by default. The default server port is 49. The default timeout value is 5 seconds.

There is `no` command to enable authorization. Authorization functionality is enabled by default when remote authentication is enabled with TACACS+.



---

**Command Mode**

Configure mode

**Applicability**

This command was introduced before OcNOS version 1.3.

**Examples**

```
#configure terminal
(config)#tacacs-server login host 203.0.113.31 vrf management
```

---

## tacacs-server login key

Use this command to set a global preshared key (“shared secret”) which is a text string shared between the device and TACACS+ servers.

Use the `no` form of this command to remove a global preshared key.

### Command Syntax

```
tacacs-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
no tacacs-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
```

### Parameters

0	Unencrypted (clear text) shared key
WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 512 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
vrf	Virtual Routing and Forwarding
management	Management VRF

### Default

Disabled

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#tacacs-server login key 7 jvn05mlQH1 vrf management
```

---

## tacacs-server login timeout

Use this command to set the period to wait for a response from the server before the client declares a timeout failure. The default timeout value is 5 seconds.

You can only give this command when the TACACS+ feature is enabled.

Use the `no` form of this command to set the timeout value to its default value (5 seconds).

**Note:** TELNET client session's default timeout is 60 seconds, so configuring timeout of 60 seconds timeout impacts TELNET client applications, because it cannot be fallback to use the other configured server/group. Hence it is recommended to configure 57 seconds or lesser timeout while using TELNET. This timeout doesn't have an impact on SSH connections.

### Command Syntax

```
tacacs-server login timeout <1-60> (vrf management|)
no tacacs-server login timeout (vrf management|)
```

### Parameters

<1-60>	Timeout value in seconds
vrf	Virtual Routing and Forwarding
management	Management VRF

### Default

Disabled

### Command Mode

Configure mode

### Applicability

This command is introduced in OcNOS version 1.3.9

### Examples

```
#configure terminal
(config)#tacacs-server login timeout 35 vrf management
```



---

## CHAPTER 27 Telnet

---

This chapter describes telnet commands.

Telnet is a client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of functions.

Note: In OcNOS, the default Linux terminal type is "export TERM=xterm"

Note: The commands below are supported only on the "management" VRF.

This chapter contains these commands:

- [debug telnet server](#)
- [feature telnet](#)
- [show debug telnet-server](#)
- [show running-config telnet server](#)
- [show telnet-server](#)
- [telnet](#)
- [telnet6](#)
- [telnet server port](#)
- [telnet server session-limit](#)

---

## debug telnet server

Use this command to display telnet debugging information.

Use the `no` form of this command to stop displaying telnet debugging information.

### Command Syntax

```
debug telnet server
no debug telnet server
```

### Parameters

None

### Default

By default, disabled.

### Command Mode

Executive mode and configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show debug telnet-server

telnet server debugging is on
#
```

---

## feature telnet

Use this command to enable the telnet server.

Use the `no` form of this command to disable the telnet server.

### Command Syntax

```
feature telnet (vrf management|)
no feature telnet (vrf management|)
```

### Parameters

management	Virtual Routing and Forwarding name
------------	-------------------------------------

### Default

By default, feature telnet is enabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#feature telnet vrf management
```

---

## show debug telnet-server

Use this command to display whether telnet debugging is enabled.

### Command Syntax

```
show debug telnet-server
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show debug telnet-server  
telnet server debugging is on
```



---

## show running-config telnet server

Use this command to display telnet settings in the running configuration.

### Command Syntax

```
show running-config telnet server
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show running-config telnet server
telnet server port 1025 vrf management
feature telnet vrf management
```

---

## show telnet-server

Use this command to display the telnet server status.

### Command Syntax

```
show telnet server
```

### Parameters

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#show telnet server  
telnet server enabled port: 23
```

---

## telnet

Use this command to open a telnet session to an ipv4 address or host name resolved to ipv4 address.

### Command Syntax

```
telnet (A.B.C.D | HOSTNAME) (vrf (NAME|management))  
telnet (A.B.C.D | HOSTNAME) (<1-65535>) (vrf (NAME|management))
```

### Parameters

A.B.C.D	Destination IPv4 Address to open a telnet session.
HOSTNAME	Destination Hostname to resolve into IPv4 address to open a telnet session.
1-65535	Destination Port to open a telnet session. Default is 23.
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

### Default

By default, telnet is 23

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#telnet 10.12.16.17 2543 vrf management  
Trying 10.12.16.17...
```

---

## telnet6

Use this command to open a telnet session to an ipv6 address or host name resolved to ipv6 address.

### Command Syntax

```
telnet6 (X:X::X:X| HOSTNAME) (vrf (NAME|management))
telnet6 (X:X::X:X | HOSTNAME) (<1-65535>) (vrf (NAME|management))
```

### Parameters

X:X::X:X	Destination IPv6 Address to open a telnet session.
HOSTNAME	Destination Host name to resolve into IPv6 address to open a telnet session.
1-65535	Destination Port to open a telnet session. Default is 23.
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

### Default

By default, telnet is 23.

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#telnet6 2:2::2:2 2543 vrf management
Trying 2:2::2:2...
```

---

## telnet server port

Use this command to set the port number on which the telnet server listens for connections. The default port on which the telnet server listens is 23.

You can only give this command when the telnet server is disabled. See the [feature telnet](#) command.

Use the `no` form of this command to set the default port number (23).

### Command Syntax

```
telnet server (port <1024-65535>) (vrf management|)
no telnet server port (vrf management|)
```

### Parameters

<1024-65535>	Port number
management	Virtual Routing and Forwarding name

### Default

By default, telnet server port number is 23

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Examples

```
#configure terminal
(config)#telnet server port 1157 vrf management
```

---

## telnet server session-limit

Use this command to limit number of Telnet sessions. Only 40 sessions allowed including Telnet and SSH.

This command can be used only when the telnet server is disabled. Refer to [feature telnet](#) command section for more information.

Use no form of this command to set to default value.

### Command Syntax

```
telnet server session-limit <1-40> (vrf management|)
no telnet server session-limit (vrf management|)
```

### Parameters

<1-40>	Number of sessions
management	Virtual Routing and Forwarding name

### Default

By default, 40 sessions are allowed.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS-SP version 4.2

### Examples

```
#configure terminal
(config)#telnet server session-limit 4 vrf management
```

## CHAPTER 28 Time Range Commands

---

This chapter describes the commands used to create and manage time range objects which are used to add a timing boundary for specified activities. The activity starts, ends, and repeats at the specific times that you set.

- [end-time \(absolute\)](#)
- [end-time after \(relative\)](#)
- [frequency](#)
- [frequency days \(specific days\)](#)
- [start-time \(absolute\)](#)
- [start-time after \(relative\)](#)
- [start-time now \(current\)](#)
- [time-range](#)

---

## end-time (absolute)

Use this command to set the end time for the time range to an absolute time.

### Command Syntax

```
end-time HH:MM <1-31> (january | february | march | april | may | june | july |  
    august | september | october | november | december) <1995-2035>
```

### Parameters

HH:MM	End time hour and minutes
<1-31>	Day of the month
april	Month of April
august	Month of August
december	Month of December
february	Month of February
january	Month of January
july	Month of July
june	Month of June
march	Month of March
may	Month of May
november	Month of November
october	Month of October
september	Month of September
<1995-2035>	Year

### Default

N/A

### Command Mode

Time range mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
(config)#time-range TIMER1  
(config-tr)#end-time 10:10 20 february 2021
```



---

## end-time after (relative)

Use this command to set the end time for the time range to a relative time in minutes, from the configured start time.

### Command Syntax

```
end-time after <1-129600>
```

### Parameters

<1-129600>	Number of minutes from the start time
------------	---------------------------------------

### Default

N/A

### Command Mode

Time range mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
(config)#time-range TIMER1  
(config-tr)#end-time after 100
```

---

## frequency

Use this command to set the frequency for the time range.

### Command Syntax

```
frequency (daily|hourly|weekly)
```

### Parameters

daily	Daily frequency
hourly	Hourly frequency
weekly	Weekly frequency

### Default

N/A

### Command Mode

Time range mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
(config)#time-range TIMER1  
(config-tr)#frequency hourly
```

---

## frequency days (specific days)

Use this command to set the frequency for the time range to specific days of the week.

### Command Syntax

```
frequency days WORD
```

### Parameters

WORD

Colon-separated list of 3-letter days of the week for the days on which the range is repeated. For example:

```
mon:tue:wed:thu:fri:sat:sun
```

### Default

N/A

### Command Mode

Time range mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
(config)#time-range TIMER1
(config-tr)#frequency days mon:wed:fri
(config)#exit
(config)#time-range TIMER2
(config-tr)#frequency days mon:tue:wed:thu:fri:sat:sun
```

---

## start-time (absolute)

Use this command to set the start time for the time range to an absolute time.

### Command Syntax

```
start-time HH:MM <1-31> (january | february | march | april | may | june | july |  
    august | september | october | november | december) <1995-2035>
```

### Parameters

HH:MM	End time hour and minutes
<1-31>	Day of the month
april	Month of April
august	Month of August
december	Month of December
february	Month of February
january	Month of January
july	Month of July
june	Month of June
march	Month of March
may	Month of May
november	Month of November
october	Month of October
september	Month of September
<1995-2035>	Year

### Default

N/A

### Command Mode

Time range mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
(config)#time-range TIMER1  
(config-tr)#start-time 09:09 20 february 2021
```

---

## start-time after (relative)

Use this command to set the start time for the time range to a relative time in minutes, from the current time.

### Command Syntax

```
start-time after <1-129600>
```

### Parameters

<1-129600>	Number of minutes from the current time
------------	---

### Default

N/A

### Command Mode

Time range mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
(config)#time-range TIMER1
(config-tr)#start-time after 100
```

---

## start-time now (current)

Use this command to set the start time for the time range to the current system time.

