

**Interface Masters**

◀ TECHNOLOGIES ▶

*Innovative Network Solutions*

**ISS**

CLI User Manual\_Vol7

INTERFACE MASTERS: ISSCLlum\_Vol7/20101001

---

Revision Number: 28.0

**Copyright © 2010 Interface Masters Inc. All Rights Reserved.** No part of this document may be reproduced, stored in a retrieval system or transmitted, in any form, or by any means, electronic or otherwise, including photocopying, reprinting, or recording, for any purpose, without the express written permission of Interface Masters.

Printed in \_\_\_\_\_

**TRADEMARKS** INTERFACE MASTERS and THE INTERFACE MASTERS LOGO are trademarks of Interface Masters Inc. in the U.S. and other countries. The use of any of these trademarks without Interface Masters prior written consent is strictly prohibited. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Interface Masters Inc. disclaims any proprietary interest in the trademarks and trade names other than its own.

**DISCLAIMER** The information in this book is provided “as is”, with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose or any warranty otherwise arising out of any proposal, specification or sample. This document is provided for informational purposes only and should not be construed as a commitment on the part of Interface Masters. Information in this document is subject to change without notice.

**REQUESTS** For information or obtaining permission for use of material of this work, please submit a written request to: Corporate Marketing and Legal, Interface Masters on [www.InterfaceMasters.com](http://www.InterfaceMasters.com).

**DOCUMENT No.:** INTERFACE MASTERS: ISSCLlum\_Vol7/20101001

# Contents

---

<b>CHAPTER 64:</b>	<b>QOS (QUALITY OF SERVICE)</b>	<b>7</b>
	64.1 BCM SPECIFIC COMMANDS	8
	64.1.1 shutdown qos	10
	64.1.2 qos	11
	64.1.3 priority-map	12
	64.1.4 class-map	13
	64.1.5 meter	14
	64.1.6 policy-map	15
	64.1.7 queue-type	16
	64.1.8 shape-template	17
	64.1.9 scheduler	18
	64.1.10 queue	20
	64.1.11 queue-map	22
	64.1.12 sched-hierarchy	23
	64.1.13 qos interface	24
	64.1.14 map	25
	64.1.15 match access-group	27
	64.1.16 set class	28
	64.1.17 meter-type	29
	64.1.18 set policy	31
	64.1.19 set meter	32
	64.1.20 set algo-type	35
	64.1.21 random-detect dp	36
	64.1.22 show qos global info	37
	64.1.23 show priority-map	38
	64.1.24 show class-map	40
	64.1.25 show class-to-priority-map	41
	64.1.26 show meter	42
	64.1.27 show policy-map	43
	64.1.28 show queue-template	44
	64.1.29 show shape-template	45
	64.1.30 show scheduler	46
	64.1.31 show queue	47
	64.1.32 show queue-map	48
	64.1.33 show sched-hierarchy	49
	64.1.34 show qos def-user-priority	50
	64.1.35 show qos meter-stats	52
	64.1.36 show qos queue-stats	53
	64.2 XCAT SPECIFIC COMMANDS	54
	64.2.1 shutdown qos	56
	64.2.2 qos	57
	64.2.3 priority-map	58
	64.2.4 class-map	59
	64.2.5 meter	60
	64.2.6 policy-map	61
	64.2.7 queue-type	62
	64.2.8 shape-template	63
	64.2.9 scheduler	64
	64.2.10 queue	66
	64.2.11 queue-map	68

64.2.12 sched-hierarchy .....	69
64.2.13 qos interface .....	70
64.2.14 map .....	71
64.2.15 match access-group .....	73
64.2.16 set class .....	74
64.2.17 meter-type .....	75
64.2.18 set policy .....	77
64.2.19 set meter .....	78
64.2.20 set algo-type .....	81
64.2.21 random-detect dp .....	82
64.2.22 show qos global info .....	83
64.2.23 show priority-map .....	84
64.2.24 show class-map .....	86
64.2.25 show class-to-priority-map .....	87
64.2.26 show meter .....	88
64.2.27 show policy-map .....	89
64.2.28 show queue-template .....	90
64.2.29 show shape-template .....	91
64.2.30 show scheduler .....	92
64.2.31 show queue .....	93
64.2.32 show queue-map .....	94
64.2.33 show sched-hierarchy .....	95
64.2.34 show qos def-user-priority .....	96
64.2.35 show qos meter-stats .....	98
64.2.36 show qos queue-stats .....	99
64.3 DCB PRODUCT OVERVIEW .....	100
64.3.1 DCBX .....	100
64.3.1.1 shutdown ets .....	102
64.3.1.2 ets .....	103
64.3.1.3 ets trap .....	104
64.3.1.4 set priority grouping .....	106
64.3.1.5 priority-grouping mode .....	107
64.3.1.6 set priority-group willing .....	108
64.3.1.7 map priority .....	109
64.3.1.8 set priority-group bandwidth .....	110
64.3.1.9 set priority-group recommendation bandwidth .....	112
64.3.1.10 dcbx tlv-select etstlv .....	114
64.3.1.11 show interfaces - priority-grouping .....	115
64.3.1.12 show interfaces priority-grouping counters .....	118
64.3.1.13 show ets global info .....	120
64.3.1.14 clear priority-grouping counters .....	121
64.3.1.15 shutdown pfc .....	123
64.3.1.16 pfc .....	124
64.3.1.17 set pfc threshold limit .....	126
64.3.1.18 pfc trap .....	128
64.3.1.19 set priority-flow-control .....	130
64.3.1.20 priority-flow-control mode .....	131
64.3.1.21 set priority-flow-control willing .....	133
64.3.1.22 set priority flow-control .....	134
64.3.1.23 dcbx tlv-select pfctlv .....	135
64.3.1.24 show interfaces - priority-flow-control .....	136
64.3.1.25 show interfaces priority-flow-control counters .....	139
64.3.1.26 show priority-flow-control config .....	141
64.3.1.27 show pfc global info .....	142
64.3.1.28 clear priority-flow-control counters .....	143
64.3.1.29 set dcbx .....	145

	64.3.1.30 show dcbx ports -----	147
	64.3.1.31 debug dcbx -----	148
	64.3.2 CN -----	150
	64.3.2.1 set cn -----	151
	64.3.2.2 set cn cnm-transmit-priority -----	152
	64.3.2.3 cn cnpv -----	153
	64.3.2.4 cn cnpv defense -----	154
	64.3.2.5 cn cnpv - alternate-priority -----	156
	64.3.2.6 cn cnpv - defense-mode -----	157
	64.3.2.7 cn cnpv - port-default-defense -----	159
	64.3.2.8 cn cnpv - lldp-instance-choice -----	161
	64.3.2.9 cn cnpv - lldp-instance-selector -----	163
	64.3.2.10 shutdown cn -----	164
	64.3.2.11 cn trap -----	165
	64.3.2.12 cn cnpv - defense -----	166
	64.3.2.13 cn cnpv - defense-mode -----	167
	64.3.2.14 cn cnpv - lldp-instance-choice -----	169
	64.3.2.15 cn cnpv - lldp-instance-selector -----	170
	64.3.2.16 cn cnpv - alternate-priority -----	171
	64.3.2.17 cn cp-properties -----	172
	64.3.2.18 debug cn -----	174
	64.3.2.19 clear cn counters -----	176
	64.3.2.20 show cn global information -----	178
	64.3.2.21 show cn interface counters -----	179
	64.3.2.22 show cn cnpv -----	181
	64.3.2.23 show cn cp-properties -----	183
<b>CHAPTER 65:</b>	<b>ACL -----</b>	<b>185</b>
	65.1 LINUX ENVIRONMENT COMMANDS -----	186
	65.1.1 ip access-list -----	188
	65.1.2 mac access-list extended -----	190
	65.1.3 user-defined access-list -----	191
	65.1.4 traffic-separation control -----	192
	65.1.5 userdefined-list -----	193
	65.1.6 permit usr-defined-packet-type -----	195
	65.1.7 deny usr-defined-packet-type -----	198
	65.1.8 permit - standard mode -----	200
	65.1.9 deny - standard mode -----	202
	65.1.10 copy-to-cpu - standard mode -----	203
	65.1.11 permit- ip/ospf/pim/protocol type -----	205
	65.1.12 permit ipv6 -----	211
	65.1.13 deny - ip/ospf/pim/protocol type -----	213
	65.1.14 copy-to-cpu - ip / ospf / pim / protocol-type -----	218
	65.1.15 deny ipv6 -----	222
	65.1.16 copy-to-cpu ipv6 -----	223
	65.1.17 permit tcp -----	225
	65.1.18 deny tcp -----	231
	65.1.19 copy-to-cpu tcp -----	237
	65.1.20 permit udp -----	242
	65.1.21 deny udp -----	248
	65.1.22 copy-to-cpu udp -----	253
	65.1.23 permit icmp -----	258
	65.1.24 deny icmp -----	262
	65.1.25 copy-to-cpu icmp -----	266
	65.1.26 ip access-group -----	270
	65.1.27 mac access-group -----	271

65.1.28 user-defined access-group.....	272
65.1.29 permit - MAC .....	273
65.1.30 deny - MAC.....	278
65.1.31 copy-to-cpu - MAC.....	282
65.1.32 show access-lists.....	287
65.2 BCM SPECIFIC COMMANDS.....	291
65.2.1 ip access-list.....	292
65.2.2 mac access-list extended.....	294
65.2.3 permit - standard mode.....	295
65.2.4 deny - standard mode.....	296
65.2.5 permit- ip/ospf/pim/protocol type.....	297
65.2.6 permit ipv6.....	300
65.2.7 deny ipv6.....	301
65.2.8 deny - ip/ospf/pim/protocol type.....	302
65.2.9 permit tcp.....	305
65.2.10 deny tcp.....	308
65.2.11 permit udp.....	311
65.2.12 deny udp.....	314
65.2.13 permit icmp.....	317
65.2.14 deny icmp.....	321
65.2.15 ip access-group.....	325
65.2.16 mac access-group.....	326
65.2.17 permit.....	327
65.2.18 deny.....	330
65.2.19 show access-lists.....	333
65.3 CXE SPECIFIC COMMANDS.....	336
65.3.1 ip access-list.....	337
65.3.2 mac access-list extended.....	339
65.3.3 permit - standard mode.....	340
65.3.4 deny - standard mode.....	341
65.3.5 permit- ip/ospf/pim/protocol type.....	342
65.3.6 deny - ip/ospf/pim/protocol type.....	344
65.3.7 permit tcp.....	346
65.3.8 deny tcp.....	348
65.3.9 permit udp.....	350
65.3.10 deny udp.....	352
65.3.11 permit icmp.....	354
65.3.12 deny icmp.....	357
65.3.13 mac access-group.....	360
65.3.14 permit.....	361
65.3.15 deny.....	364
65.3.16 show access-lists.....	367
65.4 MARVELL 6095 SPECIFIC COMMANDS.....	370
65.4.1 ip access-list.....	371
65.4.2 mac access-list extended.....	373
65.4.3 permit - standard mode.....	374
65.4.4 deny - standard mode.....	375
65.4.5 permit host.....	376
65.4.6 deny host.....	377
65.4.7 permit- ip/ospf/pim/protocol type.....	378
65.4.8 deny - ip/ospf/pim/protocol type.....	380
65.4.9 permit tcp.....	382
65.4.10 deny tcp.....	385
65.4.11 permit udp.....	388
65.4.12 deny udp.....	391
65.4.13 permit icmp.....	394

	65.4.14 deny icmp .....	397
	65.4.15 ip access-group .....	400
	65.4.16 mac access-group.....	401
	65.4.17 permit .....	402
	65.4.18 deny .....	405
	65.4.19 show access-lists .....	408
	65.5 XCAT SPECIFIC COMMANDS.....	410
	65.5.1 ip access-list.....	411
	65.5.2 mac access-list extended.....	413
	65.5.3 user-defined access-list .....	414
	65.5.4 userdefined-list .....	415
	65.5.5 permit usr-defined-packet-type.....	417
	65.5.6 deny usr-defined-packet-type.....	420
	65.5.7 permit - standard mode.....	422
	65.5.8 deny - standard mode .....	424
	65.5.9 permit- ip/ospf/pim/protocol type .....	425
	65.5.10 permit ipv6.....	428
	65.5.11 deny ipv6 .....	430
	65.5.12 deny - ip/ospf/pim/protocol type.....	431
	65.5.13 permit tcp.....	434
	65.5.14 deny tcp.....	438
	65.5.15 permit udp .....	441
	65.5.16 deny udp.....	445
	65.5.17 permit icmp.....	448
	65.5.18 deny icmp.....	452
	65.5.19 ip access-group .....	455
	65.5.20 mac access-group.....	456
	65.5.21 user-defined access-group.....	457
	65.5.22 Permit.....	458
	65.5.23 deny .....	462
	65.5.24 show access-lists .....	465
<b>CHAPTER 66:</b>	<b>DIFFSERV</b> .....	<b>469</b>
	66.1 BCM SPECIFIC COMMANDS.....	470
	66.1.1 set qos.....	471
	66.1.2 class-map .....	472
	66.1.3 policy-map.....	473
	66.1.4 match .....	474
	66.1.5 class .....	475
	66.1.6 set cos .....	476
	66.1.7 police.....	477
	66.1.8 shutdown qos .....	478
	66.1.9 cosq scheduling algorithm.....	479
	66.1.10 traffic class.....	480
	66.1.11 show policy-map .....	481
	66.1.12 show class-map .....	483
	66.1.13 show cosq algorithm .....	484
	66.1.14 show cosq weights-bw .....	485
	66.2 CXE SPECIFIC COMMANDS .....	486
	66.2.1 set qos.....	488
	66.2.2 class-map .....	489
	66.2.3 policy-map.....	490
	66.2.4 qos traffic-class.....	491
	66.2.5 qos random-detect.....	492
	66.2.6 qos map dscp-queue .....	493
	66.2.7 qos queue-precedence switched.....	494

66.2.8	qos queue-precedence routed.....	495
66.2.9	match .....	496
66.2.10	class .....	497
66.2.11	set cos .....	498
66.2.12	set qos traffic-class .....	499
66.2.13	bandwidth .....	500
66.2.14	min-reserved-bandwidth.....	501
66.2.15	queue-threshold.....	502
66.2.16	set random-detect.....	503
66.2.17	fair-queue .....	504
66.2.18	weight .....	505
66.2.19	qos bandwidth .....	506
66.2.20	qos queue threshold .....	507
66.2.21	qos set random-detect .....	508
66.2.22	shutdown qos .....	509
66.2.23	show policy-map.....	510
66.2.24	show class-map.....	511
66.2.25	show qos maps dscp-queue.....	512
66.2.26	show qos maps trafficclass-fairqueue map.....	513
66.2.27	show qos queue precedence .....	514
66.2.28	show qos traffic-class.....	515
66.2.29	show qos random-detect.....	518
66.2.30	show qos interface.....	519
66.2.31	show qos statistics.....	520
66.3	MARVELL 6095 SPECIFIC COMMANDS .....	521
66.3.1	shutdown qos .....	522
66.3.2	qos .....	523
66.3.3	priority-map.....	524
66.3.4	queue-map .....	525
66.3.5	qos scheduling policy .....	526
66.3.6	qos match.....	527
66.3.7	qos override.....	528
66.3.8	qos tagifboth match.....	529
66.3.9	map .....	530
66.3.10	map vlan.....	532
66.3.11	show qos global info .....	533
66.3.12	show priority-map .....	534
66.3.13	show queue-map .....	536
66.3.14	show qos port config.....	539
66.3.15	show qos port override config.....	541
66.3.16	show qos scheduling policy.....	543
66.4	XCAT SPECIFIC COMMANDS.....	544
66.4.1	set qos.....	545
66.4.2	class-map.....	546
66.4.3	policy-map.....	547
66.4.4	match .....	548
66.4.5	class .....	549
66.4.6	set cos.....	550
66.4.7	shutdown qos .....	551
66.4.8	cosq scheduling algorithm.....	552
66.4.9	traffic class.....	553
66.4.10	show policy-map.....	554
66.4.11	show class-map.....	556
66.4.12	show cosq algorithm .....	557
66.4.13	show cosq weights-bw .....	558

# Chapter

# 64

## QoS (Quality of Service)

---

**QoS** (Quality of Service) defines the ability to provide different priorities to different applications, users or data flows or the ability to guarantee a certain level of performance to a data flow. **QoS** refers to resource reservation control mechanisms rather than the achieved service quality and specifies a guaranteed throughput level.

**Interface Masters QoS** provides a complete IP Quality of Service solution across VPNs and helps in implementing service provisioning policies for application or customers, who desire to have an enhanced performance for their traffic on the Internet.

## 64.1 BCM Specific Commands

This section describes the CLI commands executable only in BCM target for configuring QoS feature supported by ISS.

The list of CLI commands for the configuration of QoS is as follows:

- shutdown qos
- qos
- priority-map
- class-map
- meter
- policy-map
- queue-type
- shape-template
- scheduler
- queue
- queue-map
- sched-hierarchy
- qos interface
- map
- match access-group
- set class
- meter-type
- set policy
- set meter
- set
- random-detect dp
- show qos global info
- show priority-map
- show class-map
- show class-to-priority-map
- show meter
- show policy-map
- show queue-template
- show shape-template
- show scheduler

- show queue
- show queue-map
- show sched-hierarchy
- show qos def-user-priority
- show qos meter-stats
- show qos queue-stats

## 64.1.1 shutdown qos

This command shuts down the QoS subsystem. The no form of the command starts the QoS subsystem.

**shutdown qos**

**no shutdown qos**

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** QoS subsystem is started and enabled by default.

**Example** `iss(config)# shutdown qos`



- Resources required by QoS subsystem are allocated and QoS subsystem starts running, when started.
- All the MemPools used by the QoS subsystem will be released, when shutdown.

**Related Commands** `show qos global info` – Displays QoS related global configurations.

## 64.1.2 qos

This command enables or disables the QoS subsystem.

**qos {enable | disable}**

**Syntax Description**      **enable**                      - Enables QoS subsystem

**disable**                      - Disables Qos subsystem

**Mode**                      Global Configuration Mode

**Package**                  Workgroup, Enterprise and Metro

**Defaults**                Enabled

**Example**                `iss(config)# qos enable`



- QoS module programs the hardware and starts protocol operation, when set as **enable**.
- QoS module stops protocol operation by deleting the hardware configuration, when set as **disable**.

**Related Commands**      `show qos global info` – Displays QoS related global configurations.

## 64.1.3 priority-map

This command adds a Priority Map entry. The no form of the command deletes a Priority Map entry.

```
priority-map <priority-map-Id(1-65535)>
```

```
no priority-map <priority-map-Id(1-65535)>
```

**Syntax Description**     **Priority-map-Id**     - Priority map index for the incoming packet received over ingress Port/VLAN with specified incoming priority. This value ranges between 1 and 65535.

**Mode**                     Global Configuration Mode

**Package**                 Workgroup, Enterprise and Metro

**Example**                 iss(config)# priority-map 1



QoS subsystem should have been started.

**Related Commands**     **show priority-map** – Displays the Priority Map entry.

## 64.1.4 class-map

This command adds a Class Map entry. The no form of the command deletes a Class Map entry.

```
class-map <class-map-id(1-65535)>
```

```
no class-map <class-map-id(1-65535)>
```

<b>Syntax Description</b>	<b>class-map-id</b>	- Index that enumerates the MultiField Classifier table entries. This value ranges between 1 and 65535.
---------------------------	---------------------	---

<b>Mode</b>	Global Configuration Mode
-------------	---------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Example</b>	<pre>iss(config)# class-map 1</pre>
----------------	-------------------------------------



QoS subsystem should have been started.

<b>Related Commands</b>	<b>show class-map</b> – Displays the Class Map entry.
-------------------------	---

## 64.1.5 meter

This command creates a Meter. The no form of the command deletes a Meter.

```
meter <meter-id(1-65535)>
```

```
no meter <meter-id(1-65535)>
```

<b>Syntax Description</b>	<b>meter-id</b>	- Index that enumerates the Meter entries. This value ranges between 1 and 65535.
---------------------------	-----------------	---

<b>Mode</b>	Global Configuration Mode
-------------	---------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Example</b>	<code>iss(config)# meter 1</code>
----------------	-----------------------------------



QoS subsystem should have been started.

<b>Related Commands</b>	<code>show meter</code> – Displays the Meter entry.
-------------------------	---

## 64.1.6 policy-map

This command creates a policy map. The no form of the command deletes a policy map.

```
policy-map <policy-map-id (1-65535)>
```

```
no policy-map <policy-map-id (1-65535)>
```

<b>Syntax</b>	<b>policy-map-id</b>	- Index that enumerates the policy-map table entries.
<b>Description</b>		This value ranges between 1 and 65535.

<b>Mode</b>	Global Configuration Mode
-------------	---------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Example</b>	iss(config)# policy-map 1
----------------	---------------------------



QoS subsystem should have been started.

<b>Related Commands</b>	<b>show policy-map</b> – Displays the Policy Map entry.
-------------------------	---

## 64.1.7 queue-type

This command creates a Queue Template Type. The no form of the command deletes a Queue Template Type.

```
queue-type <Q-Template-Id(1-65535)>
```

```
no queue-type <Q-Template-Id(1-65535)>
```

**Syntax Description**    **Q-Template-Id**       - Queue Template Table index. This value ranges between 1 and 65535.

**Mode**                Global Configuration Mode

**Package**            Workgroup, Enterprise and Metro

**Example**            `iss(config)# queue-type 1`

**Related Commands**    `show queue-template` – Displays the Q Template and Random Detect configurations.

## 64.1.8 shape-template

This command creates a Shape Template. The no form of the command deletes a Shape Template.

```
shape-template <integer(1-65535)> [cir <integer(1-65535)>] [cbs <integer(0-65535)>] [eir <integer(0-65535)>] [ebs <integer(0-65535)>]
```

```
no shape-template <Shape-Template-Id(1-65535)>
```

<b>Syntax Description</b>	<b>Shape-Template-Id</b> - Shape Template Table index.
	<b>cir</b> - Committed information rate for packets through the queue.
	<b>cbs</b> - Committed burst size for packets through the queue.
	<b>eir</b> - Excess information rate for packets through the hierarchy.
	<b>ebs</b> - Excess burst size for packets through the hierarchy.
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise and Metro
<b>Example</b>	iss(config)# shape-template 1 cir 20 cbs 40 eir 50 ebs 40
<b>Related Commands</b>	<b>show shape-template</b> – Displays the Shape Template configurations.

## 64.1.9 scheduler

This command creates a Scheduler and configures the Scheduler parameters. The no form of the command deletes a scheduler.

```
scheduler <integer(1-65535)> interface <iftype> <ifnum> [sched-algo {strict-priority | rr | wrr | wfq | strict-rr | strict-wrr | strict-wfq | deficit-rr}] [shaper <integer(0-65535)>] [hierarchy-level <integer(0-10)>]
```

```
no scheduler <Scheduler-Id(1-65535)> interface <iftype> <ifnum>
```

<b>Syntax Description</b>	<b>Scheduler-Id</b>	- Scheduler identifier that uniquely identifies the scheduler in the system/egress interface.
	<b>iftype</b>	- Interface type.
	<b>ifnum</b>	- Interface number.
	<b>sched-algo</b>	- Packet scheduling algorithm for the port. The algorithms are: <ul style="list-style-type: none"> <li>• <b>strict-priority</b> – strictPriority.</li> <li>• <b>rr</b> – roundRobin.</li> <li>• <b>wrr</b> – weightedRoundRobin.</li> <li>• <b>wfq</b> – weightedFairQueing.</li> <li>• <b>strict-rr</b> – strictRoundRobin.</li> <li>• <b>strict-wrr</b> – strictWeightedRoundRobin.</li> <li>• <b>strict-wfq</b> – strictWeightedFairQueing.</li> <li>• <b>deficit-rr</b> – deficitRoundRobin.</li> </ul>
	<b>shaper</b>	- Shaper identifier that specifies the bandwidth requirements for the scheduler.
	<b>hierarchy-level</b>	- Depth of the queue/scheduler hierarchy.
<b>Mode</b>	Global Configuration Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	

---

**Defaults**      sched-algo                      -    strict-priority

                  hierarchy-level                -    0

**Example**      iss(config)# scheduler 1 interface giga 0/1 sched-algo rr  
                  shaper 1 hierarchy-level 1



Shaper identifier is not mandatory for the creation of the conceptual row.

**Related  
Commands**

- **show scheduler** – Displays the configured Scheduler.
- **sched-hierarchy** – Creates a Scheduler Hierarchy.
- **show sched-hierarchy** – Displays the configured hierarchy scheduler.

## 64.1.10 queue

This command creates a Queue and configures the Queue parameters. The no form of the command deletes a Queue.

```
queue <integer(1-65535)> interface <iftype> <ifnum> [qtype <integer(1-65535)>]
[scheduler <integer(1-65535)>] [weight <integer(0-1000)>] [priority
<integer(0-15)>] [shaper <integer(0-65535)>]
```

```
no queue <integer(1-65535)> interface <iftype> <ifnum>
```

<b>Syntax Description</b>	<b>queue</b>	- Queue identifier that uniquely identifies the queue in the system/port.
	<b>iftype</b>	- Interface type.
	<b>ifnum</b>	- Interface number.
	<b>qtype</b>	- Queue Type identifier.
	<b>scheduler</b>	- Scheduler identifier that manages the specified queue.
	<b>weight</b>	- User assigned weight to the CoS queue.
	<b>priority</b>	User assigned priority for the CoS queue.
	<b>shaper</b>	Shaper identifier that specifies the bandwidth requirements for the queue.

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** weight - 0

priority - 0

**Example**      `iss(config)# queue 1 interface giga 0/1 qtype 2 scheduler 1`  
`weight 20 priority 10 shaper 1.`



- Scheduler identifier is unique relative to an egress interface.
- User assigned weights are used only when scheduling algorithm is a weighted scheduling algorithm.
- User assigned priority is used only when the scheduler uses a priority based scheduling algorithm.
- Shaper identifier is not mandatory for the creation of the row.

**Related  
Commands**

- `queue-type` – Creates a Queue Template Type.
- `scheduler` – Creates a Scheduler and configures the Scheduler parameters.
- `shape-template` – Creates a Shape Template.
- `show queue` – Displays the configured Queues.

## 64.1.11 queue-map

This command creates a Map for a Queue with Class or regenerated priority. The no form of the command deletes a Queue map entry.

```
queue-map { CLASS <integer(1-65535)> | regn-priority { vlanPri | ipTos | ipDscp | mplsExp | vlanDEI } <integer(0-63)> } [interface <iftype> <ifnum>] queue-id <integer(1-65535)>
```

```
no queue-map { CLASS <integer(1-65535)> | regn-priority { vlanPri | ipTos | ipDscp | mplsExp | vlanDEI } <integer(0-63)> } [interface <iftype> <ifnum>]
```

<b>Syntax Description</b>	<b>CLASS</b>	- Input CLASS that needs to be mapped to an outbound queue.
	<b>regn-priority</b>	- Regenerated-priority type and regenerated-priority that needs to be mapped to an outbound queue. The types are <ul style="list-style-type: none"> <li>• vlanPri – VLAN Priority.</li> <li>• ipTos – IP Type of Service.</li> <li>• ipDscp – IP Differentiated Services Code Point.</li> <li>• mplsExp – MPLS Experimental</li> <li>• vlanDEI – VLAN Drop Eligibility Indicator.</li> </ul>
	<b>iftype</b>	- Interface type.
	<b>ifnum</b>	- Interface number.
	<b>queue-id</b>	- Queue identifier that uniquely identifies a queue relative to an interface.

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config)# queue-map CLASS 1 interface giga 0/1 queue-id 1`



- CLASS should be zero while configuring RegenPriority specific Q.
- Regenerated-priority should be zero while configuring CLASS specific Queue.

**Related Commands** `show queue-map` – Displays the configured Queue map.

## 64.1.12 sched-hierarchy

This command creates a Scheduler Hierarchy. The no form of the command deletes a Scheduler Hierarchy.

```

sched-hierarchy interface <iftype> <ifnum> hierarchy-level <integer(1-10)>
sched-id <integer(1-65535)> {next-level-queue <integer(0-65535)> | next-level-
scheduler <integer(0-65535)>} [priority <integer(0-15)>] [weight <integer(0-
1000)>]
  
```

```

no sched-hierarchy interface <iftype> <ifnum> hierarchy-level <integer(1-10)>
sched-id <integer(1-65535)>
  
```

<b>Syntax Description</b>	<b>iftype</b>	- Interface type.
	<b>ifnum</b>	- Interface number.
	<b>hierarchy-level</b>	- Depth of the queue/scheduler hierarchy.
	<b>sched-id</b>	- Scheduler identifier. <ul style="list-style-type: none"> <li>• next-level-queue – Next-level queue to which the scheduler output needs to be sent.</li> <li>• next-level-scheduler – Next-level scheduler to which the scheduler output needs to be sent.</li> </ul>
	<b>priority</b>	- Scheduler priority.
	<b>weight</b>	- Scheduler weight.
<b>Mode</b>	Global Configuration Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Defaults</b>	<b>priority</b>	- 0
<b>Example</b>	<pre> iss(config)# sched-hierarchy interface giga 0/1 hierarchy-level 3 sched-id 1 next-level-queue 2 priority 5 weight 50           </pre>	
	<ul style="list-style-type: none"> <li>• The priority is specified when the scheduler is connecting to any of the priorities ( EF, AF, BE) of the next level strict-priority scheduler.</li> <li>• The weight is specified if the scheduler is connecting to a WeightedFairQueuing of another scheduler.</li> </ul>	
<b>Related Commands</b>	<b>show sched-hierarchy</b> – Displays the configured hierarchy scheduler.	

## 64.1.13 qos interface

This command sets the default ingress user priority for the port.

```
qos interface <iftype> <ifnum> def-user-priority <integer (0-7)>
```

<b>Syntax Description</b>	<b>iftype</b>	- Interface type
	<b>ifnum</b>	- Interface number
	<b>def-user-priority</b>	- Default ingress user priority for the port
<b>Mode</b>	Global Configuration Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Example</b>	iss(config)# qos interface giga 0/1 def-user-priority 3	
	The default ingress user priority will be used to set priority for untagged packets.	
<b>Related Commands</b>	<b>show qos def-user-priority</b> – Displays the configured default ingress user priority for a port.	