### Command Syntax

```
start-time now
```

### Parameters

None

### Default

N/A

### Command Mode

Time range mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
(config)#time-range TIMER1  
(config-tr)#start-time now
```

---

## time-range

Use this command to create a time range and go into the time range mode to configure the time range. If the time range already exists, then it will be edited.

Use the `no` form of this command to remove a time range object.

### Command Syntax

```
time-range NAME
no time-range NAME
```

### Parameters

NAME	Name of the time range.
------	-------------------------

### Default

N/A

### Command Mode

Configuration mode

### Applicability

This command was introduced in OcNOS-SP version 5.0.

### Example

```
#configure terminal
(config)# time-range TIMER1
(config-tr)#?
```

Time Range configuration commands:

WORD	String
abort	Abort Transaction
commit	commit
end	End current mode and change to EXEC mode
end-time	The end time for the Time Range
exit	End current mode and down to previous mode
frequency	The frequency of the Time Range
help	Description of the interactive help system
no	Delete
quit	Exit current mode and down to previous mode
show	Show running system information
start-time	The start time for the Time Range





---

## CHAPTER 29 Traffic Mirroring Commands

---

This chapter provides a description of syntax, and examples for Traffic Mirroring. It includes the following commands:

- `monitor session`
- `monitor session shut`
- `source port`
- `source vlan`
- `destination port`
- `no shut`
- `shut`
- `filter`
- `description`
- `remote destination`
- `show monitor`
- `show monitor session`
- `show filter`
- `show monitor running configuration`

---

## 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

<code>&lt;1-18&gt;</code>	Session number
<code>local</code>	Create a local session
<code>remote</code>	Create a remote source node session
<code>all</code>	All sessions

### Default

By default, monitor session type is local and will not be active by default

### Command Mode

Configure 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
```

---

## 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

Configure 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
```

---

## source port

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.

`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: source interface xe10 rx
source interface xe10 tx → running-config: source interface xe10 both
```

its direction is changed to as follows

```
source interface xe10 rx → running-config: source interface xe10 rx
source interface xe10 tx → running-config: 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 configure 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.

### 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 configure 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
```

---

## destination port

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.

### Command Syntax

```
destination interface IFNAME
no destination interface IFNAME
```

### Parameters

IFNAME	Interface name
--------	----------------

### Default

No default value is specified

### Command Mode

Monitor configure 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
```

---

## 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 configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#no shut
```

---

## 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 configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#shut
```



## 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.

### Command Syntax

```
(<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 |))}
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.

### Command Mode

Monitor configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#35 filter vlan 200
(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)#no 10 filter  
(config-monitor)#no 20 filter  
(config-monitor)#no 35 filter
```

---

## 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 configure 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
```

---

## 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 configure 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
```

# 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

Exec mode and Privileged Exec 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
```

Table 29-85 explains the output fields.

Table 29-85: show monitor fields

Entry	Description
Session admin shut	If the monitoring session is administratively shutdown, session will be in this state. This is the default state for any newly created monitoring session. Monitoring sessions can be activated using the command 'no shut' on monitoring session mode.
Dst in wrong mode	If both source and destination is configured on monitoring session and session is activated, then:  1. In case of local monitoring, if the destination port is not configured with 'switchport' or the destination is associated with bridge, then session will be in this state. Destination port shouldn't participate in regular switching. Hence this configuration state is mandatory.  2. In case of remote monitoring, if the reflector port is not configured with 'switchport' or the destination is associated with bridge and/or if remote VLAN is part of bridge then session will be in this state. Remote VLAN ID used for encapsulation should be unused VLAN ID by bridge on the mirroring node.
No sources configured	If no source configured on the monitoring session (either source VLAN or source ports) and monitoring session is activated, then the session will be in this state. In order to recover, source needs to be configured on the monitoring session. Multiple sources can be configured on a monitoring session.
No dest configured	If a session is not configured with destination (either destination port in case of local monitoring or with remote vlan and reflector port in case of remote monitoring) and if the monitoring session is activated, then session will be in this state. In order to recover, destination needs to be configured on the monitoring session. Only one destination can be configured per monitoring session.

**Table 29-85: show monitor fields**

Entry	Description
No operational src/dst	If both source and destination configured on monitoring session, destination is configured in right mode and session is activated, but <ol style="list-style-type: none"><li>1. In case of local monitoring, if the destination port link state is down, then session will be in this state.</li><li>2. In case of remote monitoring, if the reflector port link state is down, then session will be in this state.</li><li>3. In case the sources configured are ports and none of them are in link up state, then session will be in this state.</li><li>4. In case the sources configured are VLAN and none of the VLANs are part of bridge forwarding, then session will be in this state.</li></ol>
No hardware resource	If all the configurations are correct and multiple sessions are configured and activated, then one of the hardware limitation may be reached: <ol style="list-style-type: none"><li>1. Destination port exceeding maximum limit.</li><li>2. Filters exceeding maximum limit.</li><li>3. VLAN source ports exceeding maximum limit.</li></ol> In these cases, effected sessions will be in this state.
Hardware failure	If all the configurations are correct and sessions are activated but due to some expected or unexpected cases if the configuration cannot be applied in hardware, then the session will be in this state. This is not accepted state for a session and the issue needs to be analyzed and fixed.

---

## 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

Exec mode or Privileged Exec 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 29-86 explains the output fields.

**Table 29-86: show monitor session output fields**

Entry	Description
Type	Type of monitor session.
State	State of the security flow filter. There are different error messages when you do RSPAN configuration: <ol style="list-style-type: none"> <li>1. Session admin shut</li> <li>2. Dst in wrong mode</li> <li>3. No sources configured</li> <li>4. No dest configured</li> <li>5. No operational src/dst</li> <li>6. No hardware resource</li> <li>7. Hardware failure.</li> </ol>
Session admin shut	If the monitoring session is administratively shutdown, session will be in this state. This is the default state for any newly created monitoring session. Monitoring sessions can be activated using the command 'no shut' on monitoring session mode.
Dst in wrong mode	If both source and destination is configured on monitoring session and session is activated, then: <ol style="list-style-type: none"> <li>1. In case of local monitoring, if the destination port is not configured with 'switchport' or the destination is associated with bridge, then session will be in this state. Destination port shouldn't participate in regular switching. Hence this configuration state is mandatory.</li> <li>2. In case of remote monitoring, if the reflector port is not configured with 'switchport' or the destination is associated with bridge and/or if remote VLAN is part of bridge then session will be in this state. Remote VLAN ID used for encapsulation should be unused VLAN ID by bridge on the mirroring node.</li> </ol>
No sources configured	If no source configured on the monitoring session (either source VLAN or source ports) and monitoring session is activated, then the session will be in this state. In order to recover, source needs to be configured on the monitoring session. Multiple sources can be configured on a monitoring session.
No dest configured	If a session is not configured with destination (either destination port in case of local monitoring or with remote vlan and reflector port in case of remote monitoring) and if the monitoring session is activated, then session will be in this state. In order to recover, destination needs to be configured on the monitoring session. Only one destination can be configured per monitoring session.
No operational src/dst	If both source and destination configured on monitoring session, destination is configured in right mode and session is activated, but: <ol style="list-style-type: none"> <li>1. In case of local monitoring, if the destination port link state is down, then session will be in this state.</li> <li>2. In case of remote monitoring, if the reflector port link state is down, then session will be in this state.</li> <li>3. In case the sources configured are ports and none of them are in link up state, then session will be in this state.</li> <li>4. In case the sources configured are VLAN and none of the VLANs are part of bridge forwarding, then session will be in this state.</li> </ol>
No hardware resource	If all the configurations are correct and multiple sessions are configured and activated, then one of the hardware limitation may be reached: <ol style="list-style-type: none"> <li>1. Destination port exceeding maximum limit.</li> <li>2. Filters exceeding maximum limit.</li> <li>3. VLAN source ports exceeding maximum limit.</li> </ol> In these cases, effected sessions will be in this state.
Hardware failure	If all the configurations are correct and sessions are activated but due to some expected or unexpected cases if the configuration cannot be applied in hardware, then the session will be in this state. This is not accepted state for a session and the issue needs to be analyzed and fixed.



**Table 29-86: show monitor session output fields**

Entry	Description
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.

---

## 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

Exec mode or Privileged Exec 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 address : 2.2.2.8
-----

match set 3
-----
destination mac address : 0000.0001.1453 (host)
frame type : ipv4
source ip address : 3.3.3.5
#
```

---

## 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

Exec mode or Privileged Exec 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

#
```



---

## CHAPTER 30 Trigger Failover Commands

---

This chapter describes the trigger failover (TFO) commands.

- `clear tfo counter`
- `fog`
- `fog tfo`
- `fog type`
- `link-type`
- `show tfo`
- `tfo`

---

## clear tfo counter

Use this command to clear the TFO counters. If you do not specify a parameter, this command clears counters for all FOG indexes.

### Command Syntax

```
clear tfo counter
clear tfo counter fog <1-64>
```

### Parameters

<1-64>	Clear counters for this Failover Group Index
--------	--

### Default

None

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear tfo counter
```

---

## fog

Use this command to:

- Create or delete a failover group (FOG)
- Enable or disable an existing FOG

Even if FOG index does not exist, FOG can be created as enabled with “enable” option in CLI.

If the FOG index already exists:

- When the FOG status is disabled and Control Port Group (CPG) links are previously disabled (because of TFO), then the links are enabled. If a particular CPG member belongs to multiple CPGs, then this CPG member is enabled only if all corresponding Monitor Port Groups (MPG) are enabled.
- When the FOG status is enabled and MPG is down, then the corresponding CPG links are disabled.

Use the `no` form of this command to delete a FOG.

### Command Syntax

```
fog <1-64> (enable|disable)
no fog <1-64>
```

### Parameters

<1-64>	Failover Group Index
enable	Enable Failover Group
disable	Disable Failover Group

### Default

None

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#fog 5 enable
```

---

## fog tfc

Use this command to set the number of links to trigger failover for a Monitor Port Groups (MPG).

### Command Syntax

```
fog <1-64> tfc <0-63>
```

### Parameters

<1-64>	Failover Group index
<0-63>	Trigger failover count

### Default

None

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#fog 5 tfc 7
```



---

## fog type

Use this command to map upstream/downstream links in a FOG as a Monitor Port Group (MPG) or Control Port Group (CPG).

Use the `no` form of this command to unmap upstream/downstream links.

### Command Syntax

```
fog <1-64> type (mpg|cpg)
no fog <1-64> type (mpg|cpg)
```

### Parameters

<1-64>	Failover Group Index
mpg	Map the interface to an MPG
cpg	Map the interface to a CPG

### Default

None

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
#interface eth1
(config-if)#fog 5 type mpg
```

---

## link-type

Use this command to make a port an uplink or downlink.

Use the `no` form of this command to remove the configuration.

### Command Syntax

```
link-type (uplink|downlink)
no link-type
```

### Parameters

uplink	Make the port an uplink
downlink	Make the port a downlink

### Default

None

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
#interface eth1
(config-if)#link-type downlink
```

# show tfo

Use this command to display FOG configuration and statistics.

## Command Syntax

```
show tfo
```

## Parameters

None

## Default

None

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#show tfo
TFO : Enable

Failover Group 1 : Enable
Failover Status : MPG Link Failure
No. of links to trigger failover : 0
MPG Port(s) :
xe9    Status : DOWN
xe12   Status : DOWN
CPG Port :
xe4    Status : DOWN
No. of times MPG link failure : 1
No. of times MPG link recovered : 0
No. of times CPG got auto disabled : 1
No. of times CPG got auto enable : 0
```

Table 30-87 Explains the show command output fields.

Table 30-87: show tfo output fields

Field	Description
Failover Group	Enable the failover group.
Failover Status	Display the failover status.
No. of links to trigger failover	Number of links to trigger the failover group.

Field	Description
MPG Port	Details of the monitor port group.
CPG Port	Details of the control port group.

---

## tfo

Use this command to enable or disable trigger failover (TFO).

### Command Syntax

```
tfo (enable|disable)
```

### Parameters

enable	Enables Trigger failover
disable	Disables Trigger failover

### Default

By default, TFO is disabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal  
(config)#tfo enable
```



## CHAPTER 31 User Management

---

This chapter is a reference for user management commands.

This chapter includes these commands:

- `clear aaa local user lockout username`
- `clear line`
- `clear user`
- `debug user-mgmt`
- `show user-account`
- `username`

---

## clear aaa local user lockout username

Use this command to unlock the locked user due to three times wrong password login attempt.

### Command Syntax

```
clear aaa local user lockout username USERNAME
```

### Parameters

USERNAME	User name; length 2-15 characters
----------	-----------------------------------

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#clear aaa local user lockout username testuser
```



---

# clear line

Use this command to clear or close the already opened vty line sessions.

## Command Syntax

```
clear line WORD
```

## Parameters

WORD Enter the Location name (Max Size 64)

## Command Mode

Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
#show users
Current user      : (*).  Lock acquired by user : (#).
CLI user          : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

TYPE      Line      User      Idle      Location/Session  PID
(*) 130 vty 0      [C]ocnos      0d00h00m      pts/0
16725 Local network-admin
#clear line pts/0
Connection closed by foreign host.
-bash-4.1#
```

---

## clear user

Use this command to clear or close the already opened sessions based on the username.

Note: This command will close active telnet sessions if the account being cleared is already active, however the SSH sessions will continue to persist until disconnect.

### Command Syntax

clear user WORD

### Parameters

WORD Enter the username (Max Size 28)

### Command Mode

Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show users
Current user      : (*).  Lock acquired by user : (#).
CLI user         : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.
```

	Line	User	Idle	Location/Session	PID
TYPE	Role				
(*)	130 vty 0	[C]ocnos	0d00h00m	pts/0	
16725	Local	network-admin			

```
#clear user ocnos
Connection closed by foreign host.
-bash-4.1#
```

---

## debug user-mgmt

Use this command to display user management debugging information.

Use the `no` form of this command stop displaying user management debugging information.

### Command Syntax

```
debug user-mgmt
no debug user-mgmt
```

### Parameters

None

### Default

By default, disabled.

### Command Mode

Exec mode and Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#debug user-mgmt

#config t
(config)#debug user-mgmt
```

---

## show user-account

Use this command to display information about all users or a given user.

### Command Syntax

```
show user-account (WORD|)
```

### Parameters

WORD	User name
------	-----------

### Command Mode

Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#show user-account
User:user1
roles: network-operator
User:user2
roles: network-operator
User:user3
roles: network-operator
```

# username

Use this command to add a user or to change a user password.

The `role` parameter maps to privilege levels in the TACACS+ server as shown in [Table 31-88](#)

Table 31-88: Role/privilege level mapping

Role	Privilege level
Network administrator	15
Network engineer	14
Network operator	1 to 13
Network user	0 or greater than 15

Use the `no` form of this command to remove a user.

## Command Syntax

```
username USERNAME
username USERNAME password (encrypted|) PASSWORD
username USERNAME role (network-admin|network-engineer|network-operator|network-user)
username USERNAME role (network-admin|network-engineer|network-operator|network-user) password (encrypted|) PASSWORD
username USERNAME (role (network-admin|network-engineer|network-operator|network-user|ROLE-NAME)|) password (encrypted|) PASSWORD
username disable-default
no username disable-default
no username USERNAME
```

## Parameters

USERNAME	Name of the user (2-15 alphanumeric characters)
encrypted	Encrypted password
PASSWORD	Password; length 5-32 characters
network-admin	Network administrator role with all access permissions that can make permanent changes to the configuration. Changes persist after a reset/reboot of the switch.  Only network administrators can manage other users with the <a href="#">enable password</a> , <a href="#">Authentication, Authorization and Accounting</a> , <a href="#">RADIUS</a> , and <a href="#">TACACS+</a> commands.
network-engineer	Network engineer role with all access permission that can make permanent changes to the configuration. Changes persist after a reset/reboot of the switch.
network-operator	Network operator role with all access permissions that can make temporary changes to the configuration. Changes do not persist after a reset/reboot of the switch.

<code>network-user</code>	Network user role with access permissions to display the configuration, but cannot change the configuration.
<code>ROLE-NAME</code>	Refers to an user-defined RBAC role
<code>disable-default</code>	

This option is used to disable the implicit configuration of default user by the system. This command can be executed only by users with “`network-admin`” privileges. When this option is configured, explicit configuration of default user will be rejected. If default-user is explicitly configured using “`username`” CLI, it should be removed using “`no username USERNAME`” before configuring “`disable-default`”.

### Default

By default, user name is disabled.

### Command Mode

Configure mode

### Applicability

This command was introduced before OcNOS version 1.3.

### Example

```
#configure terminal
(config)#username fred_smith password fred123
```

## CHAPTER 32 VLOG Commands

---

This chapter describes virtual router log (VLOG) commands.

- [show vlog all](#)
- [show vlog clients](#)
- [show vlog terminals](#)
- [show vlog virtual-routers](#)

# show vlog all

Use this command to display the output of all virtual router log `show` commands. For column descriptions, refer to descriptions of the individual commands.

## Command Syntax

```
show vlog all
```

## Parameters

None

## Default

None

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
>enable
#show vlog all
```

Type	Name	FD	UserVR	AllVrs	VRCnt
tty	/dev/pts/8	12	vr222	---	1
tty	/dev/pts/4	13	<PVR>	---	1

VR-Name	VR-Id	PVR-Terms	VR-Terms	LogFile
CurSize				
<PVR>	0	1	0	/var/local/zebos/log/pvr/my-log
1624320				
vr111	1	0	0	n/a
n/a				
vr222	2	0	1	/var/local/zebos/log/vr222/log-
vr222	0			
vr333	3	0	0	/var/local/zebos/log/vr333/log-
vr333	0			

Name	Id	MsgCnt	ConTime	ReadTime
NSM	1	1	Fri May-15 21:05:04	Fri May-15 21:05:04
IMI	19	1	Fri May-15 21:05:02	Fri May-15 21:05:02



---

# show vlog clients

Use this command to display all attached virtual router log clients (protocol modules).

## Command Syntax

```
show vlog clients
```

## Parameters

None

## Default

None

## Command Mode

Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
>enable
#show vlog clients
```

Name	Id	MsgCnt	ConTime	ReadTime
NSM	1	1	Fri May-15 21:05:04	Fri May-15 21:05:04
IMI	19	1	Fri May-15 21:05:02	Fri May-15 21:05:02

[Table 32-89](#) explains the output:

**Table 32-89: Virtual router log clients**

Name	Name of protocol module
Id	Protocol module identifier
MsgCnt	Number of log messages received from protocol module
ConTime	Time the connection was established
ReadTime	Time the last log message was received

# show vlog terminals

Use this command to display all active connections where VLOGD is forwarding log output.