## 64.1.14 map

This command adds a Priority Map Entry for mapping an incoming priority to a regenerated priority. The no form of the command sets default value to the Interface, VLAN, regenerated inner priority.

```
map [interface <iftype> <ifnum>] [vlan <integer(1-4094)>] in-priority-type {
vlanPri | ipTos | ipDscp | mplsExp | vlanDEI } [in-priority <integer(0-63)>]
regen-priority <integer(0-63)> [regen-inner-priority <integer(0-7)>]
```

```
no map { interface | vlan | regen-inner-priority }
```

<b>Syntax Description</b>	<b>iftype</b>	- Interface type
	<b>ifnum</b>	- Interface number
	<b>vlan</b>	- VLAN identifier. This value ranges between 1 and 4094.
	<b>in-priority-type</b>	- Type of the incoming priority. The types are: <ul style="list-style-type: none"> <li>• vlanPri – VLAN Priority.</li> <li>• ipTos – IP Type of Service.</li> <li>• ipDscp – IP Differentiated Services Code Point.</li> <li>• mplsExp – MPLS Experimental</li> <li>• vlanDEI – VLAN Drop Eligibility Indicator.</li> </ul>
	<b>in-priority</b>	- Incoming priority value determined for the received frame. This value ranges between 0 and 63.
	<b>regen-priority</b>	- Regenerated priority value determined for the received frame. This value ranges between 0 and 63.
	<b>regen-inner-priority</b>	- Regenerated inner-VLAN (CVLAN) priority value determined for the received frame. This value ranges between zero and seven.

**Mode** Priority Map Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** vlan - 0

in-priority-type - vlanPri

in-priority - -1

regen-priority - 0

**Example** `iss(config-pri-map)# map interface gig 0/1 vlan 4094 in-priority-type vlanPri in-priority 0 regen-priority 7 regen-inner-priority 1`



Priority Map entry should have been created.

**Related Commands**

- **priority-map** – Adds a Priority Map entry
- **show priority-map** – Displays the Priority Map entry.

## 64.1.15 match access-group

This command sets Class Map parameters using L2and/or L3 ACL or Priority Map ID.

```
match access-group { [mac-access-list <integer(0-65535)>] [ ip-access-list
<integer(0-65535)>] | priority-map <integer(0-65535)> }
```

**Syntax Description**     **mac-access-list**     - Identifier of the MAC filter. This value ranges between 0 and 65535.

**ip-access-list**        - Identifier of the IP filter. This value ranges between 0 and 65535.

**priority-map**         - Priority Map identifier for mapping incoming priority against received packet. This value ranges between 0 and 65535.

**Mode**                    Class Map Configuration Mode

**Package**                Workgroup, Enterprise and Metro

**Defaults**                mac-access-list            - 0

                          ip-access-list             - 0

                          priority-map               - 0

**Example**                `iss(config-cls-map)# match access-group priority-map 1`



- Priority map ID should have been created.
- L2 and/or L3 ACL should have been created.

**Related Commands**

- **priority-map** – Adds a Priority Map entry.
- **show class-map** – Displays the Class Map entry.

## 64.1.16 set class

This command sets CLASS for L2and/or L3 filters or Priority Map ID and adds a CLASS to Priority Map entry with regenerated priority. The no form of the command deletes a CLASS to Priority Map Table entry.

```
set class <class integer(1-65535)> [pre-color { green | yellow | red | none }]
[ regen-priority <integer(0-7)> group-name <string(31)> ]
```

```
no set class <class integer(1-65535)>
```

<b>Syntax Description</b>	<b>class</b>	- Traffic CLASS to which an incoming frame pattern is classified.
	<b>pre-color</b>	- Color of the packet prior to metering. This can be any one of the following: <ul style="list-style-type: none"> <li>• None – Traffic is not pre-colored.</li> <li>• green – Traffic conforms to SLAs (Service Level Agreements).</li> <li>• yellow – Traffic exceeds the SLAs.</li> <li>• red – Traffic violates the SLAs.</li> </ul>
	<b>regen-priority</b>	- Regenerated priority value determined for the input CLASS. This value ranges between zero and seven.
	<b>group-name</b>	- Unique identification of the group to which an input CLASS belongs.

**Mode** Class Map Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** class - 0

**Example**

```
iss(config-cls-map)# set class 1000 pre-color none regen-
priority 1 group-name CLASS
```



- Class map should have created.
- The default value zero provided for the class is not configurable.

**Related Commands** **show class-to-priority-map** – Displays the class group Entry.

## 64.1.17 meter-type

This command sets Meter parameters CIR, CBS, EIR, EBS, Interval, meter type and color awareness.

```
meter-type { simpleTokenBucket | avgRate | srTCM | trTCM | tswTCM | mefCoupled
| mefDeCoupled } [ color-mode { aware | blind } ] [interval <short(1-10000)>]
[cir <integer(0-65535)>] [cbs <integer(0-65535)>] [eir <integer(0-65535)>]
[ebs <integer(0-65535)>] [next-meter <integer(0-65535)>]
```

<b>Syntax Description</b>	<b>simpleTokenBucket</b>	- Two Parameter Token Bucket Meter.
	<b>avgRate</b>	- Average Rate Meter.
	<b>srTCM</b>	- Single Rate Three Color Marker Metering as defined by RFC 2697.
	<b>trTCM</b>	- Two Rate Three Color Marker Metering as defined by RFC 2698
	<b>tswTCM</b>	- Time Sliding Window Three Color Marker Metering as defined by RFC 2859.
	<b>mefCoupled</b>	- Dual bucket meter as defined by RFC 4115.
	<b>mefDeCoupled</b>	- Dual bucket meter as defined by RFC 2697 and MEF coupling Flag.
	<b>color-mode</b>	- Indicates the color mode of the Meter. The color modes are: <ul style="list-style-type: none"> <li>• aware – The Meter considers the pre-color of the packet.</li> <li>• blind – The Meter ignores the pre-color of the packet.</li> </ul>
	<b>interval</b>	- Time interval used with the token bucket. This value ranges between 1 and 10000.
	<b>cir</b>	- Committed information rate. This value ranges between 0 and 65535.

- cbs** - Committed burst size. This value ranges between 0 and 65535.
- eir** - Excess information rate. This value ranges between 0 and 65535.
- ebs** - Excess burst size. This value ranges between 0 and 65535.
- next-meter** - Meter entry identifier used for applying the second/next level of conformance on the incoming packet. This value ranges between 0 and 65535.

**Mode** Meter Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults**

- color-mode - blind
- interval - 0
- next-meter - 0

**Example**

```
iss(config-meter)# meter-type simpleTokenBucket color-mode
aware interval 10 cir 1000
```



Meter should have been created.

- Related Commands**
- **meter** – Creates a Meter.
  - **show meter** – Displays the Meter entry.

## 64.1.18 set policy

This command sets CLASS for policy. The no form of the command sets the default value for interface in this policy.

```
set policy [class <number(0-65535)>] [interface <iftype> <ifnum>] default-
priority-type { none | { vlanPri | ipTos | ipDscp | mplsExp } <integer(0-63)>
}
```

**no set policy interface**

<b>Syntax Description</b>	<b>class</b>	- Traffic CLASS for which the policy-map needs to be applied.
	<b>iftype</b>	- Interface type
	<b>ifnum</b>	- Interface number
	<b>default-priority-type</b>	- Per-Hop Behavior (PHB) type to be used for filling the default PHB for the policy-map entry. The types are: <ul style="list-style-type: none"> <li>• none – No specific PHB type is set.</li> <li>• vlanPri – VLAN priority.</li> <li>• ipTos – IP Type of Service.</li> <li>• ipDscp – IP Differentiated Services Code Point.</li> <li>• mplsExp – MPLS Experimental</li> </ul>
<b>Mode</b>	Policy Map Configuration Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Defaults</b>	<b>class</b>	- 0
<b>Example</b>	<pre>iss(config-ply-map)# set policy class 1 interface giga 0/1 default-priority-type none</pre> <p> CLASS should have been created.</p>	
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• <b>class-map</b> – Adds a Class Map Entry.</li> <li>• <b>policy-map</b> – Creates a policy map.</li> <li>• <b>show policy-map</b> – Displays the Policy Map Entry.</li> </ul>	

## 64.1.19 set meter

This command sets Policy parameters such as Meter and Meter Actions. The no form of the command removes the Meter from the Policy and the Meter Actions.

```
set meter <integer(1-65535)> [ conform-action { none | set-cos-transmit
<short(0-7)> set-de-transmit <short(0-1)> | set-port <iftype> <ifnum> | set-
inner-vlan-pri <short(0-7)> | set-mpls-exp-transmit <short(0-7)> | set-ip-prec-
transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> } ] [ exceed-action
{drop | set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)> | set-
inner-vlan-pri <short(0-7)> | set-mpls-exp-transmit <short(0-7)> | set-ip-
prec-transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> } ] [ violate-
action {drop | set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)> |
set-inner-vlan-pri <short(0-7)> | set-mpls-exp-transmit <short(0-7)> | set-ip-
prec-transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> } ] [ set-
conform-newclass <integer(0-65535)> ] [ set-exceed-newclass <integer(0-65535)>
] [ set-violate-newclass <integer(0-65535)> ]
```

no set meter

<b>Syntax Description</b>	<b>meter</b>	- Meter table identifier which is the index for the Meter table.
	<b>conform-action</b>	- Action to be performed on the packet, when the packets are found to be In profile (conform). Options are: <ul style="list-style-type: none"> <li>• none – No action is configured.</li> <li>• set-cos-transmit – Sets the VLAN priority of the outgoing packet.</li> <li>• set-de-transmit – Sets the VLAN Drop Eligible indicator of the outgoing packet.</li> <li>• set-port – Sets the new port value.</li> <li>• set-inner-vlan-pri – Sets the inner VLAN priority of the outgoing packet.</li> <li>• set-mpls-exp-transmit – Sets the MPLS Experimental bits of the outgoing packet.</li> <li>• set-ip-prec-transmit – Sets the new IP TOS value.</li> <li>• set-ip-dscp-transmit – Sets the new DSCP value.</li> </ul>
	<b>exceed-action</b>	- Action to be performed on the packet, when the packets are found to be In profile (exceed). Options are: <ul style="list-style-type: none"> <li>• drop – Drops the packet.</li> <li>• set-cos-transmit – Sets the VLAN priority of the outgoing packet.</li> <li>• set-de-transmit – Sets the VLAN Drop Eligible indicator of the outgoing packet.</li> </ul>

		<ul style="list-style-type: none"> <li>• set-inner-vlan-pri – Sets the inner VLAN priority of the outgoing packet.</li> <li>• set-mpls-exp-transmit – Sets the MPLS Experimental bits of the outgoing packet.</li> <li>• set-ip-prec-transmit – Sets the new IP TOS value.</li> <li>• set-ip-dscp-transmit – Sets the new DSCP value.</li> </ul>
<b>violate-action</b>	-	<p>Action to be performed on the packet, when the packets are found to be out of profile. Options are:</p> <ul style="list-style-type: none"> <li>• drop – Drops the packet.</li> <li>• set-cos-transmit – Sets the VLAN priority of the outgoing packet.</li> <li>• set-de-transmit – Sets the VLAN Drop Eligible indicator of the outgoing packet.</li> <li>• set-inner-vlan-pri – Sets the inner VLAN priority of the outgoing packet.</li> <li>• set-mpls-exp-transmit – Sets the MPLS Experimental bits of the outgoing packet.</li> <li>• set-ip-prec-transmit – Sets the new IP TOS value.</li> <li>• set-ip-dscp-transmit – Sets the new DSCP value.</li> </ul>
<b>set-conform-newclass</b>	-	Represents the Traffic CLASS to which an incoming frame pattern is classified after metering.
<b>set-exceed-newclass</b>	-	Represents the Traffic CLASS to which an incoming frame pattern is classified after metering.
<b>set-violate-newclass</b>	-	Represents the Traffic CLASS to which an incoming frame pattern is classified after metering.
<b>Mode</b>	Policy Map Configuration Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Defaults</b>	set-cos-transmit	- 0
	set-de-transmit	- 0
	set-mpls-exp-transmit	- 0

---

set-inner-vlan-pri - 0

**Example** iss(config-ply-map)# set meter 1 exceed-action drop violate-action drop



VLAN priority can be set to a non-zero value only when MPLS Experimental bits is set to zero.

**Related Commands** `show meter` – Displays the Meter entry.

## 64.1.20 set algo-type

This command sets Q Template entry parameters.

```
set algo-type { tailDrop | headDrop | red | wred } [queue-limit <integer(1-65535)>] [queue-drop-algo {enable | disable }]
```

<b>Syntax Description</b>	<b>algo-type</b>	<ul style="list-style-type: none"> <li>- Type of drop algorithm used by the queue template. Options are: <ul style="list-style-type: none"> <li>• tailDrop – Beyond the maximum depth of the queue, all newly arriving packets will be dropped.</li> <li>• headDrop – Packets currently at the head of the queue are dropped to make room for the new packet to be enqueued at the tail of the queue, when the current depth of the queue is at the maximum depth of the queue.</li> <li>• red – On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet.</li> <li>• wred – On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet.</li> </ul> </li> </ul>
	<b>queue-limit</b>	<ul style="list-style-type: none"> <li>- Queue size. This value ranges between 1 and 65535.</li> </ul>
	<b>queue-drop-algo</b>	<ul style="list-style-type: none"> <li>- Enable/disable Drop Algorithm for Congestion Management. Options are: <ul style="list-style-type: none"> <li>• enable – Enables Drop Algorithm.</li> <li>• disable – Disables Drop Algorithm.</li> </ul> </li> </ul>
<b>Mode</b>	Queue Template Configuration mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Defaults</b>	<b>queue-drop-algo</b>	- enable
<b>Example</b>	<pre>iss(config-qtype)# set algo-type red queue-limit 18 queue-drop-algo enable</pre>	
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• Queue size must be greater than or equal to the minimum average threshold and less than or equal to the maximum average threshold.</li> <li>• Drop algorithm for Congestion Management can be enabled only when the Random Detect Table entry is created for the Queue.</li> <li>• <b>random-detect dp</b> – Sets Random Detect Table entry parameters.</li> <li>• <b>show queue-template</b> – Displays the Q Template and Random Detect configurations.</li> </ul>	

## 64.1.21 random-detect dp

This command sets Random Detect Table entry parameters. The no form of the command deletes Random Detect Table entry.

```
random-detect dp <short(0-2)> [min-threshold <short(1-65535)>] [max-threshold
<short(1-65535)>] [max-pkt-size <short(1-65535)>] [mark-probability-
denominator <short(1-100)>] [exponential-weight <integer(0-31)>]
```

```
no random-detect dp <short(0-2)>
```

<b>Syntax Description</b>	<b>dp</b>	<ul style="list-style-type: none"> <li>- Drop Precedence. Options are: <ul style="list-style-type: none"> <li>• 0 – low drop precedence.</li> <li>• 1 – medium drop precedence.</li> <li>• 2 – high drop precedence.</li> </ul> </li> </ul>
	<b>min-threshold</b>	- Minimum average threshold for the random detect algorithm. This value ranges between 1 and 65535.
	<b>max-threshold</b>	- Maximum average threshold for the random detect algorithm. This value ranges between 1 and 65535.
	<b>max-pkt-size</b>	- Maximum allowed packet size. This value ranges between 1 and 65535.
	<b>mark-probability-denominator</b>	- Maximum probability of discarding a packet in units of percentage. This value ranges between 1 and 100.
	<b>exponential-weight</b>	- Exponential weight for determining the average queue size. This value ranges between 0 and 31.

**Mode** Queue Template Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** mark-probability-denominator - 100

exponential-weight - 0

**Example**

```
iss(config-qtype)# random-detect dp 1 min-threshold 1200 max-
threshold 13000 max-pkt-size 100 mark-probability-denominator
50 exponential-weight 30
```

## 64.1.22 show qos global info

This command displays QoS related global configurations.

### show qos global info

**Mode** Privileged EXEC Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show qos global info

```
QoS Global Information
```

```
-----
```

```
System Control           : Start
System Control           : Enable
Rate Unit                 : kbps
Rate Granularity         : 64
Trace Flag                : 0
```

- Related Commands**
- **shutdown qos** – Shutdown the QoS subsystem.
  - **qos** – Enables or disables the QoS subsystem.

## 64.1.23 show priority-map

This command displays the Priority Map entry.

```
show priority-map [<priority-map-id(1-65535)>]
```

**Syntax Description** **priority-map-id** - Output priority map index for the incoming packet received over ingress Port/VLAN with specified incoming priority.

**Mode** Privileged EXEC Mode.

**Package** Workgroup, Enterprise and Metro

**Example**

```
iss# show priority-map

QoS Priority Map Entries
=====
PriorityMapId           : 1
IfIndex                 : 1
VlanId                  : 4094
InPriorityType           : VlanPriority
InPriority               : 0
RegenPriority           : 7
InnerRegenPriority       : 1

iss# show priority-map 9

QoS Priority Map Entries
-----
PriorityMapId           : 9
IfIndex                 : gi 0/5
VlanId                  : 2
InPriorityType           : IP Protocol
InPriority               : -1
RegenPriority           : 5
InnerRegenPriority       : 7
```



If executed without the optional parameters, this command displays all the available Priority Map information.

**Related Commands**

- **priority-map** – Adds a Priority Map entry

- **map** - Adds a Priority Map entry for mapping an incoming priority to a regenerated priority

## 64.1.24 show class-map

This command displays the Class Map entry.

```
show class-map [<class-map-id(1-65535)>]
```

**Syntax Description**     **class-map-id**     - Index that enumerates the MultiField Classifier table entries.

**Mode**     Privileged EXEC Mode.

**Package**     Workgroup, Enterprise and Metro

**Example**     iss# show class-map

```

QoS Class Map Entries
=====
ClassMapId           : 1
L2FilterId           : None
L3FilterId           : None
PriorityMapId        : 1
CLASS                : 1000
PolicyMapId          : 1
PreColor             : None
Status               : Active

```



If executed without the optional parameters, this command displays all the available Class Map information

**Related Commands**

- **class-map** – Adds a Class Map entry.
- **priority-map** – Adds a Priority Map entry

## 64.1.25 show class-to-priority-map

This command displays the class group entry.

```
show class-to-priority-map <group-name (31)>
```

**Syntax Description**      **Group-name**                      - Unique identification of the group to which an input CLASS belongs.

**Mode**                      Privileged EXEC Mode.

**Package**                  Workgroup, Enterprise and Metro

**Example**                  iss# show class-to-priority-map CLASS1

```
QoS Class To Priority Map Entries
```

```
-----
GroupName      : CLASS1
Class           LocalPriority
-----
2               2
```

**Related Commands**

- **show class-map** – Displays the Class Map entry.
- **set class** – Sets CLASS for L2and/or L3 filters or Priority Map ID and adds a CLASS to Priority Map Entry with regenerated priority.

## 64.1.26 show meter

This command displays the Meter entry.

**show meter** [<meter-id(1-65535)>]

**Syntax Description**     **meter-id**                    - Index that enumerates the Meter entries.

**Mode**                    Privileged EXEC Mode.

**Package**                Workgroup, Enterprise and Metro

**Example**                iss# show meter

QoS Meter Entries

=====

```

MeterId                : 1
Type                   : Simple Token Bucket
Color Mode              : Color Aware
Interval               : 10
CIR                    : 1000
CBS                    : None
EIR                    : None
EBS                    : None
NextMeter              : None
Status                 : Active
  
```



If executed without the optional parameters, this command displays all the available Meter information.

**Related Commands**     **set meter** – Sets Policy parameters such as Meter and Meter Actions.

## 64.1.27 show policy-map

This command displays the Policy Map entry.

```
show policy-map [<meter-id(1-65535)>]
```

**Syntax Description**     **meter-id**                    - Index that enumerates the Meter entries.

**Mode**                    Privileged EXEC Mode.

**Package**                Workgroup, Enterprise and Metro

**Example**                iss# show policy-map

```
QoS Policy Map Entries
=====
PolicyMapId   : 1
IfIndex       : 0
Class         : 0
DefaultPHB    : None.
MeterId       : 1
ConNClass     : 0
ExcNClass     : 0
VioNClass     : 0
ConfAct       : Port 1
ExcAct        : Drop.
VioAct        : Drop.
```



If executed without the optional parameter, this command displays all the available Policy Map information

**Related Commands**     **set policy** – Sets CLASS for policy.

## 64.1.28 show queue-template

This command displays the Q Template and Random Detect configurations.

```
show queue-template [<queue-template-Id (1-65535)>]
```

**Syntax Description** `queue-template-Id` - Queue Template Table index.

**Mode** Privileged EXEC Mode.

**Package** Workgroup, Enterprise and Metro

**Example** `iss# show queue-template`

```
Queue Template Entries
```

```
-----
```

```
Q Template Id           : 1
Q Limit                 : 10000
Drop Type               : Tail Drop
Drop Algo Status       : Disable
```



If executed without the optional parameter, this command displays all the available Queue Template information.

**Related Commands** `queue-type` – Creates a Queue Template Type.

## 64.1.29 show shape-template

This command displays the Shape Template configurations.

```
show shape-template [<shape-template-Id (1-65535)>]
```

**Syntax Description**     **shape-template-Id** - Shape Template Table index.

**Mode**                    Privileged EXEC Mode.

**Package**                Workgroup, Enterprise and Metro

**Example**                iss# show shape-template

```
QoS Shape Template Entries
```

```
-----  
ShapeTemplate Id            CIR      CBS      EIR      EBS  
-----  
1                            1        1        1        1
```



If executed without the optional parameter, this command displays all the available Shape Template information

**Related Commands**     **shape-template** – Creates a Shape Template.

## 64.1.30 show scheduler

This command displays the configured Scheduler.

```
show scheduler [interface <iftype> <ifnum>]
```

**Syntax Description**

**iftype** - Interface type.

**ifnum** - Interface number.

**Mode** Privileged EXEC Mode.

**Package** Workgroup, Enterprise and Metro

**Example**

```
iss# show scheduler

QoS Scheduler Entries
-----

IfIndex Scheduler Index Scheduler Algo Shape Index Scheduler HL
GlobalId
-----
-----
Gi0/1      1                strictPriority      0                0
1
```



If executed without the optional parameter, this command displays all the available scheduler entries.

**Related Commands** **scheduler** – Creates a Scheduler and configures the Scheduler parameters.

## 64.1.31 show queue

This command displays the configured Queues.

```
show queue [interface <iftype> <ifnum>]
```

<b>Syntax Description</b>	<b>iftype</b>	- Interface type.
	<b>ifnum</b>	- Interface number.

**Mode** Privileged EXEC Mode.

**Package** Workgroup, Enterprise and Metro

**Example** iss# show queue

```

QoS Queue Entries
-----
IfIndex Queue Idx Queue Type Scheduler Idx Weight Priority
Shape Idx Global Id
-----
-----
Gi0/1      1          1          1          1          1
1          1

```



If executed without the optional parameter, this command displays all the available queue entries

**Related Commands**

- **queue** – Creates a Queue and configures the Queue parameters.
- **queue-type** – Creates a Queue Template Type.
- **show queue-template** – Displays the Q Template and Random Detect configurations.

## 64.1.32 show queue-map

This command displays the configured Queue map.

```
show queue-map [interface <iftype> <ifnum>]
```

**Syntax Description**

**iftype** - Interface type.

**ifnum** - Interface number.

**Mode** Privileged EXEC Mode.

**Package** Workgroup, Enterprise and Metro

**Example**

```
iss# show queue-map
```

QoS Queue Map Entries

```
-----
```

IfIndex	CLASS	PriorityType	Priority Value	Mapped Queue
Gi0/1	1	none	0	1



If executed without the optional parameter, this command displays all the available queue map entries.

**Related Commands** **queue-map** – Creates a Map for a Queue with Class or regenerated priority.

## 64.1.33 show sched-hierarchy

This command displays the configured hierarchy scheduler.

```
show sched-hierarchy [interface <iftype> <ifnum>]
```

<b>Syntax Description</b>	<b>iftype</b>	- Interface type.
	<b>ifnum</b>	- Interface number.

**Mode** Privileged EXEC Mode.

**Package** Workgroup, Enterprise and Metro

**Example** iss# show sched-hierarchy

```
QoS Hierarchy Scheduler Entries
```

```
-----
```

IfIndex	Hierarchy	Level	Sched	Index	NextQueue	Id	NextSched	Id
Weight	Priority							

```
-----
```

Gi0/1		1		1		0		2
1	1							



If executed without the optional parameter, this command displays all the available hierarchy scheduler entries

**Related Commands**

- **scheduler** – Creates a Scheduler and configures the Scheduler parameters.
- **sched-hierarchy** – Creates a Scheduler Hierarchy.

## 64.1.34 show qos def-user-priority

This command displays the configured default ingress user priority for a port.

```
show qos def-user-priority [interface <iftype> <ifnum>]
```

**Syntax Description**

**iftype** - Interface type.

**ifnum** - Interface number.

**Mode** Privileged EXEC Mode.

**Package** Workgroup, Enterprise and Metro

**Example**

```
iss# show qos def-user-priority
```

QoS Default User Priority Entries

```
-----
```

IfIndex	Default User Priority
-----	-----
Gi0/1	0
Gi0/2	0
Gi0/3	0
Gi0/4	0
Gi0/5	0
Gi0/6	0
Gi0/7	0
Gi0/8	0
Gi0/9	0
Gi0/10	0
Gi0/11	0
Gi0/12	0
Gi0/13	0
Gi0/14	0
Gi0/15	0
Gi0/16	0
Gi0/17	0

---

Gi0/18	0
Gi0/19	0
Gi0/20	0
Gi0/21	0
Gi0/22	0
Gi0/23	0
Gi0/24	0



If executed without the optional parameter, this command displays the available default ingress user priority entries for all the interface.

**Related  
Commands**

**qos interface** – Sets the default ingress user priority for the port.

## 64.1.35 show qos meter-stats

This command displays the Meters statistics for conform, exceed, violate packets and octets count.

**show qos meter-stats** [<Meter-Id(1-65535)>]

**Syntax Description**     **Meter-Id**                     -    Index that enumerates the Meter entries.

**Mode**                     Privileged EXEC Mode.

**Package**                 Workgroup, Enterprise and Metro

**Example**                 iss# show qos meter-stats

```
QoS Meter (Policer) Stats
```

```
-----
```

```
Meter Index                     : 1
Conform Packets                 : 00
Conform Octets                 : 00
Exceed Packets                 : 00
Exceed Octets                 : 00
Violate Packets                 : 00
Violate Octets                 : 0
```



If executed without the optional parameter, this command displays the Meter statistics for all the available Meters.

**Related Commands**

- **show meter** – Displays the Meter entry.
- **set meter** – Sets Policy parameters such as Meter and Meter Actions.

## 64.1.36 show qos queue-stats

This command displays Queue statistics for EnQ, DeQ, discarded packets and octets Count, Management Algo Drop and Q occupancy.

```
show qos queue-stats [interface <iftype> <ifnum>]
```

**Syntax Description**     **iftype**                     - Interface Type.

**ifnum**                     - Interface Number.

**Mode**                     Privileged EXEC Mode.

**Package**                 Workgroup, Enterprise and Metro

**Example**                 iss# show qos queue-stats

```
QoS Queue Stats
```

```
-----
```

```
Interface Index                 : Gi 0/1
Queue Index                     : 2
EnQ Packets                     : 00
EnQ Octets                      : 00
DeQ Packets                     : 00
DeQ Octets                      : 00
Discard Packets                 : 00
Discard Octets                 : 00
Occupancy Octets               : 00
CongMgmtAlgoDrop Octets       : 00
```



If executed without the optional parameter, this command displays the Queue statistics for all the available Interfaces.

**Related Commands**     **show queue** – Displays the configured Queues.

## 64.2 xCAT Specific Commands

This section describes the CLI commands executable only in xCAT target for configuring QoS feature supported by ISS.

The list of CLI commands for the configuration of **QoS** is as follows:

- shutdown qos
- qos
- priority-map
- class-map
- meter
- policy-map
- queue-type
- shape-template
- scheduler
- queue
- queue-map
- sched-hierarchy
- qos interface
- map
- match access-group
- set class
- meter-type
- set policy
- set meter
- set algo-type
- random-detect dp
- show qos global info
- show priority-map
- show class-map
- show class-to-priority-map
- show meter
- show policy-map
- show queue-template
- show shape-template
- show scheduler

- show queue
- show queue-map
- show sched-hierarchy
- show qos def-user-priority
- show qos meter-stats
- show qos queue-stats

## 64.2.1 shutdown qos

This command shuts down the QoS subsystem. The no form of the command starts the QoS subsystem.

**shutdown qos**

**no shutdown qos**

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** QoS subsystem is started and enabled by default.

**Example** `iss(config)# shutdown qos`



- Resources required by QoS subsystem are allocated and QoS subsystem starts running, when started.
- All the MemPools used by the QoS subsystem will be released, when shutdown.

**Related Commands** `show qos global info` - Displays QoS related global configurations.

## 64.2.2 qos

This command enables or disables the QoS subsystem.

**qos {enable | disable}**

**Syntax Description**      **enable**                      - Enables QoS subsystem

**disable**                      - Disables Qos subsystem

**Mode**                      Global Configuration Mode

**Package**                  Workgroup, Enterprise and Metro

**Defaults**                  Enabled

**Example**                  `iss(config)# qos enable`



- QoS module programs the hardware and starts protocol operation, when set as **enable**.
- QoS module stops protocol operation by deleting the hardware configuration, when set as **disable**.

**Related Commands**      `show qos global info` - Displays QoS related global configurations.

## 64.2.3 priority-map

This command adds a Priority Map entry. The no form of the command deletes a Priority Map entry.

```
priority-map <priority-map-Id(1-65535)>
```

```
no priority-map <priority-map-Id(1-65535)>
```

<b>Syntax Description</b>	<b>Priority-map-Id</b>	- Priority map index for the incoming packet received over ingress Port/VLAN with specified incoming priority. This value ranges between 1 and 65535.
---------------------------	------------------------	---

<b>Mode</b>	Global Configuration Mode
-------------	---------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Example</b>	<code>iss(config)# priority-map 1</code>
----------------	--



QoS subsystem should have been started.