## Command Syntax

```
show vlog terminals
```

## Parameters

None

## Default

None

## Command Mode

Privileged exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
>enable
#show vlog terminals

Type      Name      FD  UserVR  AllVrs  VRCnt
tty       /dev/pts/8  12  vr222   ---     1
tty       /dev/pts/4  13  <PVR>   ---     1
```

Table 32-90 explains the output:

Table 32-90: Virtual router log terminals

Type	Type of terminal
Name	Device name
FD	File descriptor
UserVR	Name of the Virtual Router where in which the user is logged in
AllVRs	Whether the PVR user requested debug output from all VRs
VRCnt	Number of VRs to which a terminal is attached

# show vlog virtual-routers

Use this command to display virtual router statistics such as the number of terminals attached.

## Command Syntax

```
show vlog virtual-routers
```

## Parameters

None

## Default

None

## Command Mode

Privileged exec mode

## Applicability

This command was introduced before OcNOS version 1.3.

## Example

```
>enable
#show vlog virtual-routers

VR-Name  VR-Id  PVR-Terms  VR-Terms  LogFile
CurSize
<PVR>      0   1           0          /var/local/zebos/log/pvr/my-log
1624320
vr111      1   0           0          n/a
vr222      2   0           1          /var/local/zebos/log/vr222/log-vr222
vr333      3   0           0          /var/local/zebos/log/vr333/log-vr333
```

Table 32-91 explains the output:

Table 32-91: Virtual router statistics

VR-Name	Virtual router name
VR-Id	Virtual router identifier
PVR-Terms	Number of attached PVR terminals
VR-Terms	Number of attached VR terminals
LogFile	Name of VR log file (this column is empty if writing to a log file is disabled)
CurSize	Log file current size



## CHAPTER 33 FMS Command Reference

---

This chapter describes the fault management system (FMS) commands:

- [fault-management \(enable | disable\)](#)
- [fault-management close](#)
- [fault-management flush-db](#)
- [fault-management shelve](#)
- [show alarm active](#)
- [show alarm closed](#)
- [show alarm history](#)
- [show alarm shelved](#)
- [show alarm statistics](#)
- [show alarm transitions](#)
- [show fms status](#)
- [show fms supported-alarm-types](#)
- [show running-config fault-management](#)

---

## fault-management (enable | disable)

Use this command to enable or disable the fault management system (FMS).

### Command Syntax

```
fault-management (enable | disable)
```

### Parameters

enable	Enable FMS
disable	Disable FMS

### Command Mode

Configuration mode

### Applicability

This command was introduced in OcNOS version 3.0.

### Example

```
(config)#fault-management enable
(config)#fault-management disable
(config)#
```

---

## fault-management close

Use this command to close an active alarm.

### Command Syntax

```
fault-management close ACTIVE-ALARM-ID
```

### Parameter

ACTIVE-ALARM-ID

Identifier of an active alarm

### Command Mode

Exec and Privileged Exec mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
#fault-management close CMM_MONITOR_CPU:15min_load:CPU
CMM_MONITOR_CPU:15min_load:CPU closed.
#
```

---

## fault-management flush-db

Use this command to flush the alarms from the database.

### Command Syntax

```
fault-management flush-db
```

### Parameter

None

### Command Mode

Exec and Privileged Exec mode

### Applicability

This command was introduced in OcNOS version 3.0.

### Example

```
#fault-management flush-db
```



---

## fault-management shelve

Use this command to shelve (disable) an alarm type.

### Command Syntax

```
fault-management shelve ALARM-TYPE
```

### Parameter

`ALARM-TYPE`      Type of alarm as displayed by [show fms supported-alarm-types](#)

### Command Mode

Exec and Privileged Exec mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
#fault-management shelve CMM_MONITOR_CPU
CMM_MONITOR_CPU shelved.
#
```

---

## show alarm active

Use this command to display the current active alarms in the database.

### Command Syntax

```
show alarm active
```

### Parameters

None

### Command Mode

Exec and Privileged Exec mode

### Applicability

This command was introduced in OcNOS version 3.0.

### Example

```
#show alarm active
Active Alarms received:-
Active-Alarms-Count: 1
Alarm-Date-Time          Severity      Alarm-ID          Alarm-Description
-----
2019-02-15T19:57:14.525Z  MAJOR        IFMGR_IF_DOWN::xe8  OcNOS [IFMGR_IF_DOWN]
Interface xe8 changed state to down
#
```

---

# show alarm closed

Use this command to display alarms that are manually closed.

## Command Syntax

```
show alarm closed
```

## Parameters

None

## Command Mode

Exec and Privileged Exec mode

## Applicability

This command was introduced in OcNOS version 6.0.

## Example

```
#show alarm closed
Alarm Count: 1
Severity    Alarm_Type_ID  Alarm_ID          Description
-----
MAJOR      EQPT                IFMGR_IF_DOWN::xe7  FMS [IFMGR_IF_DOWN] Interface xe7
changed state to down

#
```

---

## show alarm history

Use this command to show the alarm history.

### Command Syntax

```
show alarm history (1-day | 1-hr | 1-week | all)
```

### Parameters

1-day	Display alarms in the last 1 day
1-hr	Display alarms in the last 1 hour
1-week	Display alarms in the last 1 week
all	Display all the alarms

### Command Mode

Exec and Privileged Exec mode

### Applicability

This command was introduced in OcNOS version 3.0.

### Example

```
#show alarm history ?  
1-day    Display alarms in the last 1 day  
1-hr     Display alarms in the last 1 hour  
1-week   Display alarms in the last 1 week  
all      Display all the alarms
```

---

## show alarm shelved

Use this command to display shelved (disabled) alarm types.

### Command Syntax

```
show alarm shelved
```

### Parameters

None

### Command Mode

Exec and Privileged Exec mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
#show alarm shelved
Alarm-type Count: 1
Alarm Type
-----
IFMGR_IF_DOWN

#
```

---

## show alarm statistics

Use this command to display the alarm statistics.

### Command Syntax

```
show alarm statistics
```

### Parameters

None

### Command Mode

Exec and Privileged Exec mode

### Applicability

This command was introduced in OcNOS version 3.0.

### Example

```
#show alarm statistics
Alarm Statistics received:-
Alarm Count: 0
Severity      Count      Alarm Description
#
```

---

# show alarm transitions

Use this command to display severity transitions for every alarm in the device.

## Command Syntax

```
show alarm transitions
```

## Parameters

None

## Command Mode

Exec and Privileged Exec mode

## Applicability

This command was introduced in OcNOS version 6.0.

## Example

```
#show alarm transitions
Alarms received:-
Alarm Count: 3
Transition      From      To      Alarm ID
Downgraded      CRITI     MAJOR   CMM_MONITOR_CPU:1min_load:CPU
Upgraded        MAJOR     CRITI   CMM_MONITOR_CPU:1min_load:CPU
Downgraded      CRITI     MAJOR   CMM_MONITOR_CPU:1min_load:CPU

#
```

---

## show fms status

Use this command to display the FMS status.

### Command Syntax

```
show fms status
```

### Parameters

None

### Command Mode

Exec and Privileged Exec mode

### Applicability

This command was introduced in OcNOS version 3.0.

### Example

```
#
#show fms status
% FMS Status: Enabled
% FMS Node Application Status: Up
#
```



---

## show fms supported-alarm-types

Use this command to display the supported alarm types.

### Command Syntax

```
show fms supported-alarm-types
```

### Parameters

None

### Command Mode

Exec and Privileged Exec mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
#show fms supported-alarm-types
Alarm-types Count: 38
```

```
IFMGR_IF_DOWN
IFMGR_IF_UP
CMM_MONITOR_RAM
CMM_MONITOR_CPU
...
#
```

---

## show running-config fault-management

Use this command to display FMS status in the running configuration.

### Command Syntax

```
show running-config fault-management
```

### Parameters

None

### Command Mode

Exec and Privileged Exec mode

### Applicability

This command was introduced in OcNOS version 3.0.

### Example

```
#show running-config fault-management
!
fault-management enable
!
#
```

## CHAPTER 34 NetConf Call Home Commands

---

This chapter describes these commands:

- [callhome server](#)
- [debug callhome](#)
- [feature netconf callhome](#)
- [management-port](#)
- [netconf callhome](#)
- [reconnect](#)
- [retry-interval](#)
- [retry-max-attempts](#)
- [show \(xml\) running-config netconf-callhome](#)

---

## callhome server

Use this command to add a call home server. A maximum 5 servers can be configured.

Reconnect and debug configurations present at the time of server addition will be applied. Reconnect and debug configurations done later are applied only to newly added servers.

Use the `no` form of this command to delete a call home server. If the specified call home server is already connected with the OcNOS NetConf server, deleting it will not disconnect it.

### Command Syntax

```
callhome server WORD (A.B.C.D|X:X::X:X|HOSTNAME) (port <1-65535>|)
no callhome server WORD
```

### Parameters

WORD	An arbitrary name for the NetConf listen endpoint. Any valid string with length 1-64 can be used.
A.B.C.D	IPv4 address of the call home server
X:X::X:X	IPv4 address of the call home server
HOSTNAME	Host name of the call home server
<1-65535>	Callhome server listening port

**Note:** The same address can be configured with different endpoint names, so use a different port number in those cases. For example:

```
callhome server name-1 1.1.1.1
callhome server name-2 1.1.1.1 # Avoid this is kind of redundant configuration
callhome server name-3 1.1.1.1 5555
```

### Default

Default value for the port is IANA assigned port 4334.

### Mode

NetConf call home mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
!
(netconf-callhome)#
(netconf-callhome)#callhome server remote-client 169.154.45.12
(netconf-callhome)#callhome server nat-client 192.168.56.1 port 12234
(netconf-callhome)#commit
(netconf-callhome)#
```

```
config)#do show running-config netconf-callhome
(config)#
OcNOS(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
  callhome server remote-client 169.154.45.12
  callhome server nat-client 192.168.56.1 port 12234
!
(netconf-callhome)#
(netconf-callhome)#no callhome server nat-client
(netconf-callhome)#commit
(netconf-callhome)#
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
  callhome server remote-client 169.154.45.12
!
(netconf-callhome)#
```

---

## debug callhome

Use this command to enable debugging for the call home module. Once enabled, all debugging related information will be logged in the system logger file.