<b>Related Commands</b>	<code>show priority-map</code> – Displays the Priority Map entry.
-------------------------	---

## 64.2.4 class-map

This command adds a Class Map entry. The no form of the command deletes a Class Map entry.

```
class-map <class-map-id(1-65535)>
```

```
no class-map <class-map-id(1-65535)>
```

<b>Syntax Description</b>	<b>class-map-id</b>	- Index that enumerates the MultiField Classifier table entries. This value ranges between 1 and 65535.
---------------------------	---------------------	---

<b>Mode</b>	Global Configuration Mode
-------------	---------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Example</b>	<pre>iss(config)# class-map 1</pre>
----------------	-------------------------------------



QoS subsystem should have been started.

<b>Related Commands</b>	<b>show class-map</b> – Displays the Class Map entry.
-------------------------	---

## 64.2.5 meter

This command creates a Meter. The no form of the command deletes a Meter.

```
meter <meter-id(1-65535)>
```

```
no meter <meter-id(1-65535)>
```

<b>Syntax Description</b>	<b>meter-id</b>	- Index that enumerates the Meter entries. This value ranges between 1 and 65535.
---------------------------	-----------------	---

<b>Mode</b>	Global Configuration Mode
-------------	---------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Example</b>	<code>iss(config)# meter 1</code>
----------------	-----------------------------------



QoS subsystem should have been started.

<b>Related Commands</b>	<code>show meter</code> – Displays the Meter entry.
-------------------------	---

## 64.2.6 policy-map

This command creates a policy map. The no form of the command deletes a policy map.

```
policy-map <policy-map-id (1-65535)>
```

```
no policy-map <policy-map-id (1-65535)>
```

<b>Syntax Description</b>	<b>policy-map-id</b>	- Index that enumerates the policy-map table entries. This value ranges between 1 and 65535.
---------------------------	----------------------	--

<b>Mode</b>	Global Configuration Mode
-------------	---------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Example</b>	<pre>iss(config)# policy-map 1</pre>
----------------	--------------------------------------



QoS subsystem should have been started.

<b>Related Commands</b>	<b>show policy-map</b> – Displays the Policy Map entry.
-------------------------	---

## 64.2.7 queue-type

This command creates a Queue Template Type. The no form of the command deletes a Queue Template Type.

```
queue-type <Q-Template-Id(1-65535)>
```

```
no queue-type <Q-Template-Id(1-65535)>
```

<b>Syntax Description</b>	<b>Q-Template-Id</b>	- Queue Template Table index. This value ranges between 1 and 65535.
---------------------------	----------------------	--

<b>Mode</b>	Global Configuration Mode
-------------	---------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Example</b>	<code>iss(config)# queue-type 1</code>
----------------	--

<b>Related Commands</b>	<code>show queue-template</code> - Displays the Q Template and Random Detect configurations.
-------------------------	--

## 64.2.8 shape-template

This command creates a Shape Template. The no form of the command deletes a Shape Template.

```
shape-template <integer(1-65535)> [cir <integer(1-65535)>] [cbs <integer(0-65535)>] [eir <integer(0-65535)>] [ebs <integer(0-65535)>]
```

```
no shape-template <Shape-Template-Id(1-65535)>
```

<b>Syntax Description</b>	<b>Shape-Template-Id</b> - Shape Template Table index.
	<b>cir</b> - Committed information rate for packets through the queue.
	<b>cbs</b> - Committed burst size for packets through the queue.
	<b>eir</b> - Excess information rate for packets through the hierarchy.
	<b>ebs</b> - Excess burst size for packets through the hierarchy.
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise and Metro
<b>Example</b>	iss(config)# shape-template 1 cir 20 cbs 40 eir 50 ebs 40
<b>Related Commands</b>	<b>show shape-template</b> – Displays the Shape Template configurations.

## 64.2.9 scheduler

This command creates a Scheduler and configures the Scheduler parameters. The no form of the command deletes a scheduler.

```
scheduler <integer(1-65535)> interface <iftype> <ifnum> [sched-algo {strict-
priority | rr | wrr | wfq | strict-rr | strict-wrr | strict-wfq | deficit-rr}]
[shaper <integer(0-65535)>] [hierarchy-level <integer(0-10)>]
no scheduler <Scheduler-Id(1-65535)> interface <iftype> <ifnum>
```

<b>Syntax Description</b>	<b>Scheduler-Id</b>	- Scheduler identifier that uniquely identifies the scheduler in the system/egress interface.
	<b>iftype</b>	- Interface type.
	<b>ifnum</b>	- Interface number.
	<b>sched-algo</b>	- Packet scheduling algorithm for the port. The algorithms are: <ul style="list-style-type: none"> <li>• strict-priority – strictPriority.</li> <li>• rr – roundRobin.</li> <li>• wrr – weightedRoundRobin.</li> <li>• wfq – weightedFairQueing.</li> <li>• strict-rr – strictRoundRobin.</li> <li>• strict-wrr – strictWeightedRoundRobin.</li> <li>• strict-wfq – strictWeightedFairQueing.</li> <li>• deficit-rr – deficitRoundRobin.</li> </ul>
	<b>shaper</b>	- Shaper identifier that specifies the bandwidth requirements for the scheduler.
	<b>hierarchy-level</b>	- Depth of the queue/scheduler hierarchy.
<b>Mode</b>	Global Configuration Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Defaults</b>	sched-algo	- strict-priority

hierarchy-level - 0

**Example** `iss(config)# scheduler 1 interface giga 0/1 sched-algo rr  
shaper 1 hierarchy-level 1`



Shaper identifier is not mandatory for the creation of the conceptual row.

**Related  
Commands**

- **show scheduler** – Displays the configured Scheduler.
- **sched-hierarchy** – Creates a Scheduler Hierarchy.
- **show sched-hierarchy** – Displays the configured hierarchy scheduler.

## 64.2.10 queue

This command creates a Queue and configures the Queue parameters. The no form of the command deletes a Queue.

```
queue <integer(1-65535)> interface <iftype> <ifnum> [qtype <integer(1-65535)>]
[scheduler <integer(1-65535)>] [weight <integer(0-1000)>] [priority
<integer(0-15)>] [shaper <integer(0-65535)>]
```

```
no queue <integer(1-65535)> interface <iftype> <ifnum>
```

<b>Syntax Description</b>	<b>queue</b>	- Queue identifier that uniquely identifies the queue in the system/port.
	<b>iftype</b>	- Interface type.
	<b>ifnum</b>	- Interface number.
	<b>qtype</b>	- Queue Type identifier.
	<b>scheduler</b>	- Scheduler identifier that manages the specified queue.
	<b>weight</b>	- User assigned weight to the CoS queue.
	<b>priority</b>	User assigned priority for the CoS queue.
	<b>shaper</b>	Shaper identifier that specifies the bandwidth requirements for the queue.

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** weight - 0

priority - 0

**Example** iss(config)# queue 1 interface giga 0/1 qtype 2 scheduler 1  
 weight 20 priority 10 shaper 1.



- Scheduler identifier is unique relative to an egress interface.
- User assigned weights are used only when scheduling algorithm is a weighted scheduling algorithm.
- User assigned priority is used only when the scheduler uses a priority based scheduling algorithm.
- Shaper identifier is not mandatory for the creation of the row.

**Related  
Commands**

- **queue-type** – Creates a Queue Template Type.
- **scheduler** – Creates a Scheduler and configures the Scheduler parameters.
- **shape-template** – Creates a Shape Template.
- **show queue** – Displays the configured Queues.

## 64.2.11 queue-map

This command creates a Map for a Queue with Class or regenerated priority. The no form of the command deletes a Queue map entry.

```
queue-map { CLASS <integer(1-65535)> | regn-priority { vlanPri | ipTos | ipDscp | mplsExp | vlanDEI } <integer(0-63)> } [interface <iftyp> <ifnum>] queue-id <integer(1-65535)>
```

```
no queue-map { CLASS <integer(1-65535)> | regn-priority { vlanPri | ipTos | ipDscp | mplsExp | vlanDEI } <integer(0-63)> } [interface <iftyp> <ifnum>]
```

<b>Syntax Description</b>	<b>CLASS</b>	- Input CLASS that needs to be mapped to an outbound queue.
	<b>regn-priority</b>	- Regenerated-priority type and regenerated-priority that needs to be mapped to an outbound queue. The types are <ul style="list-style-type: none"> <li>• vlanPri – VLAN Priority.</li> <li>• ipTos – IP Type of Service.</li> <li>• ipDscp – IP Differentiated Services Code Point.</li> <li>• mplsExp – MPLS Experimental</li> <li>• vlanDEI – VLAN Drop Eligibility Indicator.</li> </ul>
	<b>iftyp</b>	- Interface type.
	<b>ifnum</b>	- Interface number.
	<b>queue-id</b>	- Queue identifier that uniquely identifies a queue relative to an interface.

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss(config)# queue-map CLASS 1 interface giga 0/1 queue-id 1



- CLASS should be zero while configuring RegenPriority specific Q.
- Regenerated-priority should be zero while configuring CLASS specific Queue.

**Related Commands** `show queue-map` – Displays the configured Queue map.

## 64.2.12 sched-hierarchy

This command creates a Scheduler Hierarchy. The no form of the command deletes a Scheduler Hierarchy.

```

sched-hierarchy interface <iftype> <ifnum> hierarchy-level <integer(1-10)>
sched-id <integer(1-65535)> {next-level-queue <integer(0-65535)> | next-level-
scheduler <integer(0-65535)>} [priority <integer(0-15)>] [weight <integer(0-
1000)>]
  
```

```

no sched-hierarchy interface <iftype> <ifnum> hierarchy-level <integer(1-10)>
sched-id <integer(1-65535)>
  
```

<b>Syntax Description</b>	<b>iftype</b>	- Interface type.
	<b>ifnum</b>	- Interface number.
	<b>hierarchy-level</b>	- Depth of the queue/scheduler hierarchy.
	<b>sched-id</b>	- Scheduler identifier. <ul style="list-style-type: none"> <li>• next-level-queue – Next-level queue to which the scheduler output needs to be sent.</li> <li>• next-level-scheduler – Next-level scheduler to which the scheduler output needs to be sent.</li> </ul>
	<b>priority</b>	- Scheduler priority.
	<b>weight</b>	- Scheduler weight.
<b>Mode</b>	Global Configuration Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Defaults</b>	<b>priority</b>	- 0
<b>Example</b>	<pre> iss(config)# sched-hierarchy interface giga 0/1 hierarchy-level 3 sched-id 1 next-level-queue 2 priority 5 weight 50           </pre>	
	<ul style="list-style-type: none"> <li>• The priority is specified when the scheduler is connecting to any of the priorities ( EF, AF, BE) of the next level strict-priority scheduler.</li> <li>• The weight is specified if the scheduler is connecting to a WeightedFairQueuing of another scheduler.</li> </ul>	
<b>Related Commands</b>	<b>show sched-hierarchy</b> – Displays the configured hierarchy scheduler.	

## 64.2.13 qos interface

This command sets the default ingress user priority for the port.

```
qos interface <iftype> <ifnum> def-user-priority <integer (0-7)>
```

<b>Syntax Description</b>	<b>iftype</b>	- Interface type
	<b>ifnum</b>	- Interface number
	<b>def-user-priority</b>	- Default ingress user priority for the port
<b>Mode</b>	Global Configuration Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Example</b>	iss(config)# qos interface giga 0/1 def-user-priority 3	
	The default ingress user priority will be used to set priority for untagged packets.	
<b>Related Commands</b>	<b>show qos def-user-priority</b> – Displays the configured default ingress user priority for a port.	

## 64.2.14 map

This command adds a Priority Map Entry for mapping an incoming priority to a regenerated priority. The no form of the command sets default value to the Interface, VLAN, regenerated inner priority.

```
map [interface <iftype> <ifnum>] [vlan <integer(1-4094)>] in-priority-type {
vlanPri | ipTos | ipDscp | mplsExp | vlanDEI } [in-priority <integer(0-63)>]
regen-priority <integer(0-63)> [regen-inner-priority <integer(0-7)>]
```

```
no map { interface | vlan | regen-inner-priority }
```

<b>Syntax Description</b>	<b>iftype</b>	- Interface type
	<b>ifnum</b>	- Interface number
	<b>vlan</b>	- VLAN identifier. This value ranges between 1 and 4094.
	<b>in-priority-type</b>	- Type of the incoming priority. The types are: <ul style="list-style-type: none"> <li>• vlanPri – VLAN Priority.</li> <li>• ipTos – IP Type of Service.</li> <li>• ipDscp – IP Differentiated Services Code Point.</li> <li>• mplsExp – MPLS Experimental</li> <li>• vlanDEI – VLAN Drop Eligibility Indicator.</li> </ul>
	<b>in-priority</b>	- Incoming priority value determined for the received frame. This value ranges between 0 and 63.
	<b>regen-priority</b>	- Regenerated priority value determined for the received frame. This value ranges between 0 and 63.
	<b>regen-inner-priority</b>	- Regenerated inner-VLAN (CVLAN) priority value determined for the received frame. This value ranges between zero and seven.

**Mode** Priority Map Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** vlan - 0

in-priority-type - vlanPri

in-priority - -1

regen-priority - 0

**Example** `iss(config-pri-map)# map interface gig 0/1 vlan 4094 in-priority-type vlanPri in-priority 0 regen-priority 7 regen-inner-priority 1`



Priority Map entry should have been created.

**Related Commands**

- **priority-map** – Adds a Priority Map entry
- **show priority-map** – Displays the Priority Map entry.

## 64.2.15 match access-group

This command sets Class Map parameters using L2and/or L3 ACL or Priority Map ID.

```
match access-group { [mac-access-list <integer(0-65535)>] [ ip-access-list
<integer(0-65535)>] | priority-map <integer(0-65535)> }
```

**Syntax Description** **mac-access-list** - Identifier of the MAC filter. This value ranges between 0 and 65535.

**ip-access-list** - Identifier of the IP filter. This value ranges between 0 and 65535.

**priority-map** - Priority Map identifier for mapping incoming priority against received packet. This value ranges between 0 and 65535.

**Mode** Class Map Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** mac-access-list - 0

ip-access-list - 0

priority-map - 0

**Example** `iss(config-cls-map)# match access-group priority-map 1`



- Priority map ID should have been created.
- L2 and/or L3 ACL should have been created.

**Related Commands**

- **priority-map** – Adds a Priority Map entry.
- **show class-map** – Displays the Class Map entry.

## 64.2.16 set class

This command sets CLASS for L2and/or L3 filters or Priority Map ID and adds a CLASS to Priority Map entry with regenerated priority. The no form of the command deletes a CLASS to Priority Map Table entry.

```
set class <class integer(1-65535)> [pre-color { green | yellow | red | none }]
[ regen-priority <integer(0-7)> group-name <string(31)> ]
```

```
no set class <class integer(1-65535)>
```

<b>Syntax Description</b>	<b>class</b>	- Traffic CLASS to which an incoming frame pattern is classified.
	<b>pre-color</b>	- Color of the packet prior to metering. This can be any one of the following: <ul style="list-style-type: none"> <li>• None – Traffic is not pre-colored.</li> <li>• green – Traffic conforms to SLAs (Service Level Agreements).</li> <li>• yellow – Traffic exceeds the SLAs.</li> <li>• red – Traffic violates the SLAs.</li> </ul>
	<b>regen-priority</b>	- Regenerated priority value determined for the input CLASS. This value ranges between zero and seven.
	<b>group-name</b>	- Unique identification of the group to which an input CLASS belongs.

**Mode** Class Map Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** class - 0

**Example**

```
iss(config-cls-map)# set class 1000 pre-color none regen-
priority 1 group-name CLASS
```



- Class map should have created.
- The default value zero provided for the class is not configurable.

**Related Commands** `show class-to-priority-map` – Displays the class group Entry.

## 64.2.17 meter-type

This command sets Meter parameters CIR, CBS, EIR, EBS, Interval, meter type and color awareness.

```
meter-type { simpleTokenBucket | avgRate | srTCM | trTCM | tswTCM | mefCoupled
| mefDeCoupled } [ color-mode { aware | blind } ] [interval <short(1-10000)>]
[cir <integer(0-65535)>] [cbs <integer(0-65535)>] [eir <integer(0-65535)>]
[ebs <integer(0-65535)>] [next-meter <integer(0-65535)>]
```

<b>Syntax Description</b>	<b>simpleTokenBucket</b>	- Two Parameter Token Bucket Meter.
	<b>avgRate</b>	- Average Rate Meter.
	<b>srTCM</b>	- Single Rate Three Color Marker Metering as defined by RFC 2697.
	<b>trTCM</b>	- Two Rate Three Color Marker Metering as defined by RFC 2698
	<b>tswTCM</b>	- Time Sliding Window Three Color Marker Metering as defined by RFC 2859.
	<b>mefCoupled</b>	- Dual bucket meter as defined by RFC 4115.
	<b>mefDeCoupled</b>	- Dual bucket meter as defined by RFC 2697 and MEF coupling Flag.
	<b>color-mode</b>	- Indicates the color mode of the Meter. The color modes are: <ul style="list-style-type: none"> <li>• aware – The Meter considers the pre-color of the packet.</li> <li>• blind – The Meter ignores the pre-color of the packet.</li> </ul>
	<b>interval</b>	- Time interval used with the token bucket. This value ranges between 1 and 10000.
	<b>cir</b>	- Committed information rate. This value ranges between 0 and 65535.
	<b>cbs</b>	- Committed burst size. This value ranges between 0 and 65535.

- eir** - Excess information rate. This value ranges between 0 and 65535.
- ebs** - Excess burst size. This value ranges between 0 and 65535.
- next-meter** - Meter entry identifier used for applying the second/next level of conformance on the incoming packet. This value ranges between 0 and 65535.

**Mode** Meter Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** color-mode - blind

interval - 0

next-meter - 0

**Example** `iss(config-meter)# meter-type simpleTokenBucket color-mode aware interval 10 cir 1000`



Meter should have been created.

**Related Commands**

- **meter** – Creates a Meter.
- **show meter** – Displays the Meter entry.

## 64.2.18 set policy

This command sets CLASS for policy. The no form of the command sets the default value for interface in this policy.

```
set policy [class <number(0-65535)>] [interface <iftype> <ifnum>] default-
priority-type { none | { vlanPri | ipTos | ipDscp | mplsExp } <integer(0-63)>
}
```

**no set policy interface**

<b>Syntax Description</b>	<b>class</b>	- Traffic CLASS for which the policy-map needs to be applied.
	<b>iftype</b>	- Interface type
	<b>ifnum</b>	- Interface number
	<b>default-priority-type</b>	- Per-Hop Behavior (PHB) type to be used for filling the default PHB for the policy-map entry. The types are: <ul style="list-style-type: none"> <li>• none – No specific PHB type is set.</li> <li>• vlanPri – VLAN priority.</li> <li>• ipTos – IP Type of Service.</li> <li>• ipDscp – IP Differentiated Services Code Point.</li> <li>• mplsExp – MPLS Experimental</li> </ul>

**Mode** Policy Map Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** class - 0

**Example** iss(config-ply-map)# set policy class 1 interface giga 0/1  
default-priority-type none



CLASS should have been created.

- Related Commands**
- **class-map** – Adds a Class Map Entry.
  - **policy-map** – Creates a policy map.
  - **show policy-map** – Displays the Policy Map Entry.

## 64.2.19 set meter

This command sets Policy parameters such as Meter and Meter Actions. The no form of the command removes the Meter from the Policy and the Meter Actions.

```
set meter <integer(1-65535)> [ conform-action { none | set-cos-transmit
<short(0-7)> set-de-transmit <short(0-1)> | set-port <iftype> <ifnum> | set-
inner-vlan-pri <short(0-7)> | set-mpls-exp-transmit <short(0-7)> | set-ip-prec-
transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> } ] [ exceed-action
{drop | set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)> | set-
inner-vlan-pri <short(0-7)> | set-mpls-exp-transmit <short(0-7)> | set-ip-
prec-transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> } ] [ violate-
action {drop | set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)> |
set-inner-vlan-pri <short(0-7)> | set-mpls-exp-transmit <short(0-7)> | set-ip-
prec-transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> } ] [ set-
conform-newclass <integer(0-65535)> ] [ set-exceed-newclass <integer(0-65535)>
] [ set-violate-newclass <integer(0-65535)> ]
```

no set meter

<b>Syntax Description</b>	<b>meter</b>	- Meter table identifier which is the index for the Meter table.
	<b>conform-action</b>	- Action to be performed on the packet, when the packets are found to be In profile (conform). Options are: <ul style="list-style-type: none"> <li>• none – No action is configured.</li> <li>• set-cos-transmit – Sets the VLAN priority of the outgoing packet.</li> <li>• set-de-transmit – Sets the VLAN Drop Eligible indicator of the outgoing packet.</li> <li>• set-port – Sets the new port value.</li> <li>• set-inner-vlan-pri – Sets the inner VLAN priority of the outgoing packet.</li> <li>• set-mpls-exp-transmit – Sets the MPLS Experimental bits of the outgoing packet.</li> <li>• set-ip-prec-transmit – Sets the new IP TOS value.</li> <li>• set-ip-dscp-transmit – Sets the new DSCP value.</li> </ul>
	<b>exceed-action</b>	- Action to be performed on the packet, when the packets are found to be In profile (exceed). Options are: <ul style="list-style-type: none"> <li>• drop – Drops the packet.</li> <li>• set-cos-transmit – Sets the VLAN priority of the outgoing packet.</li> </ul>

	<ul style="list-style-type: none"> <li>• set-de-transmit – Sets the VLAN Drop Eligible indicator of the outgoing packet.</li> <li>• set-inner-vlan-pri – Sets the inner VLAN priority of the outgoing packet.</li> <li>• set-mpls-exp-transmit – Sets the MPLS Experimental bits of the outgoing packet.</li> <li>• set-ip-prec-transmit – Sets the new IP TOS value.</li> <li>• set-ip-dscp-transmit – Sets the new DSCP value.</li> </ul>
<b>violate-action</b>	<ul style="list-style-type: none"> <li>- Action to be performed on the packet, when the packets are found to be out of profile. Options are:           <ul style="list-style-type: none"> <li>• drop – Drops the packet.</li> <li>• set-cos-transmit – Sets the VLAN priority of the outgoing packet.</li> <li>• set-de-transmit – Sets the VLAN Drop Eligible indicator of the outgoing packet.</li> <li>• set-inner-vlan-pri – Sets the inner VLAN priority of the outgoing packet.</li> <li>• set-mpls-exp-transmit – Sets the MPLS Experimental bits of the outgoing packet.</li> <li>• set-ip-prec-transmit – Sets the new IP TOS value.</li> <li>• set-ip-dscp-transmit – Sets the new DSCP value.</li> </ul> </li> </ul>
<b>set-conform-newclass</b>	<ul style="list-style-type: none"> <li>- Represents the Traffic CLASS to which an incoming frame pattern is classified after metering.</li> </ul>
<b>set-exceed-newclass</b>	<ul style="list-style-type: none"> <li>- Represents the Traffic CLASS to which an incoming frame pattern is classified after metering.</li> </ul>
<b>set-violate-newclass</b>	<ul style="list-style-type: none"> <li>- Represents the Traffic CLASS to which an incoming frame pattern is classified after metering.</li> </ul>
<b>Mode</b>	Policy Map Configuration Mode
<b>Package</b>	Workgroup, Enterprise and Metro
<b>Defaults</b>	<ul style="list-style-type: none"> <li>set-cos-transmit - 0</li> <li>set-de-transmit - 0</li> </ul>

set-mpls-exp-transmit - 0

set-inner-vlan-pri - 0

**Example** `iss(config-ply-map)# set meter 1 exceed-action drop violate-action drop`



VLAN priority can be set to a non-zero value only when MPLS Experimental bits is set to zero.

**Related Commands** `show meter` – Displays the Meter entry.

## 64.2.20 set algo-type

This command sets Q Template entry parameters.

```
set algo-type { tailDrop | headDrop | red | wred } [queue-limit <integer(1-65535)>] [queue-drop-algo {enable | disable }]
```

<b>Syntax Description</b>	<b>algo-type</b>	<ul style="list-style-type: none"> <li>- Type of drop algorithm used by the queue template. Options are: <ul style="list-style-type: none"> <li>• tailDrop – Beyond the maximum depth of the queue, all newly arriving packets will be dropped.</li> <li>• headDrop – Packets currently at the head of the queue are dropped to make room for the new packet to be enqueued at the tail of the queue, when the current depth of the queue is at the maximum depth of the queue.</li> <li>• red – On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet.</li> <li>• wred – On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet.</li> </ul> </li> </ul>
	<b>queue-limit</b>	<ul style="list-style-type: none"> <li>- Queue size. This value ranges between 1 and 65535.</li> </ul>
	<b>queue-drop-algo</b>	<ul style="list-style-type: none"> <li>- Enable/disable Drop Algorithm for Congestion Management. Options are: <ul style="list-style-type: none"> <li>• enable – Enables Drop Algorithm.</li> <li>• disable – Disables Drop Algorithm.</li> </ul> </li> </ul>
<b>Mode</b>	Queue Template Configuration mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Defaults</b>	<b>queue-drop-algo</b>	- enable
<b>Example</b>	<pre>iss(config-qtype)# set algo-type red queue-limit 18 queue-drop-algo enable</pre>	
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• Queue size must be greater than or equal to the minimum average threshold and less than or equal to the maximum average threshold.</li> <li>• Drop algorithm for Congestion Management can be enabled only when the Random Detect Table entry is created for the Queue.</li> <li>• <b>random-detect dp</b> – Sets Random Detect Table entry parameters.</li> <li>• <b>show queue-template</b> – Displays the Q Template and Random Detect configurations.</li> </ul>	

## 64.2.21 random-detect dp

This command sets Random Detect Table entry parameters. The no form of the command deletes Random Detect Table entry.

```
random-detect dp <short(0-2)> [min-threshold <short(1-65535)>] [max-threshold
<short(1-65535)>] [max-pkt-size <short(1-65535)>] [mark-probability-
denominator <short(1-100)>] [exponential-weight <integer(0-31)>]
```

```
no random-detect dp <short(0-2)>
```

<b>Syntax Description</b>	<b>dp</b>	<ul style="list-style-type: none"> <li>- Drop Precedence. Options are:           <ul style="list-style-type: none"> <li>• 0 – low drop precedence.</li> <li>• 1 – medium drop precedence.</li> <li>• 2 – high drop precedence.</li> </ul> </li> </ul>
	<b>min-threshold</b>	- Minimum average threshold for the random detect algorithm. This value ranges between 1 and 65535.
	<b>max-threshold</b>	- Maximum average threshold for the random detect algorithm. This value ranges between 1 and 65535.
	<b>max-pkt-size</b>	- Maximum allowed packet size. This value ranges between 1 and 65535.
	<b>mark-probability-denominator</b>	- Maximum probability of discarding a packet in units of percentage. This value ranges between 1 and 100.
	<b>exponential-weight</b>	- Exponential weight for determining the average queue size. This value ranges between 0 and 31.

**Mode** Queue Template Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults**

mark-probability-denominator	-	100
exponential-weight	-	0

**Example**

```
iss(config-qtype)# random-detect dp 1 min-threshold 1200 max-
threshold 13000 max-pkt-size 100 mark-probability-denominator
50 exponential-weight 30
```

## 64.2.22 show qos global info

This command displays QoS related global configurations.

### show qos global info

**Mode** Privileged EXEC Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show qos global info

```
QoS Global Information
```

```
-----
```

```
System Control           : Start
System Control           : Enable
Rate Unit                 : kbps
Rate Granularity         : 64
Trace Flag                : 0
```

- Related Commands**
- **shutdown qos** – Shutdown the QoS subsystem.
  - **qos** – Enables or disables the QoS subsystem.

## 64.2.23 show priority-map

This command displays the Priority Map entry.

**show priority-map** [<priority-map-id(1-65535)>]

**Syntax Description**     **priority-map-id**     -     Output priority map index for the incoming packet received over ingress Port/VLAN with specified incoming priority.

**Mode**                     Privileged EXEC Mode.

**Package**                 Workgroup, Enterprise and Metro

**Example**

```

iss# show priority-map

QoS Priority Map Entries
=====
PriorityMapId           : 1
IfIndex                 : 1
VlanId                  : 4094
InPriorityType          : VlanPriority
InPriority               : 0
RegenPriority           : 7
InnerRegenPriority      : 1

iss# show priority-map 9

QoS Priority Map Entries
-----
PriorityMapId           : 9
IfIndex                 : gi 0/5
VlanId                  : 2
InPriorityType          : IP Protocol
InPriority               : -1
RegenPriority           : 5
InnerRegenPriority      : 7
    
```



If executed without the optional parameters, this command displays all the available Priority Map information.

**Related Commands**

- **priority-map** – Adds a Priority Map entry

- **map** - Adds a Priority Map entry for mapping an incoming priority to a regenerated priority

## 64.2.24 show class-map

This command displays the Class Map entry.

```
show class-map [<class-map-id(1-65535)>]
```

**Syntax Description**     **class-map-id**     - Index that enumerates the MultiField Classifier table entries.

**Mode**     Privileged EXEC Mode.

**Package**     Workgroup, Enterprise and Metro

**Example**     iss# show class-map

```
QoS Class Map Entries
```

```
=====
```

```
ClassMapId           : 1
L2FilterId           : None
L3FilterId           : None
PriorityMapId         : 1
CLASS                 : 1000
PolicyMapId          : 1
PreColor              : None
Status                : Active
```



If executed without the optional parameters, this command displays all the available Class Map information

**Related Commands**

- **class-map** – Adds a Class Map entry.
- **priority-map** – Adds a Priority Map entry

## 64.2.25 show class-to-priority-map

This command displays the class group entry.

```
show class-to-priority-map <group-name (31)>
```

**Syntax Description**      **Group-name**                      - Unique identification of the group to which an input CLASS belongs.