Use the `no` form of this command to disable debugging for the call home module.

### Command Syntax

```
debug callhome
no debug callhome
```

### Parameters

None

### Default

By default, debugging is disabled (only critical message are enabled).

### Mode

NetConf call home mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
(config) #
(config) #netconf callhome
(netconf-callhome) #do show running-config netconf-callhome
(netconf-callhome) #
(netconf-callhome) #debug callhome
(netconf-callhome) #commit
(netconf-callhome) #
(netconf-callhome) #do show running-config netconf-callhome
!
netconf callhome
  debug callhome
!
(netconf-callhome) #no debug callhome
(netconf-callhome) #commit
(netconf-callhome) #do show running-config netconf-callhome
(netconf-callhome) #
```

---

## feature netconf callhome

Use this command to enable or disable the NetConf call home feature. When the feature is disabled, all other configurations are removed except [debug callhome](#).

Enabling the call home feature is required before doing any other call home configurations.

### Command Syntax

```
feature netconf callhome (enable|disable)
```

### Parameters

enable	Enable the call home feature
disable	Disable the call home feature

### Default

By default, the call home feature is disabled.

### Mode

NetConf call home mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
(config)#do show running-config netconf-callhome
(config)#
(config)#netconf callhome
(netconf-callhome)#feature netconf callhome enable
(netconf-callhome)#commit
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
!
(netconf-callhome)#feature netconf callhome disable
(netconf-callhome)#commit
(netconf-callhome)#
(netconf-callhome)#do show running-config netconf-callhome
(netconf-callhome)#
```

---

## management-port

Use this command to add an interface to use to connect to a call home server. This is useful when in-band (front panel) ports are used as management ports.

Use the `no` form of this command to use eth0 as the management port.

### Command Syntax

```
management-port IFNAME
no management-port
```

### Parameters

IFNAME	Interface used to connect to the call home server
--------	---

### Default

By default, eth0 (out-of-band management port) is used as the management port.

### Mode

NetConf call home mode

### Applicability

This command was introduced in OcNOS version 6.0

### Example

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
!

(netconf-callhome)#management-port xe4
(netconf-callhome)#commit
(netconf-callhome)#
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
  management-port xe4
!
(netconf-callhome)#no management-port
(netconf-callhome)#commit
(netconf-callhome)#
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
!
(netconf-callhome)#
```



---

## netconf callhome

Use this command to enter NetConf call home configuration mode. All call home configurations are done in this mode.

### Command Syntax

```
netconf callhome
```

### Mode

Configure mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
(config)#netconf callhome
(netconf-callhome)#
```

---

## reconnect

Use this command to enable or disable the reconnect feature. If disabled, OcNOS only tries once and if it fails, the connection will not be re-attempted.

Reconnect-related configuration ([retry-interval](#), [retry-max-attempts](#)) at the time of server addition will be applicable to that server. Any update in reconnect configuration will get applied only to new servers added later (not to pre-existing servers).

### Command Syntax

```
reconnect (enable|disable)
```

### Parameters

enable	Enable reconnect
disable	Disable reconnect

### Default

By default, the reconnect feature is not enabled.

### Mode

NetConf call home mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
!
(netconf-callhome)#reconnect enable
(netconf-callhome)#commit
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
  reconnect enable
!
(netconf-callhome)#retry-max-attempts 10
(netconf-callhome)#retry-interval 30
(netconf-callhome)#commit
(netconf-callhome)#
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
  reconnect enable
```

```
retry-max-attempts 10
retry-interval 30
!
(netconf-callhome)#reconnect disable
(netconf-callhome)#commit
(netconf-callhome)#
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
!
(netconf-callhome)#
```

---

## retry-interval

Use this command to specify the number of seconds to wait after a connect attempt to the call home server fails.

Use the `no` form of this command to reset the retry interval to its default (300 seconds).

### Command Syntax

```
retry-interval <1-86400>
no retry-interval
```

### Parameters

<1-86400>	Retry interval in seconds
-----------	---------------------------

### Default

By default, when the [reconnect](#) feature is enabled, the default retry interval is 300 seconds.

### Mode

NetConf call home mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
  reconnect enable
!

(netconf-callhome)#retry-interval 100
(netconf-callhome)#commit
(netconf-callhome)#
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
  reconnect enable
  retry-interval 100
!
(netconf-callhome)#

(netconf-callhome)#no retry-interval
(netconf-callhome)#commit
(netconf-callhome)#
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
```

```
feature netconf callhome enable
reconnect enable
!
(netconf-callhome) #
```

---

## retry-max-attempts

Use this command to specify the number of retries the OcNOS should attempt to the call home server before giving up. Use the `no` form of this command to reset the maximum attempts to its default (3).

### Command Syntax

```
retry-max-attempts <1-255>
no retry-max-attempts
```

### Parameters

<1-255>	Number of retries
---------	-------------------

### Default

By default, when the [reconnect](#) feature is enabled, 3 attempts will be made.

### Mode

NetConf call home mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
  reconnect enable
!

(netconf-callhome)#retry-max-attempts 10
(netconf-callhome)#commit
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
  reconnect enable
  retry-max-attempts 10
!

(netconf-callhome)#no retry-max-attempts
(netconf-callhome)#commit
(netconf-callhome)#
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
  feature netconf callhome enable
  reconnect enable
```

```
!  
(netconf-callhome) #
```

---

## show (xml|) running-config netconf-callhome

Use this command to display call home configurations.

### Command Syntax

```
show (xml|) running-config netconf-callhome
```

### Parameters

xml	Display the output in XML format
-----	----------------------------------

### Mode

Exec mode

### Applicability

This command was introduced in OcNOS version 6.0.

### Example

```
#show running-config netconf-callhome
!
```

```
netconf callhome
  feature netconf callhome enable
  management-port xe10
  reconnect enable
  retry-max-attempts 10
  retry-interval 100
  callhome server local-nc 192.168.56.1
  debug callhome
!
```

```
#show xml running-config netconf-server
<netconf-server xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-management-server">
  <callhome>
    <feature-enabled></feature-enabled>
    <management-port>xe10</management-port>
    <netconf-client>
      <name>local-nc</name>
      <address>192.168.56.1</address>
    </netconf-client>
    <reconnect>
      <enable></enable>
      <retry-max-attempts>10</retry-max-attempts>
      <retry-interval>100</retry-interval>
    </reconnect>
  </callhome>
  <debug>
    <callhome-debug></callhome-debug>
  </debug>
</netconf-server>
```



## CHAPTER 35 Internet Protocol Security Commands

---

This chapter is a reference for the Internet Protocol Security (IPsec) commands.

- [crypto ipsec transform-set](#)
- [crypto map \(Configure Mode\)](#)
- [mode](#)
- [set peer \(Sequence mode\)](#)
- [set session-key \(Sequence mode\)](#)
- [set transform-set \(Sequence mode\)](#)
- [sequence](#)
- [show crypto ipsec transform-set](#)

---

## crypto ipsec transform-set

Use this command to configure a transform set that defines protocols and algorithm settings to apply to IPSec protected traffic.

During the IPSec security association negotiation, the peers agree to use a particular transform-set to be used for protecting a particular data flow.

Several transform-sets can be specified and associated with a crypto map entry.

A transform set defines the IPSec security protocols: Encapsulation Security Protocol (ESP) or Authentication Header (AH), and also specifies which algorithms to use with the selected security protocol.

### Command Syntax

```
crypto ipsec transform-set NAME mode (transport|tunnel)
crypto ipsec transform-set NAME ah (none|ah-md5|ah-sha1|ah-sha256|ah-sha384|ah-sha512)
crypto ipsec transform-set NAME esp-auth (none|esp-md5|esp-sha1|esp-sha256|esp-sha384|esp-sha512) esp-enc (esp-null|esp-3des|esp-aes|esp-aes192|esp-aes256|esp-blf|esp-blf192|esp-blf256|esp-cast)
```

### Parameters

NAME	Name of the transform set.
mode	Change the transform-set mode to tunnel or transport.
ah	Authentication Header protocol provides data authentication.
none	No authentication.
ah-md5	Authentication Header with Message Digest 5 (MD5) Hashed Message Authentication Code (HMAC) variant.
ah-sha1	Authentication Header with Secure Hash Algorithm 1 (SHA-1) Hashed Message Authentication Code (HMAC) variant.
ah-sha256	Authentication Header with Secure Hash Algorithm 256 (SHA-256) Hashed Message Authentication Code (HMAC) variant.
ah-sha384	Authentication Header with Secure Hash Algorithm 384 (SHA-384) Hashed Message Authentication Code (HMAC) variant.
ah-sha512	Authentication Header with Secure Hash Algorithm 512 (SHA-512) Hashed Message Authentication Code (HMAC) variant.
esp-auth	Encapsulating Security Payload authentication protocol provides data authentication.
none	No authentication.
esp-md5	Encapsulating Security Payload with Message Digest 5 (MD5) Hashed Message Authentication Code (HMAC) variant.
esp-sha1	Encapsulating Security Payload with Secure Hash Algorithm 1 (SHA-1) Hashed Message Authentication Code (HMAC) variant.
esp-sha256	Encapsulating Security Payload with Secure Hash Algorithm 256 (SHA-256) Hashed Message Authentication Code (HMAC) variant.
esp-sha384	Encapsulating Security Payload with Secure Hash Algorithm 384 (SHA-384) Hashed Message Authentication Code (HMAC) variant.

esp-sha512	Encapsulating Security Payload with Secure Hash Algorithm 512 (SHA-512) Hashed Message Authentication Code (HMAC) variant.
esp-enc	Encapsulating Security Payload encryption protocol
esp-null	Encapsulating Security Payload null encryption.
esp-3des	Encapsulating Security Payload with 168-bit DES encryption (3DES or Triple DES).
esp-aes	Alternative AES.
esp-aes192	Alternative AES192.
esp-aes256	Alternative AES256.
esp-blf	Alternative Blowfish.
esp-blf192	Alternative Blowfish192.
esp-blf256	Alternative Blowfish256.
esp-cast	Alternative Cast (IKEv1 not supported).

## Command Mode

Configure mode

## Example

```
#configure terminal
(config)#crypto ipsec transform-set TEST_ESP esp-auth esp-md5 esp-enc esp-3des
(config)#crypto ipsec transform-set TEST_AH ah ah-sha512
```

---

## crypto map (Configure Mode)

Use this command to create or change a crypto map entry and enter crypto map configuration mode.

Use the `no` form of this command to delete a crypto map entry or set.

### Command Syntax

```
crypto map MAP-NAME ipsec-manual
no crypto map MAP-NAME
```

### Parameters

MAP-NAME	Name of the crypto map set (maximum length 127).
ipsec-manual	Do not use IKE to establish IPSec security associations.

### Command Mode

Configure mode

### Example

```
(config)#crypto map MAP1 5 ipsec-manual
(config-crypto)#
```

---

## mode

Use this command to set the mode of negotiation for a transform set.

Use the `no` form of this command to reset the mode to its default (tunnel).

### Command Syntax

```
mode (tunnel|transport)
no mode
```

### Parameter

tunnel	The entire original IP packet is protected (default).
transport	The payload (data) of the original IP packet is protected.

### Defaults

Tunnel mode

### Command Mode

Transform set mode

### Example

```
(config)#crypto ipsec transform-set TEST_ESP mode transport
(config-transform)#mode transport
```

---

## set peer (Sequence mode)

Use this command to specify an IPSec peer IPv4 or IPv6 for a crypto map.

### Command syntax

```
set peer (A.B.C.D | X:X::X:X) (spi (<0-4096>)|)
```

### Parameters

A.B.C.D	IPv4 peer address
X:X::X:X	IPv6 peer address
spi	Specifies the security parameter index (SPI), a number that is used to uniquely identify a security association.
<0-4096>	Security parameter index (SPI) range

### Default

None

### Command Mode

Crypto map sequence mode

### Applicability

This command is introduced in OcNOS version 6.0

### Examples

```
#configure terminal
(config)#crypto map MAP1 ipsec-manual
(config-crypto)#sequence 1
(config-crypto-seq)#set transform-set TEST_ESP
(config-crypto-seq)#set peer fe80::3617:ebff:fe0e:1222 spi 200
```

---

## set session-key (Sequence mode)

Use this command to define IPSec keys for security associations via ipsec-manual crypto map entries.

When you define multiple IPSec session keys within a single crypto map, you can assign the same security parameter index (SPI) number to all the keys. The SPI is used to identify the security association used with the crypto map.

Session keys at one peer must match the session keys at the remote peer.

### Command syntax

```
set session-key (inbound|outbound) esp SPI cipher HEX-KEY-DATA authenticator HEX-KEY-DATA
no set session-key (inbound|outbound) esp SPI
```

### Parameters

inbound	Sets the inbound IPSec session key. Both inbound and outbound keys must be set.
outbound	Sets the outbound IPSec session key. Both inbound and outbound keys must be set.
esp	Sets the IPSec session key for the Encapsulation Security Protocol.
SPI	Specifies the security parameter index (SPI), a number that is used to uniquely identify a security association.
cipher	Indicates that the key string is to be used with the ESP encryption.
HEX-KEY-DATA	Specifies the session key in hexadecimal format.
authenticator	Indicates that the key string is to be used with the ESP authentication.

### Default

None

### Command Mode

Crypto map sequence mode

### Applicability

This command is introduced in OcNOS version 6.0

### Examples

```
#configure terminal
(config)#crypto map MAP1 ipsec-manual
(config-crypto)#sequence 1
(config-crypto-seq)#set session-key outbound esp 200 cipher
12345678123456781234567812345678123456781234567812345678 authenticator
123456781234567812345678
(config-crypto-seq)#set session-key inbound esp 200 cipher
12345678123456781234567812345678123456781234567812345678 authenticator
123456781234567812345678
```

---

## set transform-set (Sequence mode)

Use this command to specify which transform sets to include in a crypto map entry.

### Command syntax

```
set transform-set NAME
```

### Parameters

NAME	Transform-set name
------	--------------------

### Default

None

### Command Mode

Crypto map sequence mode

### Applicability

This command is introduced in OcNOS version 6.0

### Examples

```
#configure terminal
(config)#crypto map MAP1 ipsec-manual
(config-crypto)#sequence 1
(config-crypto-seq)#set transform-set TEST_ESP
```



---

## sequence

The number you assign to the seq-num will be used to rank multiple crypto map entries within a crypto map set. This number defines the priority of crypto-map evaluation within a crypto map set.

### Command syntax

```
sequence SEQ-NUM
```

### Parameters

SEQ-NUM	Crypto map sequence number
---------	----------------------------

### Default

None

### Command Mode

Crypto map mode

### Applicability

This command is introduced in OcNOS version 6.0

### Examples

```
#configure terminal
(config)#crypto map MAP1 ipsec-manual
(config-crypto)#sequence 1
(config-crypto-seq)#
```

---

## show crypto ipsec transform-set

Use this command to show the IPsec transform-set entries.

### Command syntax

```
show crypto ipsec transform-set NAME
```

### Parameters

NAME	Transform-set name
------	--------------------

### Default

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command is introduced in OcNOS version 6.0

### Examples

```
#show crypto ipsec transform-set TEST_ESP
Transform set t3
  Mode is Transport
  Algorithm none esp-3des esp-md5
```

## CHAPTER 36 Erbium-doped Fiber Amplifier Commands

---

This chapter is a reference for Erbium-doped fiber amplifier (EDFA) commands:

- [edfa operating-mode](#)
- [edfa target-gain](#)
- [edfa target-outpwr](#)
- [show edfa operating-mode](#)
- [show interface IFNAME transceiver](#)
- [show interface transceiver](#)
- [show interface IFNAME transceiver detail](#)
- [show interface transceiver detail](#)
- [show interface IFNAME transceiver threshold violations](#)
- [show interface transceiver threshold violations](#)

---

## edfa operating-mode

Use this command to configure EDFA interface operating-mode.

### Command Syntax

```
edfa operatingn-mode PARAM
```

### Parameters

PARAM	Specifies the operating-mode Automatic Power Control (apc) and Automatic Gain Control (agc).
-------	--

### Default

None

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 6.3.0.

### Example

```
OcNOS(config-if)#edfa operating-mode agc
OcNOS(config-if)#commit
```

---

## edfa target-gain

Use this command to configure EDFA interface target gain.

### Command Syntax

```
edfa target-gain VALUE
```

### Parameters

VALUE	Target gain value.
-------	--------------------

### Default

None

### Command Mode

Interface mode

### Applicability

This command was introduced in OcNOS version 6.3.0.

### Example

```
OcNOS(config-if)#edfa target-gain 15
OcNOS(config-if)#commit
```

---

## edfa target-outpwr

Use this command to configure EDFA interface target output power.

### Command Syntax

```
edfa target-outpwr VALUE
```

### Parameters

VALUE	Target output power value.
-------	----------------------------

### Default

None

### Command Mode

Interface mode

### Applicability

This command was introduced before OcNOS version 6.3.0.

### Example

```
OcNOS(config-if)#edfa target-outpwr 7
OcNOS(config-if)#commit
```

---

# show edfa operating-mode

Use this command for a EDFA operating-mode summary.

## Command Syntax

```
show edfa operating-mode
```

## Parameters

None

## Default

None

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 6.3.0.

## Example

```
OcNOS>show edfa operating-mode
```

```
Default Operating Mode      : AGC
Default Target OutPwr(BA)   : 17.000
Default Target OutPwr(PA)   : 7.000
Default Target Gain         : 17.000
```

-----	
Interface	Operating-Mode
-----	
ce5/1	AGC
ce7/1	AGC
ce11/1	AGC

## show interface IFNAME transceiver detail

Use this command to display EDFA attributes and their thresholds

### Command Syntax

```
show interface IFNAME transceiver detail
```

### Parameters

IFNAME                      Interface name

### Default

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 6.3.0.

### Example

```
OcNOS>show interface ce9/1 transceiver detail
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No
Power,  - Not Applicable
```

...

Intf	DDM	InPwr (dBm)	AlertMax (dBm)	CritMax (dBm)	CritMin (dBm)	AlertMin (dBm)
ce9/1	Inactive*	-2.00	-7.00	-9.00	-30.97	-32.22

Intf	DDM	OutPwr (dBm)	AlertMax (dBm)	CritMax (dBm)	CritMin (dBm)	AlertMin (dBm)
ce9/1	Inactive*	-7.00	+10.00	+8.00	-20.00	-20.97

Intf	DDM	PumpBias (Amp)	AlertMax (Amp)	CritMax (Amp)	CritMin (Amp)	AlertMin (Amp)
ce9/1	Inactive*	+0.35	+0.49	+0.45	+0.00	+0.00

Intf	DDM	Gain (dB)	AlertMax (dB)	CritMax (dB)	CritMin (dB)	AlertMin (dB)
ce9/1	Inactive*	+12.00	+26.00	+25.00	+8.00	+7.00

[Table 36-92](#) explains the output fields.



**Table 36-92: show interface transceiver details output**

Field	Description
Intf	Interface where the EDFA is present
DDM	Digital diagnostics monitor status for that particular interface
Inpwr	Input Power to the EDFA
OutPwr	Output Power from EDFA
PumpBias	Pump Bias
Gain	The total gain over the Input Power

---

## show interface IFNAME transceiver threshold violations

Use this command to show EDFA module input power, output power, pump bias and gain thresholds violations from a specific port.

### Command Syntax