**Mode**                      Privileged EXEC Mode.

**Package**                  Workgroup, Enterprise and Metro

**Example**                  iss# show class-to-priority-map CLASS1

```
QoS Class To Priority Map Entries
```

```
-----  
GroupName        : CLASS1  
Class                      LocalPriority  
-----  
2                                      2
```

**Related Commands**

- **show class-map** – Displays the Class Map entry.
- **set class** – Sets CLASS for L2and/or L3 filters or Priority Map ID and adds a CLASS to Priority Map Entry with regenerated priority.

## 64.2.26 show meter

This command displays the Meter entry.

**show meter** [<meter-id (1-65535)>]

**Syntax Description**     **meter-id**                     - Index that enumerates the Meter entries.

**Mode**                     Privileged EXEC Mode.

**Package**                 Workgroup, Enterprise and Metro

**Example**                 iss# show meter

```

QoS Meter Entries
=====
MeterId                : 1
Type                   : Simple Token Bucket
Color Mode             : Color Aware
Interval               : 10
CIR                    : 1000
CBS                    : None
EIR                    : None
EBS                    : None
NextMeter              : None
Status                 : Active

```



If executed without the optional parameters, this command displays all the available Meter information.

**Related Commands**     **set meter** – Sets Policy parameters such as Meter and Meter Actions.

## 64.2.27 show policy-map

This command displays the Policy Map entry.

```
show policy-map [<meter-id(1-65535)>]
```

**Syntax Description**     **meter-id**                     - Index that enumerates the Meter entries.

**Mode**                     Privileged EXEC Mode.

**Package**                 Workgroup, Enterprise and Metro

**Example**                 iss# show policy-map

```
QoS Policy Map Entries
=====
PolicyMapId   : 1
IfIndex       : 0
Class         : 0
DefaultPHB    : None.
MeterId       : 1
ConNClass     : 0
ExcNClass     : 0
VioNClass     : 0
ConfAct       : Port 1
ExcAct        : Drop.
VioAct        : Drop.
```



If executed without the optional parameter, this command displays all the available Policy Map information

**Related**                 **set policy** – Sets CLASS for policy.

**Commands**

## 64.2.28 show queue-template

This command displays the Q Template and Random Detect configurations.

```
show queue-template [<queue-template-Id (1-65535)>]
```

**Syntax Description** `queue-template-Id` - Queue Template Table index.

**Mode** Privileged EXEC Mode.

**Package** Workgroup, Enterprise and Metro

**Example** `iss# show queue-template`

```
Queue Template Entries
```

```
-----
```

```
Q Template Id           : 1
Q Limit                 : 10000
Drop Type               : Tail Drop
Drop Algo Status       : Disable
```



If executed without the optional parameter, this command displays all the available Queue Template information.

**Related Commands** `queue-type` – Creates a Queue Template Type.

## 64.2.29 show shape-template

This command displays the Shape Template configurations.

```
show shape-template [<shape-template-Id (1-65535)>]
```

**Syntax Description**     **shape-template-Id** - Shape Template Table index.

**Mode**                    Privileged EXEC Mode.

**Package**                Workgroup, Enterprise and Metro

**Example**                iss# show shape-template

```
QoS Shape Template Entries
```

```
-----
ShapeTemplate Id          CIR      CBS      EIR      EBS
-----
1                          1        1        1        1
```



If executed without the optional parameter, this command displays all the available Shape Template information

**Related Commands**     **shape-template** – Creates a Shape Template.

## 64.2.30 show scheduler

This command displays the configured Scheduler.

**show scheduler** [interface <iftype> <ifnum>]

**Syntax Description**

**iftype** - Interface type.

**ifnum** - Interface number.

**Mode** Privileged EXEC Mode.

**Package** Workgroup, Enterprise and Metro

**Example**

```
iss# show scheduler

QoS Scheduler Entries
-----

IfIndex Scheduler Index Scheduler Algo Shape Index Scheduler HL
GlobalId
-----
-----
Gi0/1      1                strictPriority      0          0
1
```



If executed without the optional parameter, this command displays all the available scheduler entries.

**Related Commands** **scheduler** – Creates a Scheduler and configures the Scheduler parameters.

## 64.2.31 show queue

This command displays the configured Queues.

```
show queue [interface <iftype> <ifnum>]
```

**Syntax**      **iftype**                    - Interface type.  
**Description**

**ifnum**                    - Interface number.

**Mode**            Privileged EXEC Mode.

**Package**        Workgroup, Enterprise and Metro

**Example**        iss# show queue

```
QoS Queue Entries
-----
IfIndex Queue Idx Queue Type Scheduler Idx Weight Priority Shape
Idx Global Id
-----
-
-----
Gi0/1        1                1                1                1                1
1
```



If executed without the optional parameter, this command displays all the available queue entries

**Related Commands**

- **queue** – Creates a Queue and configures the Queue parameters.
- **queue-type** – Creates a Queue Template Type.
- **show queue-template** – Displays the Q Template and Random Detect configurations.

## 64.2.32 show queue-map

This command displays the configured Queue map.

```
show queue-map [interface <iftype> <ifnum>]
```

**Syntax Description**

**iftype** - Interface type.

**ifnum** - Interface number.

**Mode** Privileged EXEC Mode.

**Package** Workgroup, Enterprise and Metro

**Example**

```
iss# show queue-map
```

QoS Queue Map Entries

```
-----
```

IfIndex	CLASS	PriorityType	Priority Value	Mapped Queue
Gi0/1	1	none	0	1



If executed without the optional parameter, this command displays all the available queue map entries.

**Related Commands** **queue-map** – Creates a Map for a Queue with Class or regenerated priority.

## 64.2.33 show sched-hierarchy

This command displays the configured hierarchy scheduler.

```
show sched-hierarchy [interface <iftype> <ifnum>]
```

**Syntax**      **iftype**                      - Interface type.  
**Description**

**ifnum**                      - Interface number.

**Mode**            Privileged EXEC Mode.

**Package**        Workgroup, Enterprise and Metro

**Example**        iss# show sched-hierarchy

```
QoS Hierarchy Scheduler Entries
```

```
-----  
IfIndex Hierarchy Level Sched Index NextQueue Id NextSched Id  
Weight Priority  
-----  
-----  
-----  
Gi0/1            1                      1                      0                      2                      1  
1
```



If executed without the optional parameter, this command displays all the available hierarchy scheduler entries

**Related Commands**

- **scheduler** – Creates a Scheduler and configures the Scheduler parameters.
- **sched-hierarchy** – Creates a Scheduler Hierarchy.

## 64.2.34 show qos def-user-priority

This command displays the configured default ingress user priority for a port.

```
show qos def-user-priority [interface <iftype> <ifnum>]
```

**Syntax Description**

**iftype** - Interface type.

**ifnum** - Interface number.

**Mode** Privileged EXEC Mode.

**Package** Workgroup, Enterprise and Metro

**Example**

```
iss# show qos def-user-priority

QoS Default User Priority Entries
-----
IfIndex  Default User Priority
-----
Gi0/1           0
Gi0/2           0
Gi0/3           0
Gi0/4           0
Gi0/5           0
Gi0/6           0
Gi0/7           0
Gi0/8           0
Gi0/9           0
Gi0/10          0
Gi0/11          0
Gi0/12          0
Gi0/13          0
Gi0/14          0
Gi0/15          0
Gi0/16          0
Gi0/17          0
```

---

Gi0/18	0
Gi0/19	0
Gi0/20	0
Gi0/21	0
Gi0/22	0
Gi0/23	0
Gi0/24	0



If executed without the optional parameter, this command displays the available default ingress user priority entries for all the interface.

**Related  
Commands**

**qos interface** – Sets the default ingress user priority for the port.

## 64.2.35 show qos meter-stats

This command displays the Meters statistics for conform, exceed, violate packets and octets count.

**show qos meter-stats** [<Meter-Id(1-65535)>]

**Syntax Description**     **Meter-Id**                     -    Index that enumerates the Meter entries.

**Mode**                     Privileged EXEC Mode.

**Package**                 Workgroup, Enterprise and Metro

**Example**                 iss# show qos meter-stats

```
QoS Meter (Policer) Stats
```

```
-----
```

```
Meter Index                     : 1
Conform Packets                 : 00
Conform Octets                  : 00
Exceed Packets                  : 00
Exceed Octets                   : 00
Violate Packets                 : 00
Violate Octets                   : 0
```



If executed without the optional parameter, this command displays the Meter statistics for all the available Meters.

**Related Commands**

- **show meter** – Displays the Meter entry.
- **set meter** – Sets Policy parameters such as Meter and Meter Actions.

## 64.2.36 show qos queue-stats

This command displays Queue statistics for EnQ, DeQ, discarded packets and octets Count, Management Algo Drop and Q occupancy.

```
show qos queue-stats [interface <iftype> <ifnum>]
```

**Syntax Description**     **iftype**                     - Interface Type.

**ifnum**                     - Interface Number.

**Mode**                     Privileged EXEC Mode.

**Package**                 Workgroup, Enterprise and Metro

**Example**                 iss# show qos queue-stats

```
QoS Queue Stats
```

```
-----
```

```
Interface Index                 : Gi 0/1
Queue Index                     : 2
EnQ Packets                     : 00
EnQ Octets                      : 00
DeQ Packets                     : 00
DeQ Octets                      : 00
Discard Packets                 : 00
Discard Octets                 : 00
Occupancy Octets               : 00
CongMgmtAlgoDrop Octets       : 00
```



If executed without the optional parameter, this command displays the Queue statistics for all the available Interfaces.

**Related Commands**     **show queue** – Displays the configured Queues.

## 64.3 DCB Product Overview

Data Center Bridging (DCB) incorporates a set of enhancements for IEEE Ethernet which enable consolidated, high performance and scalable data center Ethernet network infrastructures. Ethernet is the most widespread wired local area network (LAN) technology and the continuous advances in speeds and feeds of Ethernet makes it the choice of network users in data centers. While Ethernet has become the de facto standard for servers, routers, and network appliances in data centers, storage devices continue to use traditional storage network technologies such as fiber channel. While iSCSI allows network-attached storage devices to use Ethernet, DCB enables fiber channel networking over Ethernet. The consolidation of storage technology with Ethernet will enable a single, unified data center network that is easier to maintain and manage at a much lower total cost of ownership. Besides consolidation, DCB features also enable higher bandwidth and lower latency with maximum network efficiency to build high performance data centers of the future.

The following figure explains the logical organization of Interface Masters DCB product. The Interface Masters DCB module contains the CN implementation as defined in CN standard, DCBX protocol implementation as defined in DCBX standard and the modules like PFC, ETS and Application priority feature that uses DCBX for exchanging and deriving their operational parameters.

### 64.3.1 DCBX

DCBX is a discovery and capability exchange protocol that is used by devices enabled for Data Center Bridging to exchange configuration (DCB features) information. DCB (Data Center Bridging) refers to enhancements to Ethernet local area networks for use in data center environments. Traditional Ethernet is the primary network protocol in data centers for computer to computer communications. However, Ethernet is designed to be a best-effort network that may drop packets or deliver packets out of order when the network or devices are busy.

Interface Masters DCBX protocol supports the following DCB features:

- PFC (Priority-based Flow Control) - Provides a link level flow control mechanism that can be independently controlled for each priority.
- ETS (Enhanced Transmission Selection) - Provides a common management framework for assignment of bandwidth to the traffic classes.
- Application Priority feature – This feature is used to announce the upper layer protocols and associated priority map about the availability of the dcb link for traffic. The upper layer protocols may include L2 or L3 or L4.

Interface Masters DCBX implementation involves the DCBX Protocol development and PFC, ETS functionalities realization using DCBX protocol. PFC and ETS uses DCBX protocol to dynamically exchange and learn the operational parameters of the peers.

The list of CLI commands for the configuration of DCB is as follows:

- shutdown ets
- ets
- ets trap
- set priority grouping
- priority-grouping mode
- set priority-group willing

- map priority
- set priority-group bandwidth
- set priority-group recommendation bandwidth
- dcbx tlv-select etstlv
- show interfaces - priority-grouping
- show interfaces priority-grouping counters
- show ets global info
- clear priority-grouping counters
- shutdown pfc
- pfc
- set pfc threshold limit
- pfc trap
- set priority-flow-control
- priority-flow-control mode
- set priority-flow-control willing
- set priority flow-control
- dcbx tlv-select pfctlv
- show interfaces - priority-flow-control
- show interfaces priority-flow-control counters
- show priority-flow-control config
- show pfc global info
- clear priority-flow-control counters
- set dcbx
- show dcbx ports
- debug dcbx

### 64.3.1.1 shutdown ets

This command shutdowns the ETS subsystem in the switch. The no form of the command starts the ETS module in the switch. When the services of the ETS module are not required, it is shutdown. All the resources used by the ETS module are released back to the system.

**shutdown ets**

**no shutdown ets**

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** ETS is started

**Example** `iss(config)# shutdown ets`

- Related Commands**
- **ets** - Enables/disables the ETS module globally on the subsystem
  - **ets trap** - Enables sending trap notification messages to the ETS system
  - **ets trap** - Enables sending trap notification messages to the ETS system
  - **set priority grouping** - Enables /disables row status ETS feature on the port.
  - **priority-grouping mode** - Configures the admin mode of the ETS module on a port
  - **set priority-group willing** - Configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.
  - **map priority** - Maps the priority to the priority group identifier
  - **set priority-group bandwidth** - Configures the bandwidth limit for the port
  - **set priority-group recommendation bandwidth** - Configures the recommendation bandwidth for the port
  - **dcbx tlv-select etstlv** - Enables the transmission of ETS TLVs

### 64.3.1.2 ets

This command enables/disables the ETS module globally on the subsystem.

**ets {enable | disable}**

<b>Syntax description</b>	<b>enable</b>	Configures the ETS module as enabled. All the ports for which ETS has been enabled are enabled at this instance and starts the DCBX state machine on the port that has admin mode as auto.
	<b>disable</b>	Configures the ETS module as disabled. Disables the ETS feature in all the ports where it was previously enabled and stops the DCBX state machine on the port that has admin mode as auto.

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** ETS is enabled

**Example** `iss(config)# ets enable`



This command can be executed only if ETS module is started in the switch

#### Related Commands

- **shutdown ets** - Shuts down the ETS subsystem in the switch.
- **ets trap** - Enables sending trap notification messages to the ETS system
- **set priority grouping** - Enables /disables row status ETS feature on the port.
- **priority-grouping mode** - Configures the admin mode of the ETS module on a port
- **set priority-group willing** - Configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.
- **map priority** - Maps the priority to the priority group identifier
- **set priority-group bandwidth** - Configures the bandwidth limit for the port
- **set priority-group recommendation bandwidth** - Configures the recommendation bandwidth for the port
- **dcbx tlv-select etstlv** - Enables the transmission of ETS TLVs

### 64.3.1.3 ets trap

This command enables sending trap notification messages to the ETS system. The no form of the command disables sending trap messages to the ETS system.

```
ets trap {all | [module-status-change] [admin-mode-change] [peer-status-change] [sem-change]}
```

```
no ets trap {all | [module-status-change] [admin-mode-change] [peer-status-change] [sem-change]}
```

<b>Syntax Description</b>	<b>all</b>	- Generates all types of trap messages
<b>n</b>	<b>module-status-change</b>	- Generates the module state change trap messages
	<b>admin-mode-change</b>	- Generates admin status change trap for each port
	<b>peer-status-change</b>	- Generates peer status as up or down trap
	<b>sem-change</b>	- Generates the ETS DCBX state machine status regarding trap.

**Mode** Global configuration Mode

**Package** Workgroup, Enterprise and Metro

**Default** module-status-change and admin-mode-change

**Example** iss(config)# ets trap all

**Related Commands**

- **shutdown ets** – Shutdown the ETS subsystem in the switch
- **ets** – Enables/disables the ETS module globally on the subsystem
- **set priority grouping** – Enables /disables row status ETS feature on the port.
- **priority-grouping mode** – Configures the admin mode of the ETS module on a port
- **set priority-group willing** – Configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.
- **map priority** – Maps the priority to the priority group identifier
- **set priority-group bandwidth** – Configures the bandwidth limit for the port
- **set priority-group recommendation bandwidth** – Configures the

recommendation bandwidth for the port

- `dcbx tlv-select etstlv` - Enables the transmission of ETS TLVs

### 64.3.1.4 set priority grouping

This command enables /disables row status ETS feature on the port.

```
set priority-grouping {enable|disable}
```

<b>Syntax Description</b>	<b>enable</b>	-	Enables priority-grouping on the port.
	<b>disable</b>	-	Disables priority-grouping on the port.

**Mode** Interface configuration mode

**Package** Workgroup, Enterprise and Metro

**Defaults** Disabled on all ports

**Example** `iss(config-if)# set priority-grouping enable`

- Related Commands**
- **shutdown ets** – shutdown the ETS subsystem in the switch
  - **ets** – enables/disables the ETS module globally on the subsystem
  - **ets trap** – enables sending trap notification messages to the ETS system
  - **priority-grouping mode** – configures the admin mode of the ETS module on a port
  - **set priority-group willing** – configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.
  - **map priority** – maps the priority to the priority group identifier
  - **set priority-group bandwidth** – configures the bandwidth limit for the port
  - **set priority-group recommendation bandwidth** – configures the recommendation bandwidth for the port
  - **dcbx tlv-select etstlv** – enables the transmission of ETS TLVs
  - **show interfaces** – displays interfaces specific priority-group information
  - **show interfaces priority-grouping counters** – displays the counters for ETS TLVs on this port

### 64.3.1.5 priority-grouping mode

This command configures the admin mode of the ETS module on a port. The no form of the command disables the ETS feature on a port.

```
priority-grouping mode {auto|on}
```

```
no priority-grouping mode
```

<b>Syntax</b>	<b>auto</b>	-	Configures the admin mode as auto. If the ETS feature is enabled on this port, all the parameters for the ETS module is determined by the DCBX state machine.
---------------	-------------	---	---

<b>Description</b>	<b>on</b>	-	Configures the admin mode as on. If the ETS feature is enabled on this port, all the parameters for the ETS module is not determined by the DCBX state machine.
--------------------	-----------	---	---

<b>Mode</b>	Interface Configuration Mode.
-------------	-------------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Defaults</b>	admin mode is off.
-----------------	--------------------

<b>Example</b>	iss(config-if)# priority grouping mode auto
----------------	---

<b>Related commands</b>	<ul style="list-style-type: none"> <li>• <b>shutdown ets</b> – Shuts down the ETS subsystem in the switch</li> <li>• <b>ets</b> – enables/disables the ETS module globally on the subsystem</li> <li>• <b>ets trap</b> – enables sending trap notification messages to the ETS system</li> <li>• <b>set priority grouping</b> - enables /disables row status ETS feature on the port</li> <li>• <b>set priority-group willing</b> – configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.</li> <li>• <b>map priority</b> – maps the priority to the priority group identifier</li> <li>• <b>set priority-group bandwidth</b> – configures the bandwidth limit for the port</li> <li>• <b>set priority-group recommendation bandwidth</b> – configures the recommendation bandwidth for the port</li> <li>• <b>dcbx tlv-select etstlv</b> – enables the transmission of ETS TLVs</li> </ul>
-------------------------	--

### 64.3.1.6 set priority-group willing

This command configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.

```
set priority-group willing {enable | disable}
```

<b>Syntax Description</b>	<b>enable</b>	- Enables the acceptance status of the priority group
	<b>disable</b>	- Disables the acceptance status of the priority group

**Mode** Interface configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** disable

**Example** iss(config-if)# set priority-group willing enable

- Related commands**
- **shutdown ets** - Shuts down ets subsystem on the switch.
  - **ets** - enables/disables the ETS module globally on the subsystem
  - **ets trap** - enables sending trap notification messages to the ETS system
  - **set priority grouping** - enables /disables row status ETS feature on the port.
  - **priority-grouping mode** - configures the admin mode of the ETS module on a port
  - **map priority** - maps the priority to the priority group identifier
  - **set priority-group bandwidth** - configures the bandwidth limit for the port
  - **set priority-group recommendation bandwidth** - configures the recommendation bandwidth for the port
  - **dcbx tlv-select etstlv** - enables the transmission of ETS TLVs

### 64.3.1.7 map priority

This command maps the priority to the priority group identifier.

```
map priority <priority-list> priority-group <integer(0-7) | 15>
```

<b>Syntax Description</b>	<b>priority-list</b>	- Configures the priority-list to be assigned to the priority group. This value ranges between 0 and 7.
	<b>priority-group</b>	- Configures the priority group identifier. This value ranges between 0 and 7 or 15. 15 indicates the priority group with no bandwidth limit.

**Mode** Interface Configuration mode

**Package** Workgroup, Enterprise and Metro

**Defaults** Priority is mapped to the default priority 15 (that is, no bandwidth limit).

**Example** `iss(config-if)# map priority 1 priority-group 1`



Data center bridging should be enabled, before executing this command.

**Related Commands**

- **shutdown ets** - Shuts down ets subsystem on the switch.
- **ets** - enables/disables the ETS module globally on the subsystem
- **ets trap** - enables sending trap notification messages to the ETS system
- **set priority grouping** - enables /disables row status ETS feature on the port.
- **priority-grouping mode** - configures the admin mode of the ETS module on a port
- **set priority-group willing** - configures the willingness status of the local system to accept the ETS configuration recommended by the remote system
- **set priority-group bandwidth** - configures the bandwidth limit for the port
- **set priority-group recommendation bandwidth** - configures the recommendation bandwidth for the port
- **dcbx tlv-select etstlv** - enables the transmission of ETS TLVs

### 64.3.1.8 set priority-group bandwidth

This command configures the bandwidth limit for the port. The sum of eight bandwidth is equal to 100.

```
set priority-group bandwidth <prioritygroup-bw0> <prioritygroup-  
bw1><prioritygroup-bw2> <prioritygroup-bw3> <prioritygroup-bw4>  
<prioritygroup-bw5> <prioritygroup-bw6> <prioritygroup-bw7>
```

<b>Syntax Description</b>	<b>prioritygroup-bw0</b>	-	Configures the bandwidth value in percentage, to be allocated to the priority group 0.
	<b>prioritygroup-bw1</b>	-	Configures the bandwidth value in percentage, to be allocated to the priority group 1.
	<b>prioritygroup-bw2</b>	-	Configures the bandwidth value in percentage, to be allocated to the priority group 2.
	<b>prioritygroup-bw3</b>	-	Configures the bandwidth value in percentage, to be allocated to the priority group 3.
	<b>prioritygroup-bw4</b>	-	Configures the bandwidth value in percentage, to be allocated to the priority group 4.
	<b>prioritygroup-bw5</b>	-	Configures the bandwidth value in percentage, to be allocated to the priority group 5.
	<b>prioritygroup-bw6</b>	-	Configures the bandwidth value in percentage, to be allocated to the priority group 6.
	<b>prioritygroup-bw7</b>	-	Configures the bandwidth value in percentage, to be allocated to the priority group 7.

**Mode** Interface Configuration mode

**Package** Workgroup, Enterprise and Metro

<b>Defaults</b>	<b>prioritygroup-bw0</b>	-	12%
	<b>prioritygroup-bw1</b>	-	12%
	<b>prioritygroup-bw2</b>	-	12%
	<b>prioritygroup-bw3</b>	-	12%

prioritygroup-bw4	-	13%
prioritygroup-bw5	-	13%
prioritygroup-bw6	-	13%
prioritygroup-bw7	-	13%

**Example** `iss(config-if)# set priority-group bandwidth 25 20 15 11 11 4 6 8`



- Data center bridging should be enabled, before executing this command.
- The sum of eight bandwidth should be equal to 100.

#### Related Commands

- `shutdown ets` - Shuts down ets subsystem on the switch.
- `ets` - enables/disables the ETS module globally on the subsystem
- `ets trap` - enables sending trap notification messages to the ETS system
- `set priority grouping` - enables /disables row status ETS feature on the port.
- `priority-grouping mode` - configures the admin mode of the ETS module on a port
- `set priority-group willing` - configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.
- `map priority` - maps the priority to the priority group identifier
- `set priority-group recommendation bandwidth` - configures the recommendation bandwidth for the port
- `dcbx tlv-select etstlv` - enables the transmission of ETS TLVs
- `show interfaces` - displays interfaces specific priority-group information
- `show interfaces priority-grouping counters` - displays the counters for ETS TLVs on this port

### 64.3.1.9 set priority-group recommendation bandwidth

This command configures the recommendation bandwidth for the port. The total badwidth of eight octets is 100.

```
set priority-group recommendation bandwidth <prioritygroup-bw0>
<prioritygroup-bw1><prioritygroup-bw2> <prioritygroup-bw3> <prioritygroup-bw4>
<prioritygroup-bw5> <prioritygroup-bw6> <prioritygroup-bw7>
```

<b>Syntax Description</b>	<b>prioritygroup-bw0</b>	-	Configures the recommended bandwidth value in percentage, to be allocated to the priority group 0.
	<b>prioritygroup-bw1</b>	-	Configures the recommended bandwidth value in percentage, to be allocated to the priority group 1.
	<b>prioritygroup-bw2</b>	-	Configures the recommended bandwidth value in percentage, to be allocated to the priority group 2.
	<b>prioritygroup-bw3</b>	-	Configures the recommended bandwidth value in percentage, to be allocated to the priority group 3.
	<b>prioritygroup-bw4</b>	-	Configures the recommended bandwidth value in percentage, to be allocated to the priority group 4.
	<b>prioritygroup-bw5</b>	-	Configures the recommended bandwidth value in percentage, to be allocated to the priority group 5.
	<b>prioritygroup-bw6</b>	-	Configures the recommended bandwidth value in percentage, to be allocated to the priority group 6.
	<b>prioritygroup-bw7</b>	-	Configures the recommended bandwidth value in percentage, to be allocated to the priority group 7.
<b>Mode</b>	Interface Configuration mode		
<b>Package</b>	Workgroup, Enterprise and Metro		
<b>Defaults</b>	<b>prioritygroup-bw0</b>	-	12%
	<b>prioritygroup-bw1</b>	-	12%
	<b>prioritygroup-bw2</b>	-	12%

prioritygroup-bw3	-	12%
prioritygroup-bw4	-	13%
prioritygroup-bw5	-	13%
prioritygroup-bw6	-	13%
prioritygroup-bw7	-	13%

**Example** `iss(config-if)# set priority-group recommendation bandwidth 25 20 15 11 11 4 6 8`



- Data center bridging should be enabled, before executing this command.
- The sum of eight bandwidth should be equal to 100.

### Related Commands

- **shutdown ets** - Shuts down ets subsystem on the switch .
- **ets** - enables/disables the ETS module globally on the subsystem
- **ets trap** - enables sending trap notification messages to the ETS system
- **set priority grouping** - enables /disables row status ETS feature on the port.
- **priority-grouping mode** - configures the admin mode of the ETS module on a port
- **set priority-group willing** - configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.
- **map priority** - maps the priority to the priority group identifier
- **dcbx tlv-select etstlv** - enables the transmission of ETS TLVs
- **show interfaces** - displays interfaces specific priority-group information
- **show interfaces priority-grouping counters** - displays the counters for ETS TLVs on this port

### 64.3.1.10 dcbx tlv-select etstlv

This command enables the transmission of ETS TLVs.

```
dcbx tlv-select etstlv [configuration] [recommendation] [tc-supported]
```

```
no dcbx tlv-select etstlv [configuration] [recommendation] [tc-supported]
```

<b>Syntax Description</b>	<b>configuration</b>	-	Configures the values for ETS TLV
<b>n</b>	<b>recommendation</b>	-	Configures the recommendation of bandwidth allocation
	<b>tc-supported</b>	-	Configures the Traffic class supported TLV

**Mode** Interface Configuration mode

**Package** Workgroup, Enterprise and Metro

**Defaults** The transmission of all TLVs are disabled

**Example** `iss(config-if)# dcbx tlv-select etstlv configuration`

- Related commands**
- `shutdown ets` - Shuts down ets subsystem on the switch.
  - `ets` - enables/disables the ETS module globally on the subsystem
  - `ets trap` - enables sending trap notification messages to the ETS system
  - `set priority grouping` - enables /disables row status ETS feature on the port.
  - `priority-grouping mode` - configures the admin mode of the ETS module on a port
  - `set priority-group willing` - configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.
  - `map priority` - maps the priority to the priority group identifier
  - `set priority-group recommendation bandwidth` - configures the recommendation bandwidth for the port
  - `show interfaces` - displays interfaces specific priority-group information
  - `show interfaces priority-grouping counters` - displays the counters for ETS TLVs on this port

### 64.3.1.11 show interfaces - priority-grouping

This command displays interfaces specific priority-group information.

```
show interfaces [<ifXtype> <ifnum> ] priority-grouping [detail]
```

<b>Syntax</b>	<b>&lt;ifXtype&gt;</b>	<ul style="list-style-type: none"> <li>- Displays the information on specified type of interface. The interface can be: <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> </li> </ul>
<b>Description</b>	<b>&lt;ifnum&gt;</b>	<ul style="list-style-type: none"> <li>- Displays the information on specified interface identifier. This is a unique value that represents the specific interface.  This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.  For example: 0/1 represents that the slot number is 0 and port number is 1.  Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</li> </ul>
<b>n</b>	<b>details</b>	<ul style="list-style-type: none"> <li>- Displays the information regarding the admin port, local port and remote port table.</li> </ul>
<b>Mode</b>	Privilege EXEC Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Example</b>	<pre>iss# sh inter priority-grouping detail</pre> <hr style="border-top: 1px dashed #000;"/> <pre>ETS Port Gi0/3      Information</pre>	

-----  
 ETS Local Port Info  
 -----

TGID	Bandwidth	RecomBandwidth	Priority
0	12%	12%	
1	12%	12%	
2	12%	12%	
3	12%	12%	
4	13%	13%	
5	13%	13%	
6	13%	13%	
7	13%	13%	
15	-	-	0 1 2 3 4 5 6 7

Max Supported TC Group :0  
 Number of Traffic Class :8  
 Willing Status :Disabled

 -----  
 ETS Admin Port Info  
 -----

TGID	Bandwidth	RecomBandwidth	Priority
0	12%	12%	
1	12%	12%	
2	12%	12%	
3	12%	12%	
4	13%	13%	
5	13%	13%	
6	13%	13%	
7	13%	13%	
15	-	-	0 1 2 3 4 5 6 7

Max Supported TCG :0  
 Number of Traffic Class :8  
 Willing Status :Disabled

 -----  
 ETS Remote Port Info  
 -----

No Remote Entry is Present

 -----  
 ETS Port Related Info  
 -----

ETS Conf TLV Tx Status :Disabled  
 ETS Reco TLV Tx Status :Disabled  
 ETS TC Supp TLV Tx Status:Disabled

ETS Port Mode :OFF MODE  
 ETS Oper State :OFF STATE  
 ETS State Machine Type :Assymmetric

 -----  
 -----

**Related  
Commands**

- **shutdown ets** - Shuts down ets subsystem on the switch.
- **ets** - enables/disables the ETS module globally on the subsystem
- **ets trap** - enables sending trap notification messages to the ETS system
- **set priority grouping** - enables /disables row status ETS feature on the port.
- **priority-grouping mode** - configures the admin mode of the ETS module on a port
- **set priority-group willing** - configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.
- **map priority** - maps the priority to the priority group identifier
- **set priority-group recommendation bandwidth** - configures the recommendation bandwidth for the port
- **show interfaces priority-grouping counters** - displays the counters for ETS TLVs on this port

### 64.3.1.12 show interfaces priority-grouping counters

This command displays the counters for ETS TLVs on this port.

**show interfaces priority-grouping counters [ <ifXtype> <ifnum> ]**

- |                    |                        |   |   |
|--------------------|------------------------|---|---|
| <b>Syntax</b>      | <b>&lt;ifXtype&gt;</b> | - | <p>Displays the information on specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> |
| <b>Description</b> | <b>&lt;ifnum&gt;</b>   | - | <p>Displays the information on specified interface identifier. This is a unique value that represents the specific interface.</p> <p>This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.</p> <p>For example: 0/1 represents that the slot number is 0 and port number is 1.</p> <p>Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</p>   |

**Mode** Privilege EXEC Mode

**Package** Workgroup, Enterprise and Metro

**Example**

```

iss# show interfaces priority-grouping counters gigabitethernet
0/1
ETS TLV Counter Information
-----
Port      Configuration TLV   Recommended TLV   TC Supported TLV
          Tx      Rx      Error  Tx      Rx      Error  Tx      Rx      Error
  
```

```
Gi0/1    7    3    0    2    3    0    1    1    0
```

---

**Related  
Commands**

- **shutdown ets** - Shuts down ets subsystem on the switch.
- **ets** - enables/disables the ETS module globally on the subsystem
- **ets trap** - enables sending trap notification messages to the ETS system
- **set priority grouping** - enables /disables row status ETS feature on the port.
- **priority-grouping mode** - configures the admin mode of the ETS module on a port
- **set priority-group willing** - configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.
- **map priority** - maps the priority to the priority group identifier
- **set priority-group recommendation bandwidth** - configures the recommendation bandwidth for the port
- **show interfaces** - displays interfaces specific priority-group information

### 64.3.1.13 show ets global info

This command displays the ets global information.

```
show ets global info
```

**Mode** Privilege Exec Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show ets global info

```
Priority Grouping GLOBAL Info
-----
ETS System control status : Start
ETS Module status : Enabled
```

**Related commands**

- **shutdown ets** - Shuts down ets subsystem on the switch .
- **ets** - enables/disables the ETS module globally on the subsystem
- **ets trap** - enables sending trap notification messages to the ETS system
- **set priority grouping** - enables /disables row status ETS feature on the port.
- **priority-grouping mode** - configures the admin mode of the ETS module on a port
- **set priority-group willing** - configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.
- **map priority** - maps the priority to the priority group identifier
- **set priority-group recommendation bandwidth** - configures the recommendation bandwidth for the port
- **show interfaces** - displays interfaces specific priority-group information

### 64.3.1.14 clear priority-grouping counters

This command clears the ETS TLV counters on the specified port.

```
clear priority-grouping counters [ interface <ifXtype> <ifnum> ]
```

<b>Syntax</b>	<b>&lt;ifXtype&gt;</b>	<ul style="list-style-type: none"> <li>- Clears the counters on specified type of interface. The interface can be: <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> </li> </ul>
<b>Description</b>	<b>&lt;ifnum&gt;</b>	<ul style="list-style-type: none"> <li>- Clears the counters on specified interface identifier. This is a unique value that represents the specific interface.  This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.  For example: 0/1 represents that the slot number is 0 and port number is 1.  Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</li> </ul>
<b>Mode</b>	Privilege Exec Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Example</b>	<pre>iss# clear priority-grouping counters interface gigabitethernet 0/1</pre>	
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• <b>shutdown ets</b> – Shuts down ets subsystem on the switch.</li> <li>• <b>ets</b> – enables/disables the ETS module globally on the subsystem</li> </ul>	

- **ets trap** - enables sending trap notification messages to the ETS system
- **set priority grouping** - enables /disables row status ETS feature on the port.
- **priority-grouping mode** - configures the admin mode of the ETS module on a port
- **set priority-group willing** - configures the willingness status of the local system to accept the ETS configuration recommended by the remote system.
- **map priority** - maps the priority to the priority group identifier
- **set priority-group recommendation bandwidth** - configures the recommendation bandwidth for the port
- **show interfaces** - displays interfaces specific priority-group information

### 64.3.1.15 shutdown pfc

This command shutdown the pfc subsystem .All the resources allocated to the pfc module are released back to system. The no form of the command starts the pfc module in the switch.

**shutdown pfc**

**no shutdown pfc**

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** pfc subsystem is on start

**Example** `iss(config)# shutdown pfc`

**Related  
Commands**

- `pfc` - enables/disables pfc subsystem
- `set pfc threshold limit` - configures the minimum and maximum threshold pfc limit
- `pfc trap` - enables transmission of trap messages for pfc subsystem
- `set priority-flow-control` - enables/disables row status pfc status on the port
- `priority-flow-control mode` - configures the admin mode of the pfc module on a port
- `set priority-flow-control willing` - configures the willingness status of the local system to accept the pfc configuration of the remote system.
- `set priority flow-control` - configures the status of the priority flow control for the prority list
- `dcbx tlv-select pfctlv` - enables the transmission of PFC TLVs
- `show interfaces - priority-flow-control` - displays interface specific priority flow control information
- `show interfaces priority-flow-control counters` - displays the counters for PFC TLVs on the port
- `show priority-flow-control config` - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
- `show pfc global info` - displays the pfc global information
- `clear priority-flow-control counters` - clears the PFC TLV counters on the specified port.

### 64.3.1.16 pfc

This command enables/disables pfc subsystem.

**pfc {enable|disable}**

<b>Syntax Description</b>	<b>enable</b>	- Enables the pfc subsystem. The ports that have pfc enabled on them are enabled in the system hardware. The DCBX state machine is started on the port with the Admin mode as auto..
	<b>disable</b>	- Disables the pfc subsystem. The ports that have pfc enabled are disabled in the system. The DCBX state machine is stopped on the port. The Admin mode is set as on.

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** pfc module is enabled

**Example** iss(config)# pfc enable

- Related Commands**
- **set pfc threshold limit** - configures the minimum and maximum threshold pfc limit
  - **pfc trap** - enables transmission of trap messages for pfc subsystem
  - **set priority-flow-control** - enables/disables row status pfc status on the port
  - **priority-flow-control mode** - configures the admin mode of the pfc module on a port
  - **set priority-flow-control willing** - configures the willingness status of the local system to accept the pfc configuration of the remote system.
  - **set priority flow-control** - configures the status of the priority flow control for the priority list
  - **dcbx tlv-select pfctlv** - enables the transmission of PFC TLVs
  - **show interfaces - priority-flow-control** - displays interface specific priority flow control information
  - **show interfaces priority-flow-control counters** - displays the counters for PFC TLVs on the port
  - **show priority-flow-control config** - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.

- **show pfc global info** - displays the pfc global information
- **clear priority-flow-control counters** - clears the PFC TLV counters on the specified port.

### 64.3.1.17 set pfc threshold limit

This command configures the minimum and maximum threshold pfc limit. The minimum and maximum receive queue buffer count is configured. The minimum and maximum values for receive queue buffer count may vary based on the underlying hardware's capacity.

```
set pfc threshold limit min <integer(1-65535)> max <integer(1-65535)>
```

<b>Syntax Description</b>	<b>minimum</b>	-	Configures the minimum limit for pfc. Minimum priority based flow control threshold for the switch. This indicates the minimum receive queue buffer count. This value ranges between 1 and 65535.
	<b>maximum</b>	-	Configures the maximum limit for pfc. Maximum priority based flow control threshold for the switch. This indicates the maximum receive queue buffer count. This value ranges between 1 and 65535.

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults**

minimum	-	1
maximum	-	65535

**Example** `iss(config)# set pfc threshold limit min 500 max 800`

- Related Commands**
- `pfc` - enables/disables pfc subsystem
  - `pfc trap` - enables transmission of trap messages for pfc subsystem
  - `set priority-flow-control` - enables/disables row status pfc status on the port
  - `priority-flow-control mode` - configures the admin mode of the pfc module on a port
  - `set priority-flow-control willing` - configures the willingness status of the local system to accept the pfc configuration of the remote system.
  - `set priority flow-control` - configures the status of the priority flow control for the priority list
  - `dcbx tlv-select pfctlv` - enables the transmission of PFC TLVs
  - `show interfaces - priority-flow-control` - displays interface specific priority flow control information
  - `show interfaces priority-flow-control counters` - displays the

counters for PFC TLVs on the port

- **show priority-flow-control config** - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
- **show pfc global info** - displays the pfc global information
- **clear priority-flow-control counters** - clears the PFC TLV counters on the specified port.

### 64.3.1.18 pfc trap

This command enables transmission of trap messages for pfc subsystem. The no form of the command disables the transmission of pfc trap notification messages.

```
pfc trap {all | [module-status-change] [admin-mode-change] [peer-status-change] [sem-change]}
```

```
no pfc trap {all | [module-status-change] [admin-mode-change] [peer-status-change] [sem-change]}
```

<b>Syntax Description</b>	<b>all</b>	-	Configures all trap messages
<b>n</b>	<b>module-status-change</b>	-	Configures the module status as enable/disable
	<b>admin-mode-change</b>	-	Configures the admin status for each port.
	<b>peer-status-change</b>	-	Configures the peer status as up/down
	<b>sem-change</b>	-	Configures the status of DCBX state machine

**Mode** Global Configuration mode

**Package** Workgroup, Enterprise and Metro

**Defaults** module-status-change and admin-mode-change

**Example** iss(config)# pfc trap all

- Related Commands**
- **pfc** - enables/disables pfc subsystem
  - **set pfc threshold limit** - configures the minimum and maximum threshold pfc limit
  - **set priority-flow-control** - enables/disables row status pfc status on the port
  - **priority-flow-control mode** - configures the admin mode of the pfc module on a port
  - **set priority-flow-control willing** - configures the willingness status of the local system to accept the pfc configuration of the remote system.
  - **set priority flow-control** - configures the status of the priority flow control for the priority list
  - **dcbx tlv-select pfctlv** - enables the transmission of PFC TLVs

- **show interfaces - priority-flow-control** - displays interface specific priority flow control information
- **show interfaces priority-flow-control counters** - displays the counters for PFC TLVs on the port
- **show priority-flow-control config** - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
- **show pfc global info** - displays the pfc global information
- **clear priority-flow-control counters** - clears the PFC TLV counters on the specified port.

### 64.3.1.19 set priority-flow-control

This command enables/disables row status pfc status on the port.

```
set priority-flow-control {enable | disable}
```

<b>Syntax Description</b>	<b>enable</b>	-	Configures the row status of a port. New entries are created for physical and port channel interfaces.
	<b>disable</b>	-	Disables the configuration for the port. Entries are deleted on physical and port channel interfaces..

**Mode** Interface Configuration mode

**Package** Workgroup, Enterprise and Metro

**Defaults** disabled

**Example** `iss(config-if)# set priority-flow-control enable`

- Related commands**
- `pfc` - enables/disables pfc subsystem
  - `set pfc threshold limit` - configures the minimum and maximum threshold pfc limit
  - `pfc trap` - enables transmission of trap messages for pfc subsystem
  - `priority-flow-control mode` - configures the admin mode of the pfc module on a port
  - `set priority-flow-control willing` - configures the willingness status of the local system to accept the pfc configuration of the remote system.
  - `set priority flow-control` - configures the status of the priority flow control for the priority list
  - `dcbx tlv-select pfctlv` - enables the transmission of PFC TLVs
  - `show interfaces - priority-flow-control` - displays interface specific priority flow control information
  - `show interfaces priority-flow-control counters` - displays the counters for PFC TLVs on the port
  - `show priority-flow-control config` - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
  - `show pfc global info` - displays the pfc global information
  - `clear priority-flow-control counters` - clears the PFC TLV counters on the specified port.

### 64.3.1.20 priority-flow-control mode

This command configures the admin mode of the pfc module on a port. The no form of the command disables the pfc feature on a port.

```
priority-flow-control mode {auto|on}
```

```
no priority-flow-control mode
```

<b>Syntax Description</b>	<b>auto</b>	-	Configures the admin mode as auto. If the pfc feature is enabled on this port, all the parameters for the pfc module is determined by the DCBX state machine.
---------------------------	-------------	---	---

	<b>on</b>	-	Configures the admin mode as on. If the pfc feature is enabled on this port, all the parameters for the pfc module is not determined by the DCBX state machine.
--	-----------	---	---

<b>Mode</b>	Interface Configuration Mode.
-------------	-------------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Defaults</b>	By default the admin mode is off.
-----------------	-----------------------------------

<b>Example</b>	<code>iss(config-if)# priority-flow-control mode auto</code>
----------------	--

<b>Related commands</b>	<ul style="list-style-type: none"> <li>• <code>no shutdown ets</code> – starts the ETS module in the switch</li> <li>• <code>pfc</code> – enables/disables pfc subsystem</li> <li>• <code>set pfc threshold limit</code> – configures the minimum and maximum threshold pfc limit</li> <li>• <code>pfc trap</code> – enables transmission of trap messages for pfc subsystem</li> <li>• <code>set priority-flow-control</code> – enables/disables row status pfc status on the port</li> <li>• <code>set priority-flow-control willing</code> – configures the willingness status of the local system to accept the pfc configuration of the remote system.</li> <li>• <code>set priority flow-control</code> – configures the status of the priority flow control for the priority list</li> <li>• <code>dcbx tlv-select pfctlv</code> – enables the transmission of PFC TLVs</li> <li>• <code>show interfaces - priority-flow-control</code> – displays interface specific priority flow control information</li> <li>• <code>show interfaces priority-flow-control counters</code> – displays the counters for PFC TLVs on the port</li> </ul>
-------------------------	---

- **show priority-flow-control config** - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
- **show pfc global info** - displays the pfc global information
- **clear priority-flow-control counters** - clears the PFC TLV counters on the specified port.

### 64.3.1.21 set priority-flow-control willing

This command configures the willingness status of the local system to accept the pfc configuration of the remote system.

```
set priority-flow-control willing {enable | disable}
```

<b>Syntax Description</b>	<b>enable</b>	- Enables the acceptance state of the pfc.
	<b>disable</b>	- Disables the acceptance state of the pfc.

**Mode** Interface Configuration mode

**Package** Workgroup, Enterprise and Metro

**Defaults** disabled

**Example** `iss(config-if)# set priority-flow-control willing enable`

- Related commands**
- `pfc` - enables/disables pfc subsystem
  - `set pfc threshold limit` - configures the minimum and maximum threshold pfc limit
  - `pfc trap` - enables transmission of trap messages for pfc subsystem
  - `set priority-flow-control` - enables/disables row status pfc status on the port
  - `priority-flow-control mode` - configures the admin mode of the pfc module on a port
  - `set priority flow-control` - configures the status of the priority flow control for the priority list
  - `dcbx tlv-select pfctlv` - enables the transmission of PFC TLVs
  - `show interfaces - priority-flow-control` - displays interface specific priority flow control information
  - `show interfaces priority-flow-control counters` - displays the counters for PFC TLVs on the port
  - `show priority-flow-control config` - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
  - `show pfc global info` - displays the pfc global information
  - `clear priority-flow-control counters` - clears the PFC TLV counters on the specified port.

### 64.3.1.22 set priority flow-control

This command configures the status of the priority flow control for the priority list.

```
set priority <priority-list> flow-control {enable|disable}
```

<b>Syntax Description</b>	<p><b>&lt;priority-list&gt;</b> - Configures the priority-list.</p> <p><b>enable</b> - Enables the priority flow control for the priority list.</p> <p><b>disable</b> - Disables the priority flow control for the priority list.</p>
<b>Mode</b>	Interface Configuration mode
<b>Package</b>	Workgroup, Enterprise and Metro
<b>Example</b>	iss(config-if)# set priority dummy flow-control enable
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• <b>pf</b> - enables/disables pfc subsystem</li> <li>• <b>set pfc threshold limit</b> - configures the minimum and maximum threshold pfc limit</li> <li>• <b>pf trap</b> - enables transmission of trap messages for pfc subsystem</li> <li>• <b>set priority-flow-control</b> - enables/disables row status pfc status on the port</li> <li>• <b>priority-flow-control mode</b> - configures the admin mode of the pfc module on a port</li> <li>• <b>set priority-flow-control willing</b> - configures the willingness status of the local system to accept the pfc configuration of the remote system.</li> <li>• <b>dcx tlv-select pfctlv</b> - enables the transmission of PFC TLVs</li> <li>• <b>show interfaces - priority-flow-control</b> - displays interface specific priority flow control information</li> <li>• <b>show interfaces priority-flow-control counters</b> - displays the counters for PFC TLVs on the port</li> <li>• <b>show priority-flow-control config</b> - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.</li> <li>• <b>show pfc global info</b> - displays the pfc global information</li> <li>• <b>clear priority-flow-control counters</b> - clears the PFC TLV counters on the specified port.</li> </ul>

### 64.3.1.23 dcbx tlv-select pfctlv

This command enables the transmission of PFC TLVs. The no form of the command disables the transmission of PFC TLVs.

```
dcbx tlv-select pfctlv
```

```
no dcbx tlv-select pfctlv
```

**Mode** Interface Configuration mode

**Package** Workgroup, Enterprise and Metro

**Defaults** The transmission of PFC TLVs is disabled

**Example** `iss(config-if)# dcbx tlv-select pfctlv`

- Related commands**
- `pfctlv` - enables/disables pfctlv subsystem
  - `set pfctlv threshold limit` - configures the minimum and maximum threshold pfctlv limit
  - `pfctlv trap` - enables transmission of trap messages for pfctlv subsystem
  - `set pfctlv priority-flow-control` - enables/disables row status pfctlv status on the port
  - `pfctlv priority-flow-control mode` - configures the admin mode of the pfctlv module on a port
  - `set pfctlv priority-flow-control willing` - configures the willingness status of the local system to accept the pfctlv configuration of the remote system.
  - `set pfctlv priority flow-control` - configures the status of the priority flow control for the priority list
  - `show interfaces - pfctlv priority-flow-control` - displays interface specific priority flow control information
  - `show interfaces pfctlv priority-flow-control counters` - displays the counters for PFC TLVs on the port
  - `show pfctlv priority-flow-control config` - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
  - `show pfctlv global info` - displays the pfctlv global information
  - `clear pfctlv priority-flow-control counters` - clears the PFC TLV counters on the specified port.

### 64.3.1.24 show interfaces - priority-flow-control

This command displays interface specific priority flow control information.

```
show interfaces [<ifXtype> <ifnum> ] priority-flow-control [detail]
```

<b>Syntax Description</b>	<b>&lt;ifXtype&gt;</b>	<ul style="list-style-type: none"> <li>- Displays the information on specified type of interface. The interface can be:           <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> </li> </ul>
	<b>&lt;ifnum&gt;</b>	<ul style="list-style-type: none"> <li>- Displays the information on specified interface identifier. This is a unique value that represents the specific interface.            This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.            For example: 0/1 represents that the slot number is 0 and port number is 1.            Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</li> </ul>
	<b>detail</b>	<ul style="list-style-type: none"> <li>- Displays the information regarding the admin port, local port and remote port table.</li> </ul>
<b>Mode</b>	Privilege Exec Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Example</b>	<pre>iss# show inter priority-flow-control detail</pre>	

```

-----
PFC Port Gi0/3      Information
-----
PFC  Local Port Info
-----
PFC Willing Status      :Disabled
PFC MBC                 :Disabled
PFC Capability          :0

Priority Enabled List   :
Priority Disabled List  :0 1 2 3 4 5 6 7
-----

PFC Admin Port Info
-----
PFC Willing Status      :Disabled
PFC MBC                 :Disabled
PFC Capability          :0

Priority Enabled List   :
Priority Disabled List  :0 1 2 3 4 5 6 7
-----

PFC Remote Port Info
-----
No Remote Entry is Present
-----

PFC Port Related Info
-----
PFC TLV Tx Status      :Disabled

PFC Port Mode          :OFF MODE
PFC Oper State         :OFF STATE

```

**Related Commands**

- **pfc** - enables/disables pfc subsystem
- **set pfc threshold limit** - configures the minimum and maximum threshold pfc limit
- **pfc trap** - enables transmission of trap messages for pfc subsystem
- **set priority-flow-control** - enables/disables row status pfc status on the port
- **priority-flow-control mode** - configures the admin mode of the pfc module on a port
- **set priority-flow-control willing** - configures the willingness status of the local system to accept the pfc configuration of the remote system.
- **set priority flow-control** - configures the status of the priority flow control for the priority list
- **dcbx tlv-select pfctlv** - enables the transmission of PFC TLVs
- **show interfaces priority-flow-control counters** - displays the counters for PFC TLVs on the port
- **show priority-flow-control config** - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.

- `show pfc global info` - displays the pfc global information
- `clear priority-flow-control counters` - clears the PFC TLV counters on the specified port.

### 64.3.1.25 show interfaces priority-flow-control counters

This command displays the counters for PFC TLVs on the port.

```
show interfaces priority-flow-control counters [ <ifXtype> <ifnum> ]
```

<b>Syntax</b>	<b>&lt;ifXtype&gt;</b>	<ul style="list-style-type: none"> <li>- Displays the information on specified type of interface. The interface can be:           <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> </li> </ul>
<b>Description</b>	<b>&lt;ifnum&gt;</b>	<ul style="list-style-type: none"> <li>- Displays the information on specified interface identifier. This is a unique value that represents the specific interface.            This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.            For example: 0/1 represents that the slot number is 0 and port number is 1.            Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</li> </ul>
<b>Mode</b>	Privilege Exec Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Example</b>	<pre>iss# show interfaces priority-flow-control counters gigabitethernet 0/1</pre> <p style="text-align: center;"><a href="#">PFC TLV Counter Information</a></p> <hr style="border-top: 1px dashed #000;"/>	

---

Port	TLV transmitted	TLV Received	TLV Errors
Gi0/1	1	1	0

---

**Related  
Commands**

- **pfc** - enables/disables pfc subsystem
- **set pfc threshold limit** - configures the minimum and maximum threshold pfc limit
- **pfc trap** - enables transmission of trap messages for pfc subsystem
- **set priority-flow-control** - enables/disables row status pfc status on the port
- **priority-flow-control mode** - configures the admin mode of the pfc module on a port
- **set priority-flow-control willing** - configures the willingness status of the local system to accept the pfc configuration of the remote system.
- **set priority flow-control** - configures the status of the priority flow control for the priority list
- **dcbx tlv-select pfctlv** - enables the transmission of PFC TLVs
- **show interfaces - priority-flow-control** - displays interface specific priority flow control information
- **show priority-flow-control config** - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
- **show pfc global info** - displays the pfc global information
- **clear priority-flow-control counters** - clears the PFC TLV counters on the specified port.

### 64.3.1.26 show priority-flow-control config

This command displays the minimum and maximum threshold of the switch and the number of profiles of the switch.

```
show priority-flow-control config
```

**Mode** Privilege Exec Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show priority-flow-control config

```
Priority Flow Control GLOBAL Info
```

```
-----  
PFC Minimum ThreShold Value is:1  
PFC Maximum ThreShold Value is:65535  
PFC Maximum Profile Supported by the system is:0
```

**Related  
Commands**

- **pfcc** - enables/disables pfc subsystem
- **set pfc threshold limit** - configures the minimum and maximum threshold pfc limit
- **pfcc trap** - enables transmission of trap messages for pfc subsystem
- **set priority-flow-control** - enables/disables row status pfc status on the port
- **priority-flow-control mode** - configures the admin mode of the pfc module on a port
- **set priority-flow-control willing** - configures the willingness status of the local system to accept the pfc configuration of the remote system.
- **set priority flow-control** - configures the status of the priority flow control for the prority list
- **dcbbx tlv-select pfctlv** - enables the transmission of PFC TLVs
- **show interfaces - priority-flow-control** - displays interface specific priority flow control information
- **show interfaces priority-flow-control counters** - displays the counters for PFC TLVs on the port
- **show pfc global info** - displays the pfc global information
- **clear priority-flow-control counters** - clears the PFC TLV counters on the specified port.

### 64.3.1.27 show pfc global info

This command displays the pfc global information.

```
show pfc global info
```

**Mode** Privilege Exec Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show pfc global info

```
Priority Flow Control GLOBAL Info
-----
PFC System control status : Start
PFC Module status : Enabled
```

**Related Command**

- **pfc** - enables/disables pfc subsystem
- **set pfc threshold limit** - configures the minimum and maximum threshold pfc limit
- **pfc trap** - enables transmission of trap messages for pfc subsystem
- **set priority-flow-control** - enables/disables row status pfc status on the port
- **priority-flow-control mode** - configures the admin mode of the pfc module on a port
- **set priority-flow-control willing** - configures the willingness status of the local system to accept the pfc configuration of the remote system.
- **set priority flow-control** - configures the status of the priority flow control for the prority list
- **dcbx tlv-select pfctlv** - enables the transmission of PFC TLVs
- **show interfaces - priority-flow-control** - displays interface specific priority flow control information
- **show interfaces priority-flow-control counters** - displays the counters for PFC TLVs on the port
- **show priority-flow-control config** - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
- **clear priority-flow-control counters** - clears the PFC TLV counters on the specified port.

### 64.3.1.28 clear priority-flow-control counters

This command clears the PFC TLV counters on the specified port.

```
clear priority-flow-control counters [ interface <ifXtype> <ifnum> ]
```

<b>Syntax Description</b>	<b>&lt;ifXtype&gt;</b>	<ul style="list-style-type: none"> <li>- Displays the information on specified type of interface. The interface can be: <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> </li> </ul>
	<b>&lt;ifnum&gt;</b>	<ul style="list-style-type: none"> <li>- Displays the information on specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</li> </ul>
<b>Mode</b>	Privilege Exec Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Example</b>	<pre>iss# clear priority-flow-control counters gigabitethernet 0/1</pre>	
<b>Related commands</b>	<ul style="list-style-type: none"> <li>• <code>pfc</code> – enables/disables pfc subsystem</li> <li>• <code>set pfc threshold limit</code> – configures the minimum and maximum</li> </ul>	

threshold pfc limit

- **pfc trap** - enables transmission of trap messages for pfc subsystem
- **set priority-flow-control** - enables/disables row status pfc status on the port
- **priority-flow-control mode** - configures the admin mode of the pfc module on a port
- **set priority-flow-control willing** - configures the willingness status of the local system to accept the pfc configuration of the remote system.
- **set priority flow-control** - configures the status of the priority flow control for the prority list
- **dcbx tlv-select pfctlv** - enables the transmission of PFC TLVs
- **show interfaces - priority-flow-control** - displays interface specific priority flow control information
- **show interfaces priority-flow-control counters** - displays the counters for PFC TLVs on the port
- **show priority-flow-control config** - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
- **show pfc global info** - displays the pfc global information
- **clear priority-flow-control counters** - clears the PFC TLV counters on the specified port.

### 64.3.1.29 set dcbx

This command configures the dcbx status on the port. .

```
set dcbx {enable | disable}
```

<b>Syntax Description</b>	<b>enable</b>	- Enables dcbx related features.
	<b>disable</b>	- Disables dcbx related features..

**Mode** Interface Configuration mode

**Package** Workgroup, Enterprise and Metro

**Defaults** Data center bridging is disabled on all the interfaces.

**Example** `iss(config-if)# set dcbx enable`



The ets and pfc modules can be configured only if dcbx module is enabled.

#### Related Commands

- **pfc** - enables/disables pfc subsystem
- **set pfc threshold limit** - configures the minimum and maximum threshold pfc limit
- **pfc trap** - enables transmission of trap messages for pfc subsystem
- **set priority-flow-control** - enables/disables row status pfc status on the port
- **priority-flow-control mode** - configures the admin mode of the pfc module on a port
- **set priority-flow-control willing** - configures the willingness status of the local system to accept the pfc configuration of the remote system.
- **set priority flow-control** - configures the status of the priority flow control for the priority list
- **dcbx tlv-select pfctlv** - enables the transmission of PFC TLVs
- **show interfaces - priority-flow-control** - displays interface specific priority flow control information
- **show interfaces priority-flow-control counters** - displays the counters for PFC TLVs on the port
- **show priority-flow-control config** - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
- **show pfc global info** - displays the pfc global information

- **clear priority-flow-control counters** – clears the PFC TLV counters on the specified port.
- **show dcbx ports** – displays dcbx port admin status
- **debug dcbx** – generates dcbx related trace messages

### 64.3.1.30 show dcbx ports

This command displays dcbx port admin status.