```
show interface IFNAME transceiver threshold violations
```

### Parameters

IFNAME	Interface Name
--------	----------------

### Default

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 6.3.0.

### Example

```
OcNOS>show interface cell1/1 transceiver threshold violations
```

Intf	Lane	Timestamp	Type of alarm
----	----	-----	-----
cell1/1	1	02-14-2019 12:39:04	Pump Bias low alarm, value 0.000A threshold 0.000A
		02-14-2019 12:38:04	Gain low warning, value 7.500dB threshold 8.000dB
		02-14-2019 12:38:04	Output power low warning, value -11.000dBm threshold -10.000dBm
		02-14-2019 12:38:04	Input power low warning, value -21.000dBm threshold -20.969dBm

# show interface IFNAME transceiver

Use this command to show EDFA module input power, output power, pump bias and gain current values from a specific port.

## Command Syntax

```
show interface IFNAME transceiver
```

## Parameters

IFNAME                      Interface Name

## Default

None

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 6.3.0.

## Example

```
Cassini-3>show interface ce9/1 transceiver
Codes: * Not Qualified By IP Infusion, ** Not Supported By Module, -- No Power,
- Not Applicable

Intf      DDM      InPwr      OutPwr      PumpBias      Gain
      (dBm)      (dBm)      (Amp)      (dB)
-----
ce9/1      Inactive* -2.00      -7.00      +0.35      +12.00
OcNOS>show interface ce9/1 transceiver detail
Codes: * Not Qualified By IP Infusion, ** Not Supported By Module, -- No Power,
- Not Applicable

...

Intf      DDM      InPwr      AlertMax      CritMax      CritMin      AlertMin
      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-----
ce9/1      Inactive* -2.00      -7.00      -9.00      -30.97      -32.22

Intf      DDM      OutPwr      AlertMax      CritMax      CritMin      AlertMin
      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-----
ce9/1      Inactive* -7.00      +10.00      +8.00      -20.00      -20.97

Intf      DDM      PumpBias      AlertMax      CritMax      CritMin      AlertMin
      (Amp)      (Amp)      (Amp)      (Amp)      (Amp)      (Amp)
-----
ce9/1      Inactive* +0.35      +0.49      +0.45      +0.00      +0.00

Intf      DDM      Gain      AlertMax      CritMax      CritMin      AlertMin
      (dB)      (dB)      (dB)      (dB)      (dB)      (dB)
-----
```

ce9/1	Inactive*	+12.00	+26.00	+25.00	+8.00	+7.00
-------	-----------	--------	--------	--------	-------	-------

---

# show interface transceiver

Use this command to show EDFA module input power, output power, pump bias and gain current values from all ports.

## Command Syntax

```
show interface transceiver
```

## Parameters

None

## Default

None

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 6.3.0.

## Example

```
Cassini-3>show interface transceiver
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No Power,  - Not
Applicable

Intf      DDM      Temp      Voltage      InPwr      OutPwr      PumpBias      Gain
          (Celsius) (volt)      (dBm)      (dBm)      (Amp)      (dB)
-----
ce0       Inactive*  +33.10     +3.28        -8.12       +8.85       +0.11       +16.97
```

# show interface transceiver detail

Use this command to show EDFA module input power, output power, pump bias and gain threshold and current values from all ports.

## Command Syntax

```
show interface transceiver detail
```

## Parameters

None

## Default

None

## Command Mode

Exec mode and Privileged Exec mode

## Applicability

This command was introduced before OcNOS version 6.3.0.

## Example

```
OcNOS>show interface transceiver detail
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No
Power,  - Not Applicable
```

...

Intf	DDM	InPwr (dBm)	AlertMax (dBm)	CritMax (dBm)	CritMin (dBm)	AlertMin (dBm)
ce0	Inactive*	-8.12	+5.00	+4.00	-20.97	-21.94
Intf	DDM	OutPwr (dBm)	AlertMax (dBm)	CritMax (dBm)	CritMin (dBm)	AlertMin (dBm)
ce0	Inactive*	+8.83	+20.00	+18.00	-10.00	-11.94
Intf	DDM	PumpBias (Amp)	AlertMax (Amp)	CritMax (Amp)	CritMin (Amp)	AlertMin (Amp)
ce0	Inactive*	+0.11	+0.59	+0.53	+0.00	+0.00
Intf	DDM	Gain (dB)	AlertMax (dB)	CritMax (dB)	CritMin (dB)	AlertMin (dB)
ce0	Inactive*	+16.97	+26.00	+25.00	+8.00	+7.00

## show interface transceiver threshold violations

Use this command to show EDFA EDFA module input power, output power, pump bias and gain thresholds violations.

### Command Syntax

```
show interface transceiver threshold violations
```

### Parameters

None

### Default

None

### Command Mode

Exec mode and Privileged Exec mode

### Applicability

This command was introduced before OcNOS version 6.3.0.

### Example

```
OcNOS>show interface transceiver threshold violations
Intf      Lane      Timestamp      Type of alarm
----      -
ce9/1     1          03-05-2019 08:53:31 Gain high alarm, value 100.000dB threshold 26.000dB
                                03-05-2019 08:53:31 Pump bias high alarm, value 100.000A threshold 0.579A
                                03-05-2019 08:53:31 Output power high alarm, value 100.000dBm threshold 20.000dBm
                                03-05-2019 08:53:31 Input power high alarm, value 100.000dBm threshold 5.000dBm

OcNOS>show interface ce9/1 transceiver threshold violations
Intf      Lane      Timestamp      Type of alarm
----      -
ce9/1     1          03-05-2019 08:57:09 Gain low alarm, value -100.000dB threshold 7.000dB
                                03-05-2019 08:57:09 Pump Bias low alarm, value -100.000A threshold 0.000A
                                03-05-2019 08:57:09 Output power low alarm, value -100.000dBm threshold -11.938dBm
                                03-05-2019 08:57:09 Input power low alarm, value -100.000dBm threshold -21.938dBm

OcNOS>show interface ce9/1 transceiver threshold violations
Intf      Lane      Timestamp      Type of alarm
----      -
ce9/1     1          03-05-2019 09:03:36 Gain high warning, value 25.500db threshold 25.000db
                                03-05-2019 09:03:36 Pump bias high warning, value 0.550A threshold 0.526A
                                03-05-2019 09:03:36 Output power high warning, value 19.000dbm threshold 18.000dbm
                                03-05-2019 09:03:36 Input power high warning, value 4.500dbm threshold 4.000dbm