**show dcbx ports**

**Mode** Privilege Exec Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show dcbx ports

```
Port      Admin Status
-----
Gi0/2    Enabled
Gi0/3    Enabled
-----
```

#### Related Commands

- **pfc** - enables/disables pfc subsystem
- **set pfc threshold limit** - configures the minimum and maximum threshold pfc limit
- **pfc trap** - enables transmission of trap messages for pfc subsystem
- **set priority-flow-control** - enables/disables row status pfc status on the port
- **priority-flow-control mode** - configures the admin mode of the pfc module on a port
- **set priority-flow-control willing** - configures the willingness status of the local system to accept the pfc configuration of the remote system.
- **set priority flow-control** - configures the status of the priority flow control for the priority list
- **dcbx tlv-select pfctlv** - enables the transmission of PFC TLVs
- **show interfaces - priority-flow-control** - displays interface specific priority flow control information
- **show interfaces priority-flow-control counters** - displays the counters for PFC TLVs on the port
- **show priority-flow-control config** - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
- **show pfc global info** - displays the pfc global information
- **clear priority-flow-control counters** - clears the PFC TLV counters on the specified port.
- **debug dcbx** - generates dcbx related trace messages

### 64.3.1.31 debug dcbx

This command generates dcbx related trace messages.

```
debug dcbx {all | [mgmt] [sem] [tlv] [resource] [fail] [control-plane]}
```

```
no debug dcbx {all | [mgmt] [sem] [tlv] [resource] [fail] [control-plane]}
```

<b>Syntax Description</b>	<b>all</b>	- Generates trace messages for all types of traces.
	<b>mgmt</b>	- Generates debug statements for management plane functionality traces.
	<b>sem</b>	- Generates debug statements for state machine handling traces. This trace is generated when there is an error condition in State Machine
	<b>tlv</b>	- Generates tlv related trace messages
	<b>ctrl</b>	- Generates Control plane traces. These traces are used for cases such as MBSM card removal, failure of state change and so on.
	<b>resource</b>	- Traces related to all resources such as memory, data structure and the like. These traces are used for failure of memory allocation and so on.
	<b>fail</b>	- All failure traces. These traces are used for all valid and invalid failures. The valid failures represent the expected error. The invalid failures represent the unexpected error.

**Mode** Privileged Exec Mode / User Exec Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** fail.

**Example** iss# debug dcbx all

- Related Command**
- **pfc** - enables/disables pfc subsystem
  - **set pfc threshold limit** - configures the minimum and maximum threshold

- s** pfc limit
- **pfc trap** - enables transmission of trap messages for pfc subsystem
  - **set priority-flow-control** - enables/disables row status pfc status on the port
  - **priority-flow-control mode** - configures the admin mode of the pfc module on a port
  - **set priority-flow-control willing** - configures the willingness status of the local system to accept the pfc configuration of the remote system.
  - **set priority flow-control** - configures the status of the priority flow control for the priority list
  - **dcbx tlv-select pfctlv** - enables the transmission of PFC TLVs
  - **show interfaces - priority-flow-control** - displays interface specific priority flow control information
  - **show interfaces priority-flow-control counters** - displays the counters for PFC TLVs on the port
  - **show priority-flow-control config** - displays the minimum and maximum threshold of the switch and the number of profiles of the switch.
  - **show pfc global info** - displays the pfc global information
  - **clear priority-flow-control counters** - clears the PFC TLV counters on the specified port.
  - **show dcbx ports** - displays dcbx port admin status
  - **show debugging** - displays the traces enabled for the dcbx module.

## 64.3.2 CN

Congestion Notification (CN) provides end-to-end congestion management for protocols that do not already have congestion control mechanisms built-in. It is also expected to support protocols such as TCP that has native congestion management that reacts to congestion marginally.



The list of CLI commands for the configuration of CN are common to both SI and MI except for a difference in the prompt that appears for the switch with MI support.

The prompt for the global configuration mode is,

```
iss(config-switch)# set cn enable
```

The list of commands that for the configuration of CN is as follow:

- set cn
- set cn cnm-transmit-priority
- cn cnpv
- cn cnpv defense
- cn cnpv - alternate-priority
- cn cnpv - defense-mode
- cn cnpv - port-default-defense
- cn cnpv - lldp-instance-choice
- cn cnpv - lldp-instance-selector
- shutdown cn
- cn trap
- cn cnpv - defense
- cn cnpv - defense-mode
- cn cnpv - lldp-instance-choice
- cn cnpv - lldp-instance-selector
- cn cnpv - alternate-priority
- cn cp-properties
- debug cn
- clear cn counters
- show cn global information
- show cn interface counters
- show cn cnpv
- show cn cp-properties

## 64.3.2.1 set cn

This command enables/disables congestion notification on all the ports in a switch.

```
set cn {enable | disable}
```

<b>Syntax Description</b>	<b>enable</b>	- Enables CN module on all the ports. When enabled the necessary resources are allocated to the module..
	<b>disable</b>	- Disables CN module on all the ports. All the resources are released to the system. .

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** disable

**Example** `iss(config)# set cn enable`

**Related commands**

- **shutdown cn** - This command starts the cn module in the switch.
- **set cn cnm-transmit-priority** - This command sets the VLAN priority to be used in all the CNM packets generated by the switch. This value ranges between 0-7. .
- **cn cnpv** - This command creates a congestion notification priority value in the switch. The no form of the command deletes cnpv from the switch.
- **cn cnpv defense** - This command configures whether the default CND defense mode of a CNPV in all ports of a switch is determined by configured values or through LLDP.
- **cn cnpv - alternate-priority** - This command sets the default regenerated priority for incoming frames with a CNPV in all the ports of the switch.
- **cn cnpv - defense-mode** - This command sets the default CND defense-mode for a CNPV in all ports of a switch
- **cn cnpv - port-default-defense** - This command sets the default value for the defense-mode choice for all the ports of the switch
- **cn cnpv - lldp-instance-choice** - This command configures the CN TLV to carry a CNPV in all ports of the switch
- **cn cnpv - lldp-instance-selector** - This command configures the index to LLDP destination MAC address entry to be used in LLDP PDUs for a CNPV in all ports of the switch
- **show cn global information** - This command displays the CN global details of the switch

### 64.3.2.2 set cn cnm-transmit-priority

This command sets the VLAN priority to be used in all the CNM packets generated by the switch. This value ranges between 0-7.

```
set cn cnm-transmit-priority <priority-value (0-7)>
```

<b>Syntax description</b>	<priority-value (0-7)	- Configures the priority value for the congestion notification cnm transmit priority. This value ranges between 0 and 7.
<b>Mode</b>	Global Configuration Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Defaults</b>	6	
<b>Example</b>	iss(config)# set cn cnm-transmit-priority 5	
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• <b>set cn</b> - This command enables/disables congestion notification on all the ports on a switch.</li> <li>• <b>shutdown cn</b> - This command shutsdown the cn module in the switch.</li> <li>• <b>cn cnpv</b> - This command creates a congestion notification priority value in the switch. The no form of the command deletes cnpv from the switch.</li> <li>• <b>cn cnpv defense</b> - This command configures whether the default CND defense mode of a CNPV in all ports of a switch is determined by configured values or through LLDP.</li> <li>• <b>cn cnpv - alternate-priority</b> - This command sets the default regenerated priority for incoming frames with a CNPV in all the ports of the switch.</li> <li>• <b>cn cnpv - defense-mode</b> - This command sets the default CND defense-mode for a CNPV in all ports of a switch</li> <li>• <b>cn cnpv - port-default-defense</b> - This command sets the default value for the defense-mode choice for all the ports of the switch</li> <li>• <b>cn cnpv - lldp-instance-choice</b> - This command configures the CN TLV to carry a CNPV in all ports of the switch</li> <li>• <b>cn cnpv - lldp-instance-selector</b> - This command configures the index to LLDP destination MAC address entry to be used in LLDP PDUs for a CNPV in all ports of the switch</li> </ul>	

### 64.3.2.3 cn cnpv

This command creates a congestion notification priority value in the switch. The no form of the command deletes cnpv from the switch.

```
cn cnpv <priority-value (0-7)>
```

```
no cn cnpv <priority-value (0-7)>
```

<b>Syntax description</b>	<b>&lt;priority-value (0-7)</b>	-	Configures the priority value for the congestion notification cnpv. This value ranges between 0 and 7.
---------------------------	---------------------------------	---	--

<b>Mode</b>	Global Configuration Mode
-------------	---------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Example</b>	<code>iss(config)# cn cnpv 5</code>
----------------	-------------------------------------

- |                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <ul style="list-style-type: none"> <li>• <b>set cn</b> - This command enables/disables congestion notification on all the ports on a switch.</li> <li>• <b>shutdown cn</b> - This command shutdowns the cn module in the switch.</li> <li>• <b>set cn cnm-transmit-priority</b> - This command sets the VLAN priority to be used in all the CNM packets generated by the switch. This value ranges between 0-7.</li> <li>• <b>cn cnpv defense</b> - This command configures whether the default CND defense mode of a CNPV in all ports of a switch is determined by configured values or through LLDP.</li> <li>• <b>cn cnpv - alternate-priority</b> - This command sets the default regenerated priority for incoming frames with a CNPV in all the ports of the switch.</li> <li>• <b>cn cnpv - defense-mode</b> - This command sets the default CND defense-mode for a CNPV in all ports of a switch</li> <li>• <b>cn cnpv - port-default-defense</b> - This command sets the default value for the defense-mode choice for all the ports of the switch</li> <li>• <b>cn cnpv - lldp-instance-choice</b> - This command configures the CN TLV to carry a CNPV in all ports of the switch</li> <li>• <b>cn cnpv - lldp-instance-selector</b> - This command configures the index to LLDP destination MAC address entry to be used in LLDP PDUs for a CNPV in all ports of the switch</li> </ul> |
|-------------------------|---|

### 64.3.2.4 cn cnpv defense

This command configures whether the default CND defense mode of a CNPV in all ports of a switch is determined by configured values or through LLDP.

```
cn cnpv <priority-value(0-7)> defense { auto | on }
```

<b>Syntax Description</b>	<b>&lt;priority-value(0-7)&gt;</b>	- Configures the priority-value for the congestion notification priority value. This value ranges between 0 and 7.
	<b>auto</b>	- Configures the default CND defense mode as auto. The defense mode is derived through LLDP exchanges.
	<b>on</b>	- Configures the default CND defense mode as on. The administrator configuration determines the defense mode.

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** auto

**Example** iss(config)# cn cnpv 4 defense on

**Related Commands**

- **set cn** - This command enables/disables congestion notification on all the ports on a switch
- **shutdown cn** - This command starts the cn module in the switch.
- **set cn cnm-transmit-priority** - This command sets the VLAN priority to be used in all the CNM packets generated by the switch. This value ranges between 0-7.
- **cn cnpv** - This command creates a congestion notification priority value in the switch. The no form of the command deletes cnpv from the switch.
- **cn cnpv - alternate-priority** - This command sets the default regenerated priority for incoming frames with a CNPV in all the ports of the switch.
- **cn cnpv - defense-mode** - This command sets the default CND defense-mode for a CNPV in all ports of a switch
- **cn cnpv - port-default-defense** - This command sets the default value for the defense-mode choice for all the ports of the switch
- **cn cnpv - lldp-instance-choice** - This command configures the CN TLV to carry a CNPV in all ports of the switch
- **cn cnpv - lldp-instance-selector** - This command configures the index to LLDP destination MAC address entry to be used in LLDP PDUs for a

CNPV in all ports of the switch

### 64.3.2.5 cn cnpv - alternate-priority

This command sets the default regenerated priority for incoming frames with a CNPV in all the ports of the switch.

```
cn cnpv <priority-value (0-7)> alternate-priority <priority-value (0-7)>
```

<b>Syntax description</b>	<b>&lt;priority-value (0-7)&gt;</b>	-	Configures the priority-value for the congestion notification priority value. This value ranges between 0 and 7
	<b>alternate-priority &lt;priority-value (0-7)&gt;</b>	-	Configures the priority value to which an incoming frame is to be mapped. This value ranges between 0 and 7

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config)# cn cnpv 5 alternate-priority 5`

**Related Commands**

- **set cn** - This command enables/disables congestion notification on all the ports on a switch.
- **shutdown cn** - This command starts the cn module in the switch.
- **set cn cnm-transmit-priority** - This command sets the VLAN priority to be used in all the CNM packets generated by the switch. This value ranges between 0-7.
- **cn cnpv** - This command creates a congestion notification priority value in the switch. The no form of the command deletes cnpv from the switch.
- **cn cnpv defense** - This command configures whether the default CND defense mode of a CNPV in all ports of a switch is determined by configured values or through LLDP.
- **cn cnpv - defense-mode** - This command sets the default CND defense-mode for a CNPV in all ports of a switch
- **cn cnpv - port-default-defense** - This command sets the default value for the defense-mode choice for all the ports of the switch
- **cn cnpv - lldp-instance-choice** - This command configures the CN TLV to carry a CNPV in all ports of the switch
- **cn cnpv - lldp-instance-selector** - This command configures the index to LLDP destination MAC address entry to be used in LLDP PDUs for a CNPV in all ports of the switch

### 64.3.2.6 cn cnpv - defense-mode

This command sets the default CND defense-mode for a CNPV in all ports of a switch.

```
cn cnpv <priority-value(0-7)> defense-mode { disabled | edge | interior | interiorReady }
```

<b>Syntax Description</b>	<b>&lt;priority-value(0-7)&gt;</b>	-	Configures the priority-value for the congestion notification priority value. This value ranges between 0 and 7)
	<b>disabled</b>	-	Configures the CN capability as administratively disabled. The priority regeneration table controls the re-mapping of input frames for the priority. End station does not add the CN-tags and the bridge does not strip the CN-tags
	<b>edge</b>	-	Re-maps the priority parameters of input frames to an alternate (non-CNPV) value, in spite of the priority regeneration table for the CNPV. End station does not add CN-tags, but the bridge removes the CN-tags from frames before transmitting the frames.
	<b>interior</b>	-	Does not re-map the priority parameters of input frames for the CNPV. End station does not add CN-tags, but the bridge removes the CN-tags from frames before transmitting the frames.
	<b>interiorReady</b>	-	Does not re-map the priority parameters of input frames for the CNPV. End station adds CN-tags, but the bridge does not remove the CN-tags from frames before transmitting the frames.

**Mode** Global Configuration mode

**Package** Workgroup, Enterprise and Metro

**Defaults** interior

**Example**

```
iss(config)# cn cnpv 2 defense-mode edge
```

- Related Commands**
- **set cn** - This command enables/disables congestion notification on all the ports on a switch.
  - **shutdown cn** - This command starts the cn module in the switch.
  - **cn cnpv** - This command creates a congestion notification priority value in the switch. The no form of the command deletes cnpv from the switch.

- **cn cnpv defense** - This command configures whether the default CND defense mode of a CNPV in all ports of a switch is determined by configured values or through LLDP.
- **cn cnpv - alternate-priority** - This command sets the default regenerated priority for incoming frames with a CNPV in all the ports of the switch.
- **cn cnpv - port-default-defense** - This command sets the default value for the defense-mode choice for all the ports of the switch
- **cn cnpv - lldp-instance-choice** - This command configures the CN TLV to carry a CNPV in all ports of the switch
- **cn cnpv - lldp-instance-selector** - This command configures the index to LLDP destination MAC address entry to be used in LLDP PDUs for a CNPV in all ports of the switch

### 64.3.2.7 cn cnpv - port-default-defense

This command sets the default value for the defense-mode choice for all the ports of the switch.

```
cn cnpv <priority-value (0-7)> port-default-defense { auto-enable | auto-disable }
```

<b>Syntax Description</b>	<b>&lt;priority-value (0-7)&gt;</b>	-	Configures the priority-value for the congestion notification priority value. This value ranges between 0 and 7)
	<b>auto-enabled</b>	-	Configures the default defense mode as auto for the newly created objects. LLDP determines the defense mode of the port
	<b>auto-disable</b>	-	Configures the default defense mode as Admin for newly created objects. Administrator configured values determine the defense of the port.

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** auto-enabled

**Example**

```
iss(config)# cn cnpv 7 port-default-defense auto-enable
```

#### Related Commands

- **set cn** - This command enables/disables congestion notification on all the ports on a switch.
- **shutdown cn** - This command starts the cn module in the switch.
- **set cn cnm-transmit-priority** - This command sets the VLAN priority to be used in all the CNM packets generated by the switch. This value ranges between 0-7.
- **cn cnpv** - This command creates a congestion notification priority value in the switch. The no form of the command deletes cnpv from the switch.
- **cn cnpv defense** - This command configures whether the default CND defense mode of a CNPV in all ports of a switch is determined by configured values or through LLDP.
- **cn cnpv - alternate-priority** - This command sets the default regenerated priority for incoming frames with a CNPV in all the ports of the switch.
- **cn cnpv - defense-mode** - This command sets the default CND defense-mode for a CNPV in all ports of a switch
- **cn cnpv - lldp-instance-choice** - This command configures the CN TLV to carry a CNPV in all ports of the switch

- **cn cnpv - lldp-instance-selector** – This command configures the index to LLDP destination MAC address entry to be used in LLDP PDUs for a CNPV in all ports of the switch

### 64.3.2.8 cn cnpv - lldp-instance-choice

This command configures the CN TLV to carry a CNPV in all ports of the switch

```
cn cnpv <priority-value(0-7)> lldp-instance-choice { on | none }
```

<b>Syntax Description</b>	<b>&lt;priority-value(0-7)&gt;</b>	- Configures the priority-value for the congestion notification priority value. This value ranges between (0 and 7)
	<b>on</b>	- Configures the LLDP instance to be used to send and receive CN-TLV that is selected by the LLDP instance selector.
	<b>none</b>	- Configures the CN-TLV to be ignored without being sent.

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** on

**Example** iss(config)# cn cnpv 5 lldp-instance-choice on

#### Related Commands

- **set cn** - This command enables/disables congestion notification on all the ports on a switch.
- **shutdown cn** - This command starts the cn module in the switch.
- **set cn cnm-transmit-priority** - This command sets the VLAN priority to be used in all the CNM packets generated by the switch. This value ranges between 0-7.
- **cn cnpv** - This command creates a congestion notification priority value in the switch. The no form of the command deletes cnpv from the switch.
- **cn cnpv defense** - This command configures whether the default CND defense mode of a CNPV in all ports of a switch is determined by configured values or through LLDP.
- **cn cnpv - alternate-priority** - This command sets the default regenerated priority for incoming frames with a CNPV in all the ports of the switch.
- **cn cnpv - defense-mode** - This command sets the default CND defense-mode for a CNPV in all ports of a switch
- **cn cnpv - port-default-defense** - This command sets the default value for the defense-mode choice for all the ports of the switch
- **cn cnpv - lldp-instance-selector** - This command configures the index to LLDP destination MAC address entry to be used in LLDP PDUs for a

CNPV in all ports of the switch

### 64.3.2.9 cn cnpv - lldp-instance-selector

This command configures the index to LLDP destination MAC address entry to be used in LLDP PDUs for a CNPV in all ports of the switch

```
cn cnpv <priority-value (0-7)> lldp-instance-selector <integer (1-4096)>
```

<b>Syntax Description</b>	<b>&lt;priority-value (0-7)&gt;</b>	-	Configures the priority-value for the congestion notification priority value. This value ranges between 0 and 7
---------------------------	-------------------------------------	---	---

<b>Mode</b>	Global Configuration mode
-------------	---------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Defaults</b>	1
-----------------	---

<b>Example</b>	<pre>iss(config)# cn cnpv 5 lldp-instance-selector 500</pre>
----------------	--

- |                         |   |
|-------------------------|---|
| <b>Related Commands</b> | <ul style="list-style-type: none"> <li>• <b>set cn</b> - This command enables/disables congestion notification on all the ports on a switch.</li> <li>• <b>shutdown cn</b> - This command starts the cn module in the switch.</li> <li>• <b>set cn cnm-transmit-priority</b> - This command sets the VLAN priority to be used in all the CNM packets generated by the switch. This value ranges between 0-7.</li> <li>• <b>cn cnpv</b> - This command creates a congestion notification priority value in the switch. The no form of the command deletes cnpv from the switch.</li> <li>• <b>cn cnpv defense</b> - This command configures whether the default CND defense mode of a CNPV in all ports of a switch is determined by configured values or through LLDP.</li> <li>• <b>cn cnpv - alternate-priority</b> - This command sets the default regenerated priority for incoming frames with a CNPV in all the ports of the switch.</li> <li>• <b>cn cnpv - defense-mode</b> - This command sets the default CND defense-mode for a CNPV in all ports of a switch</li> <li>• <b>cn cnpv - port-default-defense</b> - This command sets the default value for the defense-mode choice for all the ports of the switch</li> <li>• <b>cn cnpv - lldp-instance-choice</b> - This command configures the CN TLV to carry a CNPV in all ports of the switch</li> </ul> |
|-------------------------|---|

### 64.3.2.10 shutdown cn

This command shutdowns the cn module in the switch. The no form of the command starts the cn module in the switch.

**shutdown cn**

**no shutdown cn**

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** started

**Example** iss(config)# no shutdown cn

**Related command S**

- **set cn** - This command enables/disables congestion notification on all the ports on a switch
- **set cn cnm-transmit-priority** - This command sets the VLAN priority to be used in all the CNM packets generated by the switch. This value ranges between 0-7.
- **cn cnpv** - This command creates a congestion notification priority value in the switch. The no form of the command deletes cnpv from the switch
- **cn cnpv defense** - This command configures whether the default CND defense mode of a CNPV in all ports of a switch is determined by configured values or through LLDP.
- **cn cnpv - alternate-priority** - This command sets the default regenerated priority for incoming frames with a CNPV in all the ports of the switch.
- **cn cnpv - defense-mode** - This command sets the default CND defense-mode for a CNPV in all ports of a switch.
- **cn cnpv - port-default-defense** - This command sets the default value for the defense-mode choice for all the ports of the switch
- **cn cnpv - lldp-instance-choice** - This command configures the CN TLV to carry a CNPV in all ports of the switch
- **cn cnpv - lldp-instance-selector** - This command configures the index to LLDP destination MAC address entry to be used in LLDP PDUs for a CNPV in all ports of the switch

### 64.3.2.11 cn trap

This command enables the sending of trap messages from cn to the management entity upon specific events. The no form of the command disables the sending of trap messages.

```
cn trap [error-port-table] [cnm]
```

```
no cn trap [error-port-table] [cnm]
```

<b>Syntax</b>	<b>error-port-table</b>	-	Configures the generation of trap messages when an entry is created or deleted in the ErrorPortTable.
<b>Description</b>			
<b>n</b>	<b>cnm</b>	-	Configures the generation of CNM trap when congestion occurs at CP.

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** Both error-port-table and cnm

**Example** iss(config)# cn trap cnm

**Related Commands**

- **shutdown cn** - This command starts the cn module in the switch.

### 64.3.2.12 cn cnpv - defense

This command configures whether the CND defense mode of a CNPV in the port is to be determined by the Admin values or through LLDP.

```
cn cnpv <priority-value(0-7)> defense { auto | on | component }
```

<b>Syntax Description</b>	<b>&lt;priority-value(0-7)&gt;</b>	- Configures the priority-value for the congestion notification priority value. This value ranges between 0 and 7
	<b>auto</b>	- Configures the default CND defense mode as auto. Defense mode is derived from LLDP exchanges.
	<b>on</b>	- Configures the default CND defense mode as on. The administrator configuration determines the defense mode.
	<b>component</b>	- Configures the defense mode choice to be determined from component priority table.

**Mode** Interface Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** component

**Example** iss(config-if)# cn cnpv 5 defense auto

**Related Commands**

- **shutdown cn** - This command starts the cn module in the switch.
- **cn cnpv - defense-mode** - This command sets the CND defense mode of a CNPV in a port
- **cn cnpv - lldp-instance-choice** - This command configures whether the CNPV can be sent in CN TLVs or not on a port
- **cn cnpv - lldp-instance-selector** - This command configures LLDP instance selection for automatic determination of CND defense mode for port and CNPV
- **cn cnpv - alternate-priority** - This command configures the default regenerated priority for incoming frames with a CNPV in a port
- **cn cp-properties** - This command configures the congestion point properties for a CNPV in a port

### 64.3.2.13 cn cnpv - defense-mode

This command sets the CND defense mode of a CNPV in a port.

```
cn cnpv <priority-value(0-7)> defense-mode { disabled | edge | interior | interiorReady }
```

<b>Syntax Description</b>	<b>&lt;priority-value(0-7)&gt;</b>	-	Configures the priority-value for the congestion notification priority value. This value ranges between 0 and 7)
	<b>disabled</b>	-	Configures the CN capability as administratively disabled. The priority regeneration table controls the re-mapping of input frames for the priority. End station does not add the CN-tags and the bridge does not strip the CN-tags
	<b>edge</b>	-	Re-maps the priority parameters of input frames to an alternate (non-CNPV) value, in spite of the priority regeneration table for the CNPV. End station does not add CN-tags, but the bridge removes the CN-tags from frames before transmitting the frames.
	<b>interior</b>	-	Does not re-map the priority parameters of input frames for the CNPV. End station does not add CN-tags, but the bridge removes the CN-tags from frames before transmitting the frames.
	<b>interiorReady</b>	-	Does not re-map the priority parameters of input frames for the CNPV. End station adds CN-tags, but the bridge does not remove the CN-tags from frames before transmitting the frames.

**Mode** Interface Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** disabled

**Example** `iss(config-if)# cn cnpv 5 defense-mode edge`

- Related Commands**
- **shutdown cn** - This command starts the cn module in the switch.
  - **cn cnpv - defense** - This command configures whether the CND defense mode of a CNPV in the port is to be determined by the Admin values or through LLDP.
  - **cn cnpv - lldp-instance-choice** - This command configures whether

---

the CNPV can be sent in CN TLVs or not on a port

- **cn cnpv - lldp-instance-selector** - This command configures LLDP instance selection for automatic determination of CND defense mode for port and CNPV
- **cn cnpv - alternate-priority** - This command configures the default regenerated priority for incoming frames with a CNPV in a port
- **cn cp-properties** - This command configures the congestion point properties for a CNPV in a port

### 64.3.2.14 cn cnpv - lldp-instance-choice

This command configures whether the CNPV can be sent in CN TLVs or not on a port

```
cn cnpv <priority-value(0-7)> lldp-instance-choice { on | component | none }
```

<b>Syntax Description</b>	<b>&lt;priority-value(0-7)&gt;</b>	- Configures the priority-value for the congestion notification priority value. This value ranges between 0 and 7
	<b>on</b>	- Configures the LLDP instance selected by the LLDP instance selector to be used to send and receive CN TLVs
	<b>component</b>	- Configures the instance choice to be derived from component priority table configuration.
	<b>none</b>	- Configures CNPV not to be sent on CN TLVs and ignored on receipt.

**Mode** Interface configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** component

**Example**

```
iss(config-if)# cn cnpv 5 lldp-instance-choice none
```

#### Related Commands

- **shutdown cn** - This command starts the cn module in the switch.
- **cn cnpv - defense** - This command configures whether the CND defense mode of a CNPV in the port is to be determined by the Admin values or through LLDP.
- **cn cnpv - defense-mode** - This command sets the CND defense mode of a CNPV in a port
- **cn cnpv - lldp-instance-selector** - This command configures LLDP instance selection for automatic determination of CND defense mode for port and CNPV
- **cn cnpv - alternate-priority** - This command configures the default regenerated priority for incoming frames with a CNPV in a port
- **cn cp-properties** - This command configures the congestion point properties for a CNPV in a port

### 64.3.2.15 cn cnpv - lldp-instance-selector

This command configures LLDP instance selection for automatic determination of CND defense mode for port and CNPV.

```
cn cnpv <priority-value (0-7)> lldp-instance-selector <integer>
```

<b>Syntax Description</b>	<b>&lt;priority-value (0-7)&gt;</b>	-	Configures the priority-value for the congestion notification priority value. This value ranges between 0 and 7
---------------------------	-------------------------------------	---	---

<b>Mode</b>	Interface Configuration Mode
-------------	------------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Defaults</b>	3
-----------------	---

<b>Example</b>	<code>iss(config-if)# cn cnpv 5 lldp-instance-selector 500</code>
----------------	---

<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• <b>shutdown cn</b> - This command starts the cn module in the switch.</li> <li>• <b>cn cnpv - defense</b> - This command configures whether the CND defense mode of a CNPV in the port is to be determined by the Admin values or through LLDP.</li> <li>• <b>cn cnpv - defense-mode</b> - This command sets the CND defense mode of a CNPV in a port</li> <li>• <b>cn cnpv - lldp-instance-choice</b> - This command configures whether the CNPV can be sent in CN TLVs or not on a port</li> <li>• <b>cn cnpv - alternate-priority</b> - This command configures the default regenerated priority for incoming frames with a CNPV in a port</li> <li>• <b>cn cp-properties</b> - This command configures the congestion point properties for a CNPV in a port</li> </ul>
-------------------------	---

### 64.3.2.16 cn cnpv - alternate-priority

This command configures the default regenerated priority for incoming frames with a CNPV in a port.

```
cn cnpv <priority-value(0-7)> alternate-priority <priority-value(0-7)>
```

<b>Syntax description</b>	<code>&lt;priority-value(0-7)&gt;</code>	- Configures the priority-value for the congestion notification priority value. This value ranges between 0 and 7
	<code>Alternate-priority &lt;priority-value(0-7)&gt;</code>	- Configures the priority value for which the incoming frame is to be mapped. This value ranges between 0 and 7

**Mode** Interface Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** 0

**Example** `iss(config-if)# cn cnpv 5 alternate-priority 5`

#### Related Commands

- `shutdown cn` - This command starts the cn module in the switch.
- `cn cnpv - defense` - This command configures whether the CND defense mode of a CNPV in the port is to be determined by the Admin values or through LLDP.
- `cn cnpv - defense-mode` - This command sets the CND defense mode of a CNPV in a port
- `cn cnpv - lldp-instance-choice` - This command configures whether the CNPV can be sent in CN TLVs or not on a port
- `cn cnpv - lldp-instance-selector` - This command configures LLDP instance selection for automatic determination of CND defense mode for port and CNPV.
- `cn cp-properties` - This command configures the congestion point properties for a CNPV in a port

### 64.3.2.17 cn cp-properties

This command configures the congestion point properties for a CNPV in a port.

```
cn          cp-properties          <priority-value (0-7)>          {[qsize-set-point
<integer (100..4294967295)>]      [feedback-weight          <(-10..10)>]      [samples
<integer (10000..4294967295)>] [header-octets <integer (0..64)>]}
```

<b>Syntax description</b>	<b>&lt;priority-value (0-7)&gt;</b>	-	Configures the priority-value for the congestion notification priority value. This value ranges between 0 and 7
	<b>qsize-set-point &lt;integer (100 - 4294967295)&gt;</b>	-	Configures the set point for total number of octets stored in a queue managed by congestion point. This value ranges between 100 and 4294967295
	<b>feedback-weight&lt;(-10 ..10)&gt;</b>	-	Controls weight cpw change in queue length in the calculation of cpFb when congestion point is generating CN messages. This value ranges between<-10 and 10>
	<b>Samples &lt;integer (10000.. 4294967295)&gt;</b>	-	Configures the minimum number of octets to enqueue in the congestion point queue between transmissions of CN messages. This value ranges between 10000 and 4294967295.
	<b>header-octets&lt;integer (0..64)&gt;</b>	-	Configures the minimum number of octets to be returned in a CN message from mac_service_data_unit of the data frame that triggered transmission of the CNM. This value ranges between 0 and 64.
<b>Mode</b>	Interface Configuration Mode		
<b>Package</b>	Workgroup, Enterprise and Metro		
<b>Defaults</b>	qsize-set-point	-	26000
	feedback-weight	-	1
	samples	-	150000

---

header-octets - 0

**Example** `iss(config-if)# cn cp-properties 4 qsize-set-point 101 samples 10100`

**Related  
Command  
s**

- **shutdown cn** - This command starts the cn module in the switch.
- **cn cnpv - defense** - This command configures whether the CND defense mode of a CNPV in the port is to be determined by the Admin values or through LLDP.
- **cn cnpv - defense-mode** - This command sets the CND defense mode of a CNPV in a port
- **cn cnpv - lldp-instance-choice** - This command configures whether the CNPV can be sent in CN TLVs or not on a port
- **cn cnpv - lldp-instance-selector** - This command configures LLDP instance selection for automatic determination of CND defense mode for port and CNPV.
- **cn cnpv - alternate-priority** - This command configures the default regenerated priority for incoming frames with a CNPV in a port.