OcNOS>show interface ce9/1 transceiver threshold violations
Intf      Lane      Timestamp      Type of alarm
----      -
ce9/1     1          03-05-2019 09:07:05 Gain low warning, value 7.500dB threshold 8.000dB
                                03-05-2019 09:07:05 Pump Bias low alarm, value 0.000A threshold 0.000A
                                03-05-2019 09:07:05 Output power low warning, value -11.000dBm threshold -10.000dBm
                                03-05-2019 09:07:05 Input power low warning, value -21.000dBm threshold -20.969dBm
```





# Index

## A

- aaa accounting default 382
- aaa accounting details 383
- aaa authentication attempts login 382
- aaa authentication login 382
- aaa authentication login console 384
- aaa authentication login default 385
- aaa authentication login default fallback error 388
- aaa authorization config-commands default 389
- aaa group server 389
- aaa local authentication attempts max-fail 390
- abort transaction 515
- Authentication 163
- authentication 1064

## B

- banner 403
- begin modifier 28
- BGP community value
  - command syntax 26
- braces
  - command syntax 25

## C

- Chassis Management Module Commands 463
- clear crypto sa map 1064
- clear ip prefix-list 641
- clear ipv6 neighbors 642
- clear ntp statistics 764
- clear ssh hosts 811
- clear tfo counter 1012
- Client 163
- clock timezone 404
- cml force-unlock config-datastore 517
- cml lock config-datastore 518
- cml logging 519
- cml netconf translation 520
- cml unlock config-datastore 522
- cmlsh multiple-config-session 523
- cmlsh transaction 526
- cmlsh transaction limit 527
- command abbreviations 24
- command completion 24
- command line
  - errors 24
  - help 23
  - keyboard operations 27
- command modes 31
  - configure 31
  - exec 31
  - interface 31
  - privileged exec 31

- router 31
- command negation 25
- command syntax
  - ? 26
  - . 26
  - () 25
  - { } 25
  - | 25
- A.B.C.D/M 26
- AA:NN 26
- BGP community value 26
- braces 25
- conventions 25
- curly brackets 25
- HH:MM:SS 26
- IFNAME 26
- interface name 26
- IPv4 address 26
- IPv6 address 26
- LINE 26
- lowercase 25
- MAC address 26
- monospaced font 25
- numeric range 26
- parentheses 25
- parenteses 25
- period 26
- question mark 26
- square brackets 26
- time 26
- uppercase 25
- variable placeholders 26
- vertical bars 25
- WORD 26
- X::X::X::X 26
- X::X::X/M 26
- XX:XX:XX:XX:XX:XX 26
- commit 528
- common commands 925
  - banner 403
  - clear ip prefix-list 641
  - configure terminal 406
  - copy running-config startup-config 410
  - disable 412, 438
  - enable 414
  - end 416
  - exit 418
  - ip prefix-list 661
  - ip remote-address 664
  - ip unnumbered 665
  - ipv6 prefix-list 669
  - ipv6 unnumbered 671
  - log syslog 907
  - reload 433
  - service advanced-vty 434
  - service password-encryption 435
  - service terminal-length 436
  - show access-list 438
  - show cli 438

- show ip prefix-list 731
- show list 442
- show startup-config 448
- show version 453
- write terminal 461
- Common Configure Mode Commands 925
- Common NSM Layer 2 commands
  - flowcontrol off 653
  - show flowcontrol interface 682
- configuration 267
- configure
  - GMRP 137
- configure mode 31
- configure terminal 406
- Configuring port Breakout 178
- Configuring port Breakout(100G to 4x10G) 178
- configuring sFlow 205
- Control Port Group 267, 1013, 1015
- copy 496
- copy ftp running-config 497
- copy ftp running-config (interactive) 499
- copy ftp startup-config 495
- copy ftp startup-config (interactive) 500
- copy http startup-config 499
- copy http startup-config (interactive) 505
- copy running-config 489
- copy running-config (interactive) 490
- copy running-config start-config 410
- copy scp (startup-config|running-config) 496
- copy scp running-config 496
- copy scp startup-config 496
- copy scp startup-config (interactive) 502
- copy sftp (startup-config|running-config) 497
- copy sftp running-config 497
- copy sftp startup-config 497
- copy sftp startup-config (interactive) 503
- copy startup-config 491
- copy startup-config (interactive) 492
- copy system file 493
- copy system file (interactive) 494
- copy tftp startup-config 498
- copy tftp startup-config (interactive) 504
- crypto ipsec transform-set 1064
- crypto isakmp policy 1066
- crypto map (Configure Mode) 1066
- curly brackets
  - command syntax 25

## D

- ddm monitor 566, 567
- debug cml 532
- debug cmm 464
- debug ddm 569, 572
- debug dns client 620
- debug ntp 766
- debug radius 795
- debug sflow 833
- debug snmp-server 847

- debug ssh server 812
- debug tacacs+ 952
- debug telnet server 972
- debug user-mgmt 1022
- disable 412, 438
- do 413
- domain-name, ip 623

## E

- enable 414
- end 416
- exec command mode 31
- exit 418

## F

- Fail Over Group 267
- feature dhcp 563, 578
- feature ntp 766
- feature sflow 834
- feature ssh 813
- feature tacacs+ 956
- feature telnet 973
- flowcontrol off 653
- fog tfc 1014
- fog type 1015

## G

- GARP Multicast Registration Protocol 137
- GMRP
  - configuring 137

## H

- hardware-profile portmode 655, 932
- hardware-profile portmode bundle 655
- hash 1067

## I

- if-arbiter 656
- IFNAME 26
- interface 657
- Interface Commands 629
- interface mode 31
- ip address 658
- ip address dhcp 579, 659
- ip dhcp client request 580
- ip dhcp relay 592, 593
- ip dhcp relay address 594
- ip dhcp relay information option 596
- ip domain-list 621
- ip domain-lookup 622
- ip domain-name 623
- ip forwarding 660
- ip host 624

- ip name-server 625
- ip prefix-list 661
- ip proxy-arp 663
- ip remote-address 664
- ip unnumbered 665
- ip vrf 666
- ip vrf forwarding 666
- IPv4 address
  - command syntax 26
- ipv6 access-list filter 343
- IPv6 address
  - command syntax 26
- ipv6 address 667
- ipv6 dhcp relay 600, 601, 605
- ipv6 dhcp relay address 602
- ipv6 dhcp relay subscriber-id 604
- ipv6 forwarding 668
- ipv6 prefix-list 669
- ipv6 unnumbered 671

## L

- lifetime 1067
- LINE 26
- Linkdown Policy 141
- link-type 1016
- load-balance 939
- load-balance rtag7 939
- locator led 467
- log syslog 907
- Logging Console Configuration 225
- logging level 909
- logging logfile 911
- logging source-interface 916
- logging timestamp 916
- logout 426

## M

- MAC address
  - command syntax 26
- Maxpoll and Minpoll Configuration 165
- mode 1067
- Monitor Port Group 267, 1013, 1014, 1015
- Monitor Port Groups 1014
- multicast 681
- Multicast Commands
  - multicast 681
  - show ip rpf 708

## N

- NSM Commands
  - clear ipv6 neighbors 642
  - if-arbiter 656
  - interface 657
  - ip address 658
  - ip address dhcp 659
  - ip forwarding 660

- ip proxy-arp 663
- ipv6 address 667
- ipv6 forwarding 668
- multicast 681
- show debugging nsm 441
- show ip forwarding 710
- show ip interface brief 711
- show ipv6 forwarding 726
- show ipv6 interface brief 727
- show ipv6 route 729
- show nsm client 444
- ntp access-group 768
- ntp authenticate 768
- NTP Authentication 165
- ntp authentication-key 769
- NTP Configuration 164
- ntp enable 771
- ntp logging 772
- ntp master 775
- ntp peer 775
- ntp server 778
- ntp trusted-key 782

## P

- parentheses
  - command syntax 25
- parentheses
  - command syntax 25
- Peer 163
- peer 1068
- peer public-key 1068
- period
  - command syntax 26
- ping 428
- Port 167
- Port Breakout Configuration 167
- port bundle enable 681
- prefix-list 661
- privilege 432
- privileged exec mode 31

## Q

- question mark
  - command syntax 26

## R

- RADIUS Server Accounting 201
- RADIUS Server Authentication 191
- radius-server deadtime 796
- radius-server directed-request 796
- radius-server host 796
- radius-server host acct-port 798
- radius-server host auth-port 799
- radius-server host key 802
- radius-server key 802
- radius-server retransmit 803

radius-server timeout 803  
reload 433  
reset log file 1030  
router mode 31

## S

Server 163  
server 393  
service advanced-vty 434  
service password-encryption 435  
service terminal-length 436  
set ipv6 peer 1068  
set peer 1068  
set security-association lifetime 1069  
set session-key 1069  
set transform-set 1070  
sFlow 834  
sflow collector 836  
show aaa accounting 394  
show aaa authentication 394  
show aaa authentication login 395  
show access-list 438  
show access-lists 371  
show cli 438  
show cmlsh multiple-config-session status 536  
show commands 28  
    exclude modifier 29  
    include modifier 29  
    redirect modifier 30  
show crypto ipsec transform-set 1072  
show debug radius 804  
show debug ssh server 814  
show debug tacacs+ 960  
show debug telnet server 974  
show debugging nsm 441  
show flowcontrol interface 682  
show hardware-information 468  
show hosts 626  
show ip dhcp relay 606  
show ip dhcp relay address interface 608  
show ip forwarding 710  
show ip interface brief 711  
show ip prefix-list 731  
show ip vrf 725  
show ipv6 dhcp relay 611  
show ipv6 dhcp relay address 612  
show ipv6 dhcp vendor-opts 587  
show ipv6 forwarding 726  
show ipv6 interface brief 727  
show ipv6 route 729  
show list 442  
show logging 917  
show logging last 919  
show logging logfile 920  
show logging logfile last-index 921  
show logging logfile start-seqn end-seqn 922  
show logging logfile start-time end-time 923  
show max-transaction limit 538  
show nsm client 444  
show ntp authentication-keys 783  
show ntp authentication-status 784  
show ntp client 785  
show ntp logging-status 785  
show ntp peers 788  
show ntp peer-status 786  
show ntp statistics 789  
show ntp status 791  
show ntp trusted-keys 791  
show priority-flow-control details 572  
show process 446  
show radius-server 805  
show role name 1026  
show running-config 447  
show running-config aaa 399  
show running-config dhcp 613  
show running-config dns 628  
show running-config interface 734  
show running-config interface ip 736  
show running-config interface ipv6 737  
show running-config ipv6 access-list 739  
show running-config ntp 792  
show running-config prefix-list 740  
show running-config radius 807  
show running-config snmp 848  
show running-config ssh server 815  
show running-config syslog 924  
show running-config tacacs+ 963  
show running-config telnet server 975  
show sflow 840  
show sflow interface 842  
show snmp 849  
show snmp community 850  
show snmp engine-id 852  
show snmp group 853  
show snmp host 854  
show snmp user 855  
show snmp view 856  
show ssh server 818  
show startup-config 448  
show system restore failures 542  
show system-information 481  
show tacacs-server 964  
show telnet server 976  
show tfo 1017  
show transaction current 543  
show transaction last-aborted 544  
show transceivers details 574  
show user-account 1026  
show username 819  
show users 452  
show version 453  
show vlog all 1030  
show vlog clients 1031  
show vlog terminals 1032  
show vlog virtual-routers 1033  
Simple Network Management Protocol 209  
snmp-server community 858

---

- snmp-server contact 860
- snmp-server enable snmp 863
- snmp-server enable traps 864
- snmp-server group 869
- snmp-server host 869
- snmp-server location 871
- snmp-server tcp-session 873
- snmp-server user 874
- snmp-server view 876
- square brackets
  - command syntax 26
- SSH Client session 216
- ssh key 825
- ssh login-attempts 826
- ssh server port 827

## T

- tacacs-server deadtime 966
- tacacs-server directed-request 966
- tacacs-server host 966
- tacacs-server key 968
- Telnet 971
- telnet server port 979
- time
  - command syntax 26
- traceroute 459
- trigger failover 1019

- Trigger Failover Commands 1011

## U

- username 1027
- username keypair 830
- username sshkey 829

## V

- vertical bars
  - command syntax 25
- VLOG commands 1029
  - reset log file 1030
  - show vlog all 1030
  - show vlog clients 1031
  - show vlog terminals 1032
  - show vlog virtual-routers 1033

### VPN Commands

- ip vrf 666
- ip vrf forwarding 666
- show ip vrf 725

## W

- WORD 26
- write terminal 461