### 64.3.2.18 debug cn

This command enables CN debug messages. The no form of the command disables the debug messages.

```
debug cn [mgmt] [sem] [tlv] [resource] [redundancy] [fail] [control-plane]
[switch <context name>]
```

```
no debug cn [mgmt] [sem] [tlv] [resource] [redundancy] [fail] [control-plane]
[switch <context name>]
```

<b>Syntax description</b>	<b>mgmt</b>	-	Generates debug statements for management plane functionality traces.
	<b>sem</b>	-	Generates debug statements for state machine handling traces. This trace is generated when there is an error condition in State Machine
	<b>tlv</b>	-	Generates tlv related trace messages
	<b>resource</b>	-	Generates traces related to all resources such as memory, data structure and the like. These traces are used for failure of memory allocation and so on.
	<b>redundancy</b>	-	Generates debug statements for redundancy code flow traces. This trace is generated when there is a failure in redundancy processing
	<b>fail</b>	-	All failure traces. These traces are used for all valid and invalid failures. The valid failures represent the expected error. The invalid failures represent the unexpected error.
	<b>control-plane</b>	-	Generates Control plane traces. These traces are used for cases such as MBSM card removal, failure of state change and so on.
	<b>switch&lt;context name&gt;</b>	-	Configures the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

**Mode** Privileged Exec Mode / User Exec Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** fail

**Example** iss# debug cn mgmt

**Related  
Commands**

- **shutdown cn** - This command starts the cn module in the switch.
- **clear cn counters** - This command clears the CN counters on a port or a switch
- **show cn global information** - This command displays the CN global details of the switch
- **show cn interface counters** - This command displays the CN traffic port counters.
- **show cn cnpv** - This command displays the CNPV details on a port or a switch
- **show cn cp-properties** - This command displays configured congestion point details of CNPVs in a port or switch
- **show debugging** - displays the traces enabled for the CN module

### 64.3.2.19 clear cn counters

This command clears the CN counters on a port or a switch.

```
clear cn counters [ { {interface <ifXtype> <ifnum>} | {switch <context name> } ]
```

<b>Syntax description</b>	<b>&lt;ifXtype&gt;</b>	-	<p>Clears the configurations on specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul>
	<b>&lt;ifnum&gt;</b>	-	<p>Clears the configurations for specified interface identifier. This is a unique value that represents the specific interface.</p> <p>This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.</p> <p>For example: 0/1 represents that the slot number is 0 and port number is 1.</p> <p>Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</p>
	<b>switch&lt;context name&gt;</b>	-	<p>Clears the configuratios for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.</p>
<b>Mode</b>	Privileged Exec Mode / User Exec Mode		

**Package** Workgroup, Enterprise and Metro

**Example** iss# clear cn counters interface gigabitethernet 0/2

- Related Commands**
- **shutdown cn** - This command starts the cn module in the switch.
  - **debug cn** - This command enables CN debug messages
  - **show cn global information** - This command displays the CN global details of the switch
  - **show cn interface counters** - This command displays the CN traffic port counters.
  - **show cn cnpv** - This command displays the CNPV details on a port or a switch
  - **show cn cp-properties** - This command displays configured congestion point details of CNPVs in a port or switch

### 64.3.2.20 show cn global information

This command displays the CN global details of the switch

```
show cn global information [switch <context name>]
```

<b>Syntax description</b>	<b>switch&lt;context name&gt;</b>	-	Displays the configuration information for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
---------------------------	-----------------------------------	---	--

<b>Mode</b>	Privileged Exec Mode / User Exec Mode
-------------	---------------------------------------

<b>Package</b>	Workgroup, Enterprise and Metro
----------------	---------------------------------

<b>Example</b>	<pre>iss# show cn global information Enabled Traps: Errored Port and CNM Switch default ----- Module Status          : Enabled CNPVs                  : 5 CNM Transmit Priority  : 6 GlobalDiscardedFrames : 0 GlobalTLVErrors        : 0</pre>
----------------	---

<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• <b>set cn</b> - This command enables/disables congestion notification on all the ports in a switch</li> <li>• <b>shutdown cn</b> - This command starts the cn module in the switch.</li> <li>• <b>debug cn</b> - This command enables CN debug messages</li> <li>• <b>show cn interface counters</b> - This command displays the CN traffic port counters.</li> <li>• <b>show cn cnpv</b> - This command displays the CNPV details on a port or a switch</li> <li>• <b>show cn cp-properties</b> - This command displays configured congestion point details of CNPVs in a port or switch</li> </ul>
-------------------------	---

### 64.3.2.21 show cn interface counters

This command displays the CN traffic port counters.

```
show cn interface counters [<interface-type> <interface-number>] [<cn-
priority-value (0-7)>]
```

<b>Syntax</b>	<b>&lt;interface-type&gt;</b>	-	<p>Displays the configurations information for specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul>
<b>description</b>	<b>&lt;interface-number&gt;</b>	-	<p>Displays the configuration information for the specified interface identifier. This is a unique value that represents the specific interface.</p> <p>This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.</p> <p>For example: 0/1 represents that the slot number is 0 and port number is 1.</p> <p>Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</p>
<b>n</b>	<b>&lt;cn-priority-value (0-7)&gt;</b>	-	<p>Displays the priority-value for the congestion notification priority value. This value ranges between (0-7).</p>
<b>Mode</b>	Privileged Exec Mode / User Exec Mode		

**Package** Workgroup, Enterprise and Metro

**Example** iss# show cn interface counters gigabitethernet 0/1 5

```

Interface CNPV   Transmitted Frames   Discarded Frames   Transmitted
Cnms
-----
Gi0/1           5           40234                0                   2

```

**Related commands**

- **shutdown cn** - This command starts the cn module in the switch.
- **debug cn** - This command enables CN debug messages
- **show cn global information** - This command displays the CN global details of the switch
- **show cn cnpv** - This command displays the CNPV details on a port or a switch
- **show cn cp-properties** - This command displays configured congestion point details of CNPVs in a port or switch

### 64.3.2.22 show cn cnpv

This command displays the CNPV details on a port or a switch.

```
show cn cnpv {port | comp} [<cn-priority-value(0-7)>] [ { <interface-type>
<interface-number> | switch <context name> } ]
```

<b>Syntax description</b>	<b>port</b>	-	Displays the port related configuration
	<b>comp</b>	-	Displays component priority table related configurations.
	<b>&lt;cn-priority-value(0-7)&gt;</b>	-	Displays the priority-value for the congestion notification priority value. This value ranges between 0 and 7.
	<b>&lt;interface-type&gt;</b>	-	<p>Displays the configuration information for the specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul>
	<b>&lt;interface-number&gt;</b>	-	<p>Displays the configuration information for the specified interface identifier. This is a unique value that represents the specific interface.</p> <p>This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.</p> <p>For example: 0/1 represents that the slot number is 0 and port number is 1.</p> <p>Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1</p>

represents i-lan and port-channel ID.

**Switch<context name>** - Displays the configuration information for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

**Mode** Privileged Exec Mode / User Exec Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show cn cnpv port gigabitethernet 0/1

```
Port Gi0/1 , CNPV 5

DefModeChoice      : Comp
OperDefMode        : Edge
AdminDefenseMode   : Disabled
OperAltPri         : 0
AlternatePriority   : 0
LldpInstanceChoice : Comp
LldpInstanceSelector : 3
IsErroredPort      : No
LastRcvdEvent      : Aged Out Event Received
LastRcvdEventTime  : Aug 12 16:52:10 2010
LastSentEvent      : Sent CNPV Indicator
LastSentEventTime  : Aug 12 16:52:24 2010
```

#### Related Commands

- **shutdown cn** - This command shutdowns the cn module in the switch.
- **debug cn** - This command enables CN debug messages
- **show cn global information** - This command displays the CN global details of the switch
- **show cn interface counters** - This command displays the CN traffic port counters.
- **show cn cp-properties** - This command displays configured congestion point details of CNPVs in a port or switch

### 64.3.2.23 show cn cp-properties

This command displays configured congestion point details of CNPVs in a port or switch.

```
show cn cp-properties [<CNPV(0-7)>] [ { <interface-type> <interface-number> |
switch <context name> } ]
```

<b>Syntax description</b>	<b>&lt;cn-priority-value (0-7)&gt;</b>	-	Displays the priority-value related information. This value ranges between 0 and 7.
	<b>&lt;interface-type&gt;</b>	-	<p>Displays the configuration information for the specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul>
	<b>&lt;interface-number&gt;</b>	-	<p>Displays the configuration information for the specified interface identifier. This is a unique value that represents the specific interface.</p> <p>This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.</p> <p>For example: 0/1 represents that the slot number is 0 and port number is 1.</p> <p>Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</p>
	<b>Switch&lt;context name&gt;</b>	-	Displays the configuration information for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

**Mode** Privileged Exec Mode / User Exec Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show cn cp-properties gigabitethernet 0/1

```

Interface CNPV      Cp Identifier      QSizeSetPt  FeedBackWt
MinSamBase HdrOcts
-----
Gi0/1      5    00:01:02:03:04:01:00:05  26000      1
150000    0

```

**Related  
Commands**

- **shutdown cn** - This command starts the cn module in the switch.
- **debug cn** - This command enables CN debug messages
- **show cn global information** - This command displays the CN global details of the switch
- **show cn interface counters** - This command displays the CN traffic port counters.
- **show cn cnpv** - This command displays the CNPV details on a port or a switch

# Chapter

# 65

## ACL

---

ACLs (Access Control Lists) filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. ACLs are used to block IP packets from being forwarded by a router. The router examines each packet to determine whether to forward or drop the packet, based on the criteria specified within the access lists.

Access list criteria can be the source address of the traffic, the destination address of the traffic, the upper-layer protocol or other information.

There are many reasons to configure access lists - access lists can be used to restrict contents of routing updates or to provide traffic flow control. But one of the most important reasons to configure access lists is to provide security for the network.

Access lists must be used to provide a basic level of security for accessing the network. If access lists has not been configured on the router, all packets passing through the router can be allowed onto all parts of the network.

For example, access lists can allow one host to access a part of the network and prevent another host from accessing the same area.

## 65.1 Linux Environment Commands

This section describes the CLI commands executable only in Linux environment for configuring ACL feature supported by ISS.

The list of CLI commands for the configuration of ACL is as follows:

- ip access-list
- mac access-list extended
- user-defined access-list
- traffic-separation control
- userdefined-list
- permit usr-defined-packet-type
- deny usr-defined-packet-type
- permit - standard mode
- deny - standard mode
- copy-to-cpu - standard mode
- permit- ip/ospf/pim/protocol type
- permit ipv6
- deny - ip/ospf/pim/protocol type
- copy-to-cpu - ip / ospf / pim / protocol-type
- deny ipv6
- copy-to-cpu ipv6
- permit tcp
- deny tcp
- copy-to-cpu tcp
- permit udp
- deny udp
- copy-to-cpu udp
- permit icmp
- deny icmp
- copy-to-cpu icmp
- ip access-group
- mac access-group
- user-defined access-group
- permit - MAC
- deny - MAC

- copy-to-cpu - MAC

## 65.1.1 ip access-list

This command creates IP ACLs and enters the IP Access-list configuration mode. Standard access lists create filters based on IP address and network mask only (L3 filters only). Extended access lists enables specification of filters based on the type of protocol, range of TCP/UDP ports as well as the IP address and network mask (Layer 4 filters).

Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode.

The no form of the command deletes the IP access-list.

```
ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> }
```

```
no ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> }
```

<b>Syntax Description</b>	<b>standard</b>	-	Standard access-list number
	<b>extended</b>	-	Extended access-list number

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss(config)# ip access-list standard 1



ACLs on the system perform both access control and Layer 3 field classification. To define Layer 3 fields' access-lists the **ip access-list** command must be used.

**Related Commands**

- **permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters
- **deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched
- **copy-to-cpu - standard mode** - Copies the IP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- **permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- **permit ipv6** - Specifies IP packets to be forwarded based on protocol and associated parameters.
- **deny - ip/ospf/pim/protocol type** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- **copy-to-cpu - ip / ospf / pim / protocol-type** - Copies the IP control packets of all type of protocols to control plane CPU with or without switching of

packets based on the configured parameters.

- **deny ipv6** - Specifies IPv6 packets to be rejected based on protocol and associated parameters.
- **copy-to-cpu ipv6** - Copies the IPv6 control packets to control plane CPU with or without switching of packets based on the configured parameters.
- **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters
- **deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters
- **copy-to-cpu tcp** - Copies the TCP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- **permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters
- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters
- **copy-to-cpu udp** - Copies the UDP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- **copy-to-cpu icmp** - Copies the ICMP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- **ip access-group** - Enables access control for the packets on the interface
- **show access-lists** - Displays the access list configuration

## 65.1.2 mac access-list extended

This command creates Layer 2 MAC ACLs, that is, this command creates a MAC access-list and returns the MAC-Access list configuration mode to the user. The no form of the command deletes the MAC access-list.

```
mac access-list extended <access-list-number (1-65535)>
```

```
no mac access-list extended <short (1-65535)>
```

**Syntax Description**      **access-**  
**list-number**                      -    Access list number

**Mode**                      Global Configuration Mode

**Package**                  Workgroup, Enterprise and Metro

**Example**                  `iss(config)# mac access-list extended 5`



ACLs on the system perform both access control and layer 2 field classification. To define Layer 2 access lists, the mac access-list command must be used.

### Related Commands

- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface.
- **permit - MAC** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **deny - MAC** - Specifies the packets to be rejected based on the MAC address and the associated parameters
- **copy-to-cpu - MAC** - Copies the MAC protocol control packets to control plane CPU with or without switching of packets based on the configured parameters.
- **show access-lists** - Displays the access lists configuration.

### 65.1.3 user-defined access-list

This command creates a user defined access-list. The no form of the command deletes the user defined access-list. The value ranges between 1 to 65535.

```
user-defined access-list <access-list-number (1-65535)>
```

```
no user-defined access-list <short (1-65535)>
```

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config)# user-defined access-list 5`



ACLs on the system perform both access control and layer 2 field classification based on user defined bytes in the packets.

**Related Commands**

- **permit usr-defined-packet-type** - Permits Packet Based on User Defined Packet type
- **userdefined-list**- Creates a user defined access list by applying AND, OR, NOT operation ( regular expressions) on existing ACL rules or specifying match on user-defined packet offsets.
- **permit usr-defined-packet-type** - Permits Packet Based on User Defined Packet Byte
- **user-defined access-group** - Applies a user defined access list (ACL) to an interface.
- **permit - MAC** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **deny - MAC** - Specifies the packets to be rejected based on the MAC address and the associated parameters
- **show access-lists** - Displays the access list configuration

## 65.1.4 traffic-separation control

This command globally configures the method to be implemented for carrying control packets to CPU for processing.

```
traffic-separation control {system_default | user_defined}
```

<b>Syntax Description</b>	<b>system_default</b>	<ul style="list-style-type: none"> <li>- Installs automatically the default ACL / QoS rules defined by ISS software for all control packets during system init time.</li> <li>Either a switch-and-copy-to-cpu filter or drop-and-copy-to-cpu filter is installed for sending the control packets to CPU.</li> <li>The default rules are installed while the existing user configured rules (if any) are not removed.</li> </ul>
	<b>user_defined</b>	<ul style="list-style-type: none"> <li>- Waits for administrator to install the required rules for the control packets.</li> <li>All the default ACL / QoS rules are removed and the user specific ACL / QoS rules are implemented.</li> </ul>
<b>Mode</b>	Global Configuration Mode	
<b>Package</b>	Workgroup, Enterprise and Metro	
<b>Defaults</b>	user_defined Due to limitations, the default value mentioned in MIB (system_default) is not implemented. This limitation is captured in the ISS release notes.	
<b>Example</b>	<pre>iss(config)# traffic-separation control user_defined</pre>	
		This command is available, only if the switch NPAPI_WANTED or QOSX_WANTED is set as yes during compilation of the exe.
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• <b>show access-lists</b> - Displays the access lists configuration.</li> </ul>	

## 65.1.5 userdefined-list

This command creates a user defined access list after application of regular expressions AND, OR, NOT on existing ACL rules

```
userdefined-list {{ ip-acl1-and-ip-acl2 | ip-acl1-or-ip-acl2 | mac-acl1-and-
mac-acl2 | mac-acl1-and-ip-acl2 | mac-acl1-or-mac-acl2 | ip-acl1-or-mac-acl2 }
<short (1-65535)> <short (1-65535)> | { not-ip-acl1 | not-mac-acl1 } <short (1-
65535)>} [priority <short (1-255)>]
```

<b>Syntax</b>	<b>ip-acl1-and-ip-acl2</b>	-	Performs AND operation on two Layer 3 ACL Rules ( acl1 , acl2). And create a new layer 3 ACL rule that is represented by this user defined access-list..The filter action corresponding to the new ACL rule is identical to the base rules.
<b>Description</b>	<b>n</b>		
	<b>ip-acl1-or-ip-acl2</b>	-	Performs OR operation on two layer 3 ACL Rules. This operation results in applying the action of ACL Rule 1 on ACL Rule 2
	<b>mac-acl1-and-mac-acl2</b>	-	Performs AND operation on two layer 2 ACL Rules and create a new layer 2 ACL rule that is represented by this user defined access-list. The filter action corresponding to the new ACL rule is identical to the base rules.
	<b>mac-acl1-and-ip-acl2</b>	-	Performs AND operation on two ACL rules - acl1 ( layer 2 ACL Rule) and acl2 ( Layer 3 ACL rule) and create an new ACL Rule represented by this user defined access-list. The filter action corresponding to the new ACL rule is identical to the base rules.
	<b>mac-acl1-or-mac-acl2</b>	-	Performs OR operation on two Layer 2 ACL Rules and results in application of filter-action of ACL1 on ACL2
	<b>ip-acl1-or-mac-acl2</b>	-	Performs OR operation on Layer 3 ACL Rule (ACL1) using Layer 2 ACL rule ( ACL2) and results in application of filter-action of ACL1 on ACL2.
	<b>not-ip-acl1</b>	-	Performs NOT operation on ACL Rule 1 and derive new Rule. The filter action for the derived ACL Rule is “deny” if base Rule is configured for filter action “permit” and vice-versa. Other actions are not applicable for this operation

- not-mac-acl1**
- Performs NOT operation on ACL Rule 1 and derive new Rule. The filter action for the derived ACL Rule is “deny” if base Rule is configured for filter action “permit” and vice-versa. Other actions are not applicable for this operation
- priority**
- Priority of the L2 filter. This is used to decide which filter rule is applicable,
    - when the packet matches with more than one filter rules.
    - All the filter rules result in allowing the packet.
- Higher value of filter priority implies a higher priority  
This value ranges between 1 and 255.

**Mode** User Defined Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** priority - 1

**Example** iss(config-userdef-acl)# userdefined-list ip-acl1-and-ip-acl2  
15 123

- Related Commands**
- **user-defined access-list** - Creates the user defined access-list.
  - **show access-lists** - Displays the access list configuration

## 65.1.6 permit usr-defined-packet-type

This command permits packets matching a particular User Defined Byte and by specifying the packet type – namely user-defined, tcp-ipv4, udp, mpls, ipv4, ipv6, frag-ip.

```
permit usr-defined-packet-type { user-def | tcp-ipv4 | udp-ipv4 | mpls | ipv4
| ipv6 | frag-ip }offset-base {12 | 13 | 14 | ipv6-ext-hdr | ether-type |
<short(0-127)>} offset1 <short(0-127)> <short(0-255)>[offset2 <short(0-127)>
<short(0-255)>][offset3 <short(0-127)> <short(0-255)>][offset4 <short(0-127)>
<short(0-255)>][offset5 <short(0-127)> <short(0-255)>][offset6 <short(0-127)>
<short(0-255)>][redirect {interface <ifXtype> <ifnum> | <ifXtype><iface_list>
[<ifXtype><iface_list>]}load-balance {src-ip | dst-ip | src-mac | dst-mac |
vlanid | src-tcport| dst-tcport | src-udpport | dst-udpport | udb <short(0-
127)>}}][sub-action {none | modify-vlan<short(1-4094)> | nested-vlan <short
(1-4094)>}}] [priority <short(1-255)>]
```

<b>Syntax Description</b>	<b>user-def</b>	-	Specifies the packet type as user defined.
	<b>tcp-ipv4</b>	-	Specifies the packet type as tcp in the ipv4 packet.
	<b>udp-ipv4</b>	-	Specifies the packet type as udp in the ipv4 packet.
	<b>mpls</b>	-	Specifies the packet type as mpls.
	<b>ipv4</b>	-	Specifies the packet type as ipv4.
	<b>ipv6</b>	-	Specifies the packet type as ipv6.
	<b>frag-ip</b>	-	Specifies the packet type as fragmented ip.
	<b>offset-base</b>	-	<ul style="list-style-type: none"> <li>- Specifies the start of the packet from which the user defined byte should be considered.</li> <li>• I2 – Start of the packet is considered as layer 2</li> <li>• I3 – Start of the packet is considered as layer 3</li> <li>• I4 – Start of the packet is considered as layer 4</li> <li>• ipv6-ext-hdr - Start of the packet is considered as ipv6 extended header.</li> <li>• ether-type – Start of the packet is considered as ether type.</li> </ul>
	<b>offset1</b>	-	Specifies the offset position and offset value that needs to be considered as the match for offset1.

The two input value ranges 0 to 127 and 0 to 255.

- offset2**
  - Specifies the offset position and offset value value that needs to be considered as the match for offset 2. The two input value ranges 0 to 127 and 0 to 255.
  
- Offset3**
  - Specifies the offset position and offset value that needs to be considered as the match for offset 3. The two input value ranges 0 to 127 and 0 to 255.
  
- Offset4**
  - Specifies the offset position and offset value that needs to be considered as the match for offset 4. The two input value ranges 0 to 127 and 0 to 255.
  
- Offset5**
  - Specifies the offset position and offset value that needs to be considered as the match for offset 5. The two input value ranges 0 to 127 and 0 to 255.
  
- Offset6**
  - Specifies the offset position and value that needs to be considered as the match for offset 6. The two input value ranges 0 to 127 and 0 to 255.
  
- Redirect**
  - Redirects the packet to the destination interface or set of interfaces.
    - ifXtype – Specifies the interface type
    - ifnum – Specifies the interface number
    - iface\_list – Specifies the list of interfaces
  
- load-balance**
  - Specifies the parameters based on which the traffic distribution needs to be done. Options are:
    - src-ip
    - dst-ip
    - src-mac
    - dst-mac
    - vlanid
    - src-tcpport
    - dst-tcpport
    - src-udpport
    - dst-udpport
    - udb

Options in the Layer 3 header are classified as IPv4 or IPv6 based on packet type
  
- sub-action**
  - Specifies the VLAN specific sub action to be performed on the packet -
    - none – Actions relating to the VLAN ID will not

be considered.

- **modify-vlan** – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
- **nested-vlan** – Adds an outer VLAN tag to the packet with the VLAN ID as configured.

### **priority**

- Priority of the L2 filter. This is used to decide which filter rule is applicable,
  - when the packet matches with more than one filter rules.
  - All the filter rules result in allowing the packet.

Higher value of filter priority implies a higher priority

This value ranges between 1 and 255.

**Mode** User Defined Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** priority - 1

**Example**

```
iss(config-userdef-acl)# permit usr-defined-packet-type user-def
offset-base 12 offset1 5 10 load-balance src-ip
```

- Related Commands:**
- **user-defined access-list** - Creates the user defined access-list.
  - **show access-lists** - Displays the access list configuration

## 65.1.7 deny usr-defined-packet-type

This command denies packets matching a particular User Defined Byte and by specifying the packet type – namely user-defined, tcp-ipv4, udp, mpls, ipv4, ipv6, frag-ip.

```
deny usr-defined-packet-type { user-def | tcp-ipv4 | udp-ipv4 | mpls | ipv4
| ipv6 | frag-ip }offset-base {12 | 13 | 14 | ipv6-ext-hdr | ether-type |
<short(0-127)>} offset1 <short(0-127)> <short(0-255)> [offset2 <short(0-127)>
<short(0-255)>] [offset3 <short(0-127)> <short(0-255)>] [offset4 <short(0-127)>
<short(0-255)>] [offset5 <short(0-127)> <short(0-255)>] [offset6 <short(0-127)>
<short(0-255)>] [priority <short(1-255)>]
```

### Syntax Description

- |                                |   |  |
|--------------------------------|---|--|
| <b>usr-defined-packet-type</b> | - | <ul style="list-style-type: none"> <li>• user-def – Specifies the packet type as user defined</li> <li>• tcp-ipv4 – Specifies the packet type as tcp in the ipV4 packet.</li> <li>• udp-ipv4 - Specifies the packet type as udp in the ipV4 packet.</li> <li>• mpls - Specifies the packet type as mpls.</li> <li>• ipv4 - Specifies the packet type as ipv4.</li> <li>• ipv6 - Specifies the packet type as ipv6.</li> <li>• frag-ip - Specifies the packet type as fragmented ip.</li> </ul>   |
| <b>offset-base</b>             | - | <ul style="list-style-type: none"> <li>- Specifies the start of the packet from which the user defined byte should be considered</li> <li>• 12 – Start of the packet is considered as layer 2</li> <li>• 13 – Start of the packet is considered as layer 3</li> <li>• 14 – Start of the packet is considered as layer 4</li> <li>• ipv6-ext-hdr – Start of the packet is considered as ipv6 extended header.</li> <li>• ether-type – Start of the packet is considered as ether type.</li> </ul> |
| <b>offset1</b>                 | - | <ul style="list-style-type: none"> <li>- Specifies the offset position and offset value that needs to be considered as the match for offset1. The two input value ranges 0 to 127 and 0 to 255.</li> </ul>   |
| <b>offset2</b>                 | - | <ul style="list-style-type: none"> <li>- Specifies the offset position and offset value that needs to be considered as the match for offset2.</li> </ul>   |

		The two input value ranges 0 to 127 and 0 to 255
<b>Offset3</b>	-	Specifies the offset position and offset value that needs to be considered as the match for offset3. The two input value ranges 0 to 127 and 0 to 255
<b>Offset4</b>	-	Specifies the offset position and offset value that needs to be considered as the match for offset4. The two input value ranges 0 to 127 and 0 to 255.
<b>Offset5</b>	-	Specifies the offset position and offset value that needs to be considered as the match for offset5. The two input value ranges 0 to 127 and 0 to 255
<b>Offset6</b>	-	Specifies the offset position and offset value that needs to be considered as the match for offset6. The two input value ranges 0 to 127 and 0 to 255
<b>priority</b>	-	<p>Priority of the L2 filter. This is used to decide which filter rule is applicable,</p> <ul style="list-style-type: none"> <li>• when the packet matches with more than one filter rules.</li> <li>• All the filter rules result in allowing the packet.</li> </ul> <p>Higher value of filter priority implies a higher priority This value ranges between 1 and 255.</p>
<b>Mode</b>		User Defined Configuration Mode
<b>Package</b>		Workgroup, Enterprise and Metro
<b>Defaults</b>	priority	- 1
<b>Example</b>		<pre>iss(config-userdef-acl)# deny  usr-defined-packet-type user-def offset-base 12 offset1 112 25</pre>
<b>Related Commands:</b>		<ul style="list-style-type: none"> <li>• <b>show access-lists</b> - Displays the access list configuration</li> </ul>

## 65.1.8 permit - standard mode

This command specifies the packets to be forwarded depending upon the associated parameters. Standard IP access lists use source addresses for matching operations.

```
permit { any | host <src-ip-address> | <network-src-ip> <mask> } [{ any | host
<dest-ip-address> | <network-dest-ip> <mask>}] [ForQoS] [redirect {interface
<ifXtype> <ifnum> | <ifXtype><iface_list> [<ifXtype><iface_list>] load-balance
{src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport |
src-udpport | dst-udpport}}] [sub-action {none | modify-vlan<short (1-4094)> |
nested-vlan <short (1 -4094)>}] [priority <short (1-255)>]
```

<b>Syntax</b>	any host	-	Source IP address can be
<b>Description</b>	<b>n</b> <src-ip-address>  <network-src-ip- ><mask>		<ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the dotted decimal address</li> <li>• the IP address of the host that the packet is from and the network mask to use with the source IP address</li> </ul>
	any host <dest-ip-address>  < network-dest-ip> <mask>	-	Destination IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the dotted decimal address or</li> <li>• the IP address of the host that the packet is destined for and the network mask to use with the destination IP address</li> </ul>
<b>ForQoS</b>		-	The configuration done is made available for the QoS rules also.
<b>redirect</b>		-	Redirects the action to the destination interface or set of interfaces. <ul style="list-style-type: none"> <li>• ifXtype – Specifies the interface type</li> <li>• ifnum – Specifies the interface number</li> <li>• iface_list – Specifies the list of interfaces</li> </ul>
<b>load-balance</b>		-	Specifies the parameters based on which the traffic distribution needs to be done. Options are: <ul style="list-style-type: none"> <li>• src-ip</li> <li>• src-mac</li> <li>• dst-ip</li> <li>• dst-mac</li> </ul>

- vlanid
- src-tcpport
- dst-tcpport
- src-udpport
- dst-udpport

Options in the Layer 3 header are classified as IPv4 or IPv6 based on packet type

**sub-action**

- Specifies the VLAN specific sub action to be performed on the packet -
  - none – Actions relating to the VLAN ID will not be considered.
  - modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
  - nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.

**priority**

- Priority of the L2 filter. This is used to decide which filter rule is applicable,
  - when the packet matches with more than one filter rules.
  - All the filter rules result in allowing the packet.

Higher value of filter priority implies a higher priority

This value ranges between 1 and 255.

**Mode** ACL Standard Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** priority - 1

**Example** `iss(config-std-nacl)# permit host 100.0.0.10`

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched
- **show access-lists** - Displays the access list configuration

## 65.1.9 deny - standard mode

This command denies traffic if the conditions defined in the deny statement are matched.

```
deny{ any | host <src-ip-address> | <network-src-ip> <mask> } [ { any | host
<dest-ip-address> | <network-dest-ip> <mask> } ] [priority <short (1-255)>]
```

<b>Syntax Description</b>	<p><b>any host</b></p> <p><b>src-ip-address </b> <b>&lt;network-src-ip&gt;</b> <b>&lt;mask&gt;</b></p>	<ul style="list-style-type: none"> <li>- Source IP address can be             <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is from and the network mask to use with the source IP address</li> </ul> </li> </ul>
<b>any host</b>	<p><b>dest-ip-address </b> <b>&lt;network-dest-</b> <b>ip&gt;&lt;mask&gt;</b></p>	<ul style="list-style-type: none"> <li>- Destination IP address can be             <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is destined for and the network mask to use with the destination IP address</li> </ul> </li> </ul>
<b>priority</b>		<ul style="list-style-type: none"> <li>- Priority of the L2 filter. This is used to decide which filter rule is applicable,             <ul style="list-style-type: none"> <li>• when the packet matches with more than one filter rules.</li> <li>• All the filter rules result in allowing the packet.</li> </ul> </li> </ul> <p>Higher value of filter priority implies a higher priority              This value ranges between 1 and 255.</p>

**Mode** ACL Standard Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** priority - 1

**Example** `iss(config-std-nacl)# deny host 100.0.0.10 any`

- Related Commands**
- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
  - **permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters
  - **show access-lists** -Displays the access list configuration

## 65.1.10 copy-to-cpu - standard mode

This command copies the IP control packets to control plane CPU with or without switching of packets based on the configured parameters.

```
copy-to-cpu { any | host <src-ip-address> | <src-ip-address> <mask> } [ { any
| host <dest-ip-address> | <dest-ip-address> <mask> } ] [noswitching]
```

### For Metro

```
copy-to-cpu { any | host <src-ip-address> | <network-src-ip> <mask> } [ { any
| host <dest-ip-address> | <network-dest-ip> <mask> } ] [noswitching]
```

**Syntax Description**

**any | host <src-ip-address> | <src-ip-address> <mask>** - Copies the IP control packets to control plane CPU with or without switching of packets based on the following source address configuration:

- any - Copies all control packets. Does not check for the source IP address in the packets.
- host - Copies only the control packets having the specified unicast host network IP address as the source address.
- <src-ip-address> <mask> - Copies only the control packets having the specified unicast source IP address and mask.

**any | host <dest-ip-address> | <dest-ip-address> <mask>** - Copies the IP control packets to control plane CPU with or without switching of packets based on the following destination address configuration:

- any - Copies all control packets. Does not check for the destination IP address in the packets.
- host - Copies only the control packets having the specified host network IP address as the destination address.
- <dest-ip-address> <mask> - Copies only the control packets having the specified destination IP address and mask.

**noswitching** - Copies the IP control packets to control plane CPU without switching of packets.

**Mode** ACL Standard Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** any | host <src-ip- - any

address> | <src-ip-  
address> <mask>

any | host <dest-ip-        -     any  
address> | <dest-ip-  
address> <mask>

**Example**     iss(config-std-nacl)# copy-to-cpu host 30.0.0.4 any  
noswitching



This command is available, only if the switch NPAPI\_WANTED or QOSX\_WANTED is set as yes during compilation of the exe.

**Related  
Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access lists configuration.

## 65.1.11 permit- ip/ospf/pim/protocol type

This command allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.

```
permit { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-
address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-
address> <mask> } [ {tos{max-reliability | max-throughput | min-delay | normal
|<value (0-7)>} | dscp {<value (0-63)> | af11 | af12 | af13 | af21 | af22 |
af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 |
cs6 | cs7 | default | ef}} ] [priority <value (1-255)>] [ForQoS] [{precedence
(0-7)> | fragments | log | log-input | reflect <access list> | time-range
<value>}] [redirect {interface <ifXtype> <ifnum> | <ifXtype><iface_list>
[<ifXtype><iface_list>] load-balance {src-ip | dst-ip | src-mac | dst-mac |
vlanid | src-tcpport | dst-tcpport | src-udpport | dst-udpport}}] [sub-action
{none | modify-vlan<short (1-4094)> | nested-vlan <short (1 -4094)>}]
```

### For Metro

```
permit { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-
address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-
address> <mask> } [ {tos{max-reliability | max-throughput | min-delay | normal
|<value (0-7)>} | dscp <value (0-63)> } ] [ priority <value (1-255)>] [ svlan-
id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-
4094)>] [ cvlan-priority <value (0-7)>] [ { single-tag | double-tag } ]
[ForQoS][redirect {interface <ifXtype> <ifnum> | <ifXtype><iface_list>
[<ifXtype><iface_list>] load-balance {src-ip | dst-ip | src-mac | dst-mac |
vlanid | src-tcpport | dst-tcpport | src-udpport | dst-udpport}}] [sub-action
{none | modify-vlan<short (1-4094)> | nested-vlan <short (1 -4094)>}]
```

<b>Syntax</b>	ip  ospf pim	-	Type of protocol for the packet. It can also be a protocol number.
<b>Description</b>	<protocol-type (1-255)>		
	any  host	-	Source IP address can be
	<src-ip-address>		
	<src-ip-address>		
	<mask>		
	any host	-	Destination IP address can be
	<dest-ip-address>		
	<dest-ip-address>		
	<mask>		

with the destination address

- tos**
- Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7.
- dscp**
- Differentiated services code point provides the quality of service control. The various options available are:
    - 0-63 - Differentiated services code point value
- The parameters newly added in the existing commands for industry standard CLI are:
- af11 - Matches packets with AF11 DSCP (001010)
  - af12 - Matches packets with AF12 DSCP (001100)
  - af13 - Matches packets with AF13 DSCP (001110)
  - af21 - Matches packets with AF21 DSCP (010010)
  - af22 - Matches packets with AF22 DSCP (010100)
  - af23 - Matches packets with AF23 DSCP (010110)
  - af31 - Matches packets with AF31 DSCP (011010)
  - af32 - Matches packets with AF32 DSCP (011100)
  - af33 - Matches packets with AF33 DSCP (011110)
  - af41 - Matches packets with AF41 DSCP (100010)
  - af42 - Matches packets with AF42 DSCP (100100)
  - af43 - Matches packets with AF43 DSCP (100110)
  - cs1 - Matches packets with CS1 (precedence 1) DSCP (001000)
  - cs2 - Matches packets with CS2 (precedence 2) DSCP (010000)
  - cs3 - Matches packets with CS3 (precedence 3) DSCP (011000)
  - cs4 - Matches packets with CS4 (precedence 4) DSCP (100000)
  - cs5 - Matches packets with CS5 (precedence 5) DSCP (101000)
  - cs6 - Matches packets with CS6 (precedence 6) DSCP (110000)
  - cs7 - Matches packets with CS7 (precedence 7) DSCP (111000)
  - default - Default DSCP (000000)
  - ef - Matches packets with EF DSCP (101110)
- priority**
- The priority of the L3 filter is used to decide which filter

- rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
- svlan-id** - Service VLAN value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.
- ForQoS** - The configuration done is made available for the QoS rules also.
- precedence<sup>1</sup>** - Precedence level to be used for filtering packets. This parameter is newly added in the existing command for industry standard CLI. The values are:
- 0 - Matches packets with routine precedence.
  - 1 - Matches packets with priority precedence.
  - 2 - Matches packets with immediate precedence.
  - 3 - Matches packets with flash precedence.
  - 4 - Matches packets with flash override precedence.
  - 5 - Matches packets with critical precedence.
  - 6 - Matches packets with internetwork control precedence.
  - 7 - Matches packets with network control precedence.
- fragments** - Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry.
- This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

---

<sup>1</sup> This value will always be 1. User cannot configure this value.

---

<b>log</b>	<ul style="list-style-type: none"><li>- Creates informational logging message about the packets that match the entry to be sent to the console. This message includes the access list number, whether the packet is permitted or denied; the protocol, whether the protocol is TCP (Transport Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), or a number; and if appropriate, the source and destination addresses and source and destination port numbers. This message is generated for the first packet that matches a flow. This message is then generated at 5-minute intervals with the number of packets permitted or denied in the prior 5-minute interval. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.</li></ul>
<b>log-input</b>	<ul style="list-style-type: none"><li>- Creates information logging message along with the information about the input interface. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.</li></ul>
<b>reflect</b>	<ul style="list-style-type: none"><li>- Name of the reflexive access list. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.</li></ul>
<b>time-range</b>	<ul style="list-style-type: none"><li>- Name of the time range to be applied. Time range defines the time when the permit or deny statements of the Access Control List are in effect. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.</li></ul>
<b>redirect</b>	<p>Redirects the action to the destination interface or set of interfaces.</p> <ul style="list-style-type: none"><li>• ifXtype – Specifies the interface type</li><li>• ifnum – Specifies the interface number</li><li>• iface_list – Specifies the list of interfaces</li></ul>
<b>load-balance</b>	<p>Specifies the parameters based on which the traffic distribution needs to be done. Options are:</p> <ul style="list-style-type: none"><li>• src-ip</li><li>• dst-ip</li><li>• src-mac</li></ul>

- dst-mac
- vlanid
- src-tcpport
- dst-tcpport
- src-udpport
- dst-udpport

**sub-action**

Specifies the VLAN specific sub action to be performed on the packet -

- none – Actions relating to the VLAN ID will not be considered.
- modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
- nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults**

protocol-type	-	255
priority	-	1
dscp	-	-1
svlan-id	-	0
svlan-priority	-	-1
cvlan-id	-	0
cvlan-priority	-	-1
single-tag   double-tag	-	Single tag
precedence	-	1

**Example** `iss(config-ext-nacl)# permit 200 host 100.0.0.10 any tos 6 load balance src-ip`



- Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.
- Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

**Related Commands**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `deny - ip/ospf/pim/protocol type` - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- `show access-lists` - Displays the access list configuration

## 65.1.12 permit ipv6

This command specifies IP packets to be forwarded based on protocol and associated parameters.

```
permit ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr>
<integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> }} [redirect
{interface <ifXtype> <ifnum> | <ifXtype><iface_list>
[<ifXtype><iface_list>]load-balance {src-ip | dst-ip | src-mac | dst-mac |
vlanid | src-tcpport| dst-tcpport | src-udpport | dst-udpport}}][sub-action
{none | modify-vlan<short (1-4094)> | nested-vlan <short (1 -4094)>}]
[priority <short (1-255)>]
```

### For Metro

```
permit ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr>
<integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> }} [redirect
{interface <ifXtype> <ifnum> | <ifXtype><iface_list> [<ifXtype><iface_list>]
load-balance {src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport| dst-
tcpport | src-udpport | dst-udpport}}][sub-action {none | modify-vlan<short
(1-4094)> | nested-vlan <short (1 -4094)>}]
```

<b>Syntax</b>	<b>flow-label</b>	-	Flow identifier in IPv6 header.
<b>Description</b>	<b>n</b>	-	Source address of the host / any host.
	any   host <ip6_addr> <integer(0-128)>	-	Destination address of the host / any host.
	any   host <ip6_addr> <integer(0-128)>	-	Destination address of the host / any host.
	<b>redirect</b>	-	Redirects the action to the destination interface or set of interfaces. <ul style="list-style-type: none"> <li>• ifXtype – Specifies the interface type</li> <li>• ifnum – Specifies the interface number</li> <li>• iface_list – Specifies the list of interfaces</li> </ul>
	<b>load-balance</b>	-	Specifies the parameters based on which the traffic distribution needs to be done. Options are: <ul style="list-style-type: none"> <li>• src-ip</li> <li>• dst-ip</li> <li>• src-mac</li> <li>• dst-mac</li> <li>• vlanid</li> <li>• src-tcpport</li> <li>• dst-tcpport</li> </ul>

	<ul style="list-style-type: none"> <li>• src-udpport</li> <li>• dst-udpport</li> </ul>
<b>sub-action</b>	<ul style="list-style-type: none"> <li>- Specifies the VLAN specific sub action to be performed on the packet -           <ul style="list-style-type: none"> <li>• none – Actions relating to the VLAN ID will not be considered.</li> <li>• modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</li> <li>• nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.</li> </ul> </li> </ul>
<b>priority</b>	<ul style="list-style-type: none"> <li>- Priority of the L2 filter. This is used to decide which filter rule is applicable,           <ul style="list-style-type: none"> <li>• when the packet matches with more than one filter rules.</li> <li>• All the filter rules result in allowing the packet.</li> </ul> </li> </ul> <p>Higher value of filter priority implies a higher priority This value ranges between 1 and 255.</p>
<b>Mode</b>	ACL Extended Access List Configuration Mode
<b>Package</b>	Workgroup, Enterprise and Metro
<b>Defaults</b>	priority - 1
<b>Example</b>	<pre>iss(config-ext-nacl)# permit ipv6 host c004::04 28 any load-balance src-ip</pre>
	Flow label cannot be configured along with either source/destination IP address.
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• <b>ip access-list</b> - Creates IP ACLs and enters the IP Access-list configuration mode</li> <li>• <b>show access-lists</b> - Displays the access lists configuration.</li> </ul>

## 65.1.13 deny - ip/ospf/pim/protocol type

This command denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.

```
deny { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp {<value (0-63)> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef}} ] [ priority <value (1-255)>] [{precedence (0-7)> | fragments | log | log-input | reflect <access list> | time-range <value> } ]
```

### For Metro

```
deny { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>} ] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value (0-7)>] [ { single-tag | double-tag } ]
```

<b>Syntax Description</b>	ip  ospf pim  <protocol-type (1-255)>	- Type of protocol for the packet. It can also be a protocol number.
	any  host <src-ip-address>  <src-ip-address> <mask>	- Source IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul>
	any host <dest-ip-address>  <dest-ip-address> <mask>	- Destination IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul>
	tos	- Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7.

**dscp**

- Differentiated services code point provides the quality of service control. The various options available are:
  - 0-63 - Differentiated services code point value

The parameters newly added in the existing commands for industry standard CLI are:

- af11 - Matches packets with AF11 DSCP (001010)
- af12 - Matches packets with AF12 DSCP (001100)
- af13 - Matches packets with AF13 DSCP (001110)
- af21 - Matches packets with AF21 DSCP (010010)
- af22 - Matches packets with AF22 DSCP (010100)
- af23 - Matches packets with AF23 DSCP (010110)
- af31 - Matches packets with AF31 DSCP (011010)
- af32 - Matches packets with AF32 DSCP (011100)
- af33 - Matches packets with AF33 DSCP (011110)
- af41 - Matches packets with AF41 DSCP (100010)
- af42 - Matches packets with AF42 DSCP (100100)
- af43 - Matches packets with AF43 DSCP (100110)
- cs1 - Matches packets with CS1 (precedence 1) DSCP (001000)
- cs2 - Matches packets with CS2 (precedence 2) DSCP (010000)
- cs3 - Matches packets with CS3 (precedence 3) DSCP (011000)
- cs4 - Matches packets with CS4 (precedence 4) DSCP (100000)
- cs5 - Matches packets with CS5 (precedence 5) DSCP (101000)
- cs6 - Matches packets with CS6 (precedence 6) DSCP (110000)
- cs7 - Matches packets with CS7 (precedence 7) DSCP (111000)
- default - Default DSCP (000000)
- ef - Matches packets with EF DSCP (101110)

**priority**

- The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

**svlan-id**

- Service VLAN value to match against incoming packets.

- 
- |                               |   |
|-------------------------------|---|
| <b>svlan-priority</b>         | - Service VLAN priority value to match against incoming packets.  |
| <b>cvlan-id</b>               | - Customer VLAN value to match against incoming packets.  |
| <b>cvlan-priority</b>         | - Customer VLAN priority value to match against incoming packets.   |
| <b>single-tag</b>             | - Filter to be applied on Single VLAN tagged packets.   |
| <b>double-tag</b>             | - Filter to be applied on double VLAN tagged packets.   |
| <b>precedence<sup>1</sup></b> | - Precedence level to be used for filtering packets.<br>This parameter is newly added in the existing command for industry standard CLI.<br>The values are: <ul style="list-style-type: none"><li>• 0 - Matches packets with routine precedence.</li><li>• 1 - Matches packets with priority precedence.</li><li>• 2 - Matches packets with immediate precedence.</li><li>• 3 - Matches packets with flash precedence.</li><li>• 4 - Matches packets with flash override precedence.</li><li>• 5 - Matches packets with critical precedence.</li><li>• 6 - Matches packets with internetwork control precedence.</li><li>• 7 - Matches packets with network control precedence.</li></ul> |
| <b>fragments</b>              | - Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry.<br>This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.   |
| <b>log</b>                    | - Creates informational logging message about the packets that match the entry to be sent to the console.<br>This message includes the access list number, whether the packet is permitted or denied; the protocol, whether the protocol is TCP (Transport Control Protocol), UDP (User Datagram Protocol),   |

ICMP (Internet Control Message Protocol), or a number; and if appropriate, the source and destination addresses and source and destination port numbers.

This message is generated for the first packet that matches a flow. This message is then generated at 5-minute intervals with the number of packets permitted or denied in the prior 5-minute interval.

This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

**log-input**

- Creates information logging message along with the information about the input interface.

This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

**reflect**

- Name of the reflexive access list.

This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

**time-range**

- Name of the time range to be applied.

Time range defines the time when the permit or deny statements of the Access Control List are in effect.

This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults**

protocol type	-	255
priority	-	1
dscp	-	-1
svlan-id	-	0
svlan-priority	-	-1
cvlan-id	-	0

cvlan-priority	-	-1
single-tag   double-tag	-	Single tag
precedence	-	1

**Example** `iss(config-ext-nacl)# deny ospf any host 10.0.0.1 tos max-throughput`



- Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.
- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

**Related Commands**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit- ip/ospf/pim/protocol type` - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- `show access-lists` -Displays the access list configuration

## 65.1.14 copy-to-cpu - ip / ospf / pim / protocol-type

This command copies the IP control packets of all type of protocols to control plane CPU with or without switching of packets based on the configured parameters.

```
copy-to-cpu { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-
address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-
ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay |
normal |<value (0-7)>} | dscp <value (0-63)>} ] [priority <value (1-255)>]
[noswitching]
```

### For Metro

```
copy-to-cpu { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-
address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-
ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay |
normal |<value (0-7)>} | dscp <value (0-63)>} ] [ priority <value (1-255)>] [
svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-
id (1-4094)>] [ cvlan-priority <value (0-7)>] [ { single-tag | double-tag } ]
[noswitching]
```

<b>Syntax Description</b>	<pre>ip   ospf   pim   &lt;protocol-type (1-255)&gt;</pre>	<ul style="list-style-type: none"> <li>- Copies the IP control packets to control plane CPU with or without switching of packets based on the following protocol type configuration: <ul style="list-style-type: none"> <li>• ip - Copies only the control packets of IP protocol.</li> <li>• ospf - Copies only the control packets of OSPF protocol.</li> <li>• pim - Copies only the control packets of PIM protocol.</li> <li>• &lt;protocol-type (1-255)&gt; - Copies only the control packets of administrator specified protocol type. This value ranges between 1 and 255.</li> </ul> </li> </ul>
<b>Syntax Description</b>	<pre>any   host &lt;src-ip-address&gt;   &lt;src-ip-address&gt; &lt;mask&gt;</pre>	<ul style="list-style-type: none"> <li>- Copies the IP control packets to control plane CPU with or without switching of packets based on the following source address configuration: <ul style="list-style-type: none"> <li>• any - Copies all control packets. Does not check for the source IP address in the packets.</li> <li>• host - Copies only the control packets having the specified unicast host network IP address as the source address.</li> <li>• &lt;src-ip-address&gt; &lt;mask&gt; - Copies only the control packets having the specified unicast source IP address and mask.</li> </ul> </li> </ul>

- ```
any | host <dest-  
ip-address> |  
<dest-ip-address>  
<mask>
```
- Copies the IP control packets to control plane CPU with or without switching of packets based on the following destination address configuration:
    - any - Copies all control packets. Does not check for the destination IP address in the packets.
    - host - Copies only the control packets having the specified host IP address as the destination address.
    - <dest-ip-address> <mask> - Copies only the control packets having the specified destination IP address and mask.
- tos
- Copies the IP control packets to control plane CPU with or without switching of packets based on the following type of service configuration:
    - max-reliability - Copies only the control packets having TOS field set as high reliability.
    - max-throughput - Copies only the control packets having TOS field set as high throughput.
    - min-delay - Copies only the control packets having TOS field set as low delay.
    - normal - Copies all control packets. Does not check for the TOS field in the packets.
    - <value (0-7)> - Copies the control packets based on the TOS value set. The value ranges between 0 and 7. This value represents different combination of TOS.
      - 0 - Copies all control packets. Does not check for the TOS field in the packets.
      - 1 - Copies only the control packets having TOS field set as high reliability.
      - 2 - Copies only the control packets having TOS field set as high throughput.
      - 3 - Copies the control packets having TOS field set either as high reliability or high throughput.
      - 4 - Copies only the control packets having TOS field set as low delay.
      - 5 - Copies the control packets having TOS field set either as low delay or high reliability.
      - 6 - Copies the control packets having TOS field set either as low delay or high throughput.
      - 7 - Copies the control packets having TOS field set either as low delay or high reliability

or high throughput.

- |                                        |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dscp</b>                            | - | <p>Copies only the control packets having the specified DSCP value.</p> <p>This value ranges between 0 and 63.</p>                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>priority</b>                        | - | <p>Copies only the control packets having the specified L2 priority value.</p> <p>This value ranges between 1 and 255.</p>                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>svlan-id</b>                        | - | <p>Copies only the IP control packets having the specified service VLAN ID / outer VLAN ID / VLAN ID provided in outer tag.</p> <p>This value ranges between 1 and 4094.</p>                                                                                                                                                                                                                                                                                                                                         |
| <b>svlan-priority</b>                  | - | <p>Copies only the IP control packets having the specified service VLAN priority / outer VLAN priority / VLAN priority provided in outer tag.</p> <p>This value ranges between 0 and 7.</p>                                                                                                                                                                                                                                                                                                                          |
| <b>cvlan-id</b>                        | - | <p>Copies only the IP control packets having the specified customer VLAN ID / inner VLAN ID / VLAN ID provided in inner tag.</p> <p>This value ranges between 1 and 4094.</p>                                                                                                                                                                                                                                                                                                                                        |
| <b>cvlan-priority</b>                  | - | <p>Copies only the IP control packets having the specified customer VLAN priority / inner VLAN priority / VLAN priority provided in inner tag.</p> <p>This value ranges between 0 and 7.</p>                                                                                                                                                                                                                                                                                                                         |
| <b>single-tag</b><br><b>double-tag</b> | - | <p>Copies the IP control packets to control plane CPU with or without switching of packets based on the following packet tag type configuration:</p> <ul style="list-style-type: none"> <li>• single-tag - Copies only the single VLAN tagged packets.</li> <li>• double-tag - Copies only the double VLAN tagged packets.</li> </ul> <p>The tag type is set as double-tag and cannot be configured, if any one of the parameter service VLAN ID, service VLAN priority or customer VLAN priority is configured.</p> |
| <b>noswitching</b>                     | - | <p>Copies the IP control packets to control plane CPU without switching of packets.</p>                                                                                                                                                                                                                                                                                                                                                                                                                              |

|                 |                                                         |                                                                         |
|-----------------|---------------------------------------------------------|-------------------------------------------------------------------------|
| <b>Mode</b>     | ACL Extended Access List Configuration Mode             |                                                                         |
| <b>Package</b>  | Workgroup, Enterprise and Metro                         |                                                                         |
| <b>Defaults</b> | ip   ospf   pim  <br><protocol-type (1-255)>            | - Control packets of all type of protocols are copied.                  |
|                 | any   host <src-ip-address>   <src-ip-address> <mask>   | - any                                                                   |
|                 | any   host <dest-ip-address>   <dest-ip-address> <mask> | - any                                                                   |
|                 | dscp                                                    | - -1 (that is, the packets are not checked for DSCP value)              |
|                 | priority                                                | - 1                                                                     |
|                 | svlan-id                                                | - 0 (that is, the packets are not checked for service VLAN identifier)  |
|                 | svlan-priority                                          | - -1 (that is, the packets are not checked for service VLAN priority)   |
|                 | cvlan-id                                                | - 0 (that is, the packets are not checked for customer VLAN identifier) |
|                 | cvlan-priority                                          | - -1 (that is, the packets are not checked for customer VLAN priority)  |
|                 | single-tag   double-tag                                 | - single-tag                                                            |

**Example** `iss(config-ext-nacl)# copy-to-cpu ospf host 30.0.0.4 any tos min-delay priority 2`



This command is available, only if the switch NPAPI\_WANTED or QOSX\_WANTED is set as yes during compilation of the exe.

- Related Commands**
- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
  - `show access-lists` - Displays the access lists configuration.

## 65.1.15 deny ipv6

This command specifies IPv6 packets to be rejected based on protocol and associated parameters.

```
deny ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr> <integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> }} [priority <short (1-255)>]
```

|                           |                                                           |   |                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------|-----------------------------------------------------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>flow-label</b>                                         | - | Flow identifier in IPv6 header.                                                                                                                                                                                                                                                                                                                                  |
|                           | <b>any   host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</b> | - | Source address of the host / any host.                                                                                                                                                                                                                                                                                                                           |
|                           | <b>any   host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</b> | - | Destination address of the host / any host.                                                                                                                                                                                                                                                                                                                      |
|                           | <b>priority</b>                                           | - | Priority of the L2 filter. This is used to decide which filter rule is applicable, <ul style="list-style-type: none"> <li>• when the packet matches with more than one filter rules.</li> <li>• All the filter rules result in allowing the packet.</li> </ul> Higher value of filter priority implies a higher priority<br>This value ranges between 1 and 255. |

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** priority - 1

**Example**

```
iss(config-ext-nacl)# deny ipv6 host c004::04 28 any
iss(config-ext-nacl)# deny ipv6 flow-label 40
```

 Flow label cannot be configured along with either source/destination IP address.

- Related Commands**
- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
  - **show access-lists** - Displays the access lists configuration.

## 65.1.16 copy-to-cpu ipv6

This command copies the IPv6 control packets to control plane CPU with or without switching of packets based on the configured parameters.

```
copy-to-cpu ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr>
<integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> }} [noswitching]
```

|                           |                                                           |   |                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|-----------------------------------------------------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>flow-label</b>                                         | - | Copies only the IPv6 control packets having the specified flow identifier.<br>This value ranges between 1 and 65535.                                                                                                                                                                                                                                                                                                         |
|                           | <b>any   host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</b> | - | Copies the IPv6 control packets to control plane CPU with or without switching of packets based on the following source address configuration: <ul style="list-style-type: none"> <li>• any - Copies all control packets. Does not check for the source IPv6 address in the packets.</li> <li>• host - Copies only the control packets having the specified source IPv6 address and prefix length.</li> </ul>                |
|                           | <b>any   host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</b> | - | Copies the IPv6 control packets to control plane CPU with or without switching of packets based on the following destination address configuration: <ul style="list-style-type: none"> <li>• any - Copies all control packets. Does not check for the destination IPv6 address in the packets.</li> <li>• host - Copies only the control packets having the specified destination IPv6 address and prefix length.</li> </ul> |
|                           | <b>noswitching</b>                                        | - | Copies the IPv6 control packets to control plane CPU without switching of packets.                                                                                                                                                                                                                                                                                                                                           |

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** flow-label - 0 (that is, the packets are not checked for flow identifier)

any | host <ip6\_addr> <integer(0-128)> - any

**Example** iss(config-ext-nacl)# copy-to-cpu ipv6 flow-label 40



This command is available, only if the switch NPAPI\_WANTED or QOSX\_WANTED is set as yes during compilation of the exe.

**Related  
Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access lists configuration.

## 65.1.17 permit tcp

This command specifies the TCP packets to be forwarded based on the associated parameters.

```
permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)>|eq <port-number (1-
65535)> |range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp {<value (0-
63)> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 |
af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef}}] [
priority <short(1-255)>] [ForQoS] [{precedence <short(0-7)> | fragments | log
| log-input | reflect <access-list> | time-range <value>}] [redirect
{interface <ifXtype> <ifnum> | <ifXtype><iface_list>
[<ifXtype><iface_list>]load-balance {src-ip | dst-ip | src-mac | dst-mac |
vlanid | src-tcpport| dst-tcpport | src-udpport | dst-udpport}}] [sub-action
{none | modify-vlan<short (1-4094)> | nested-vlan <short (1 -4094)>}]
```

### For Metro

```
permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)>|eq <port-number (1-
65535)> |range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp <value (0-
63)>}] [ priority <short(1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-
priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value
(0-7)>] [ { single-tag | double-tag } ] [ForQoS] [redirect {interface
<ifXtype> <ifnum> | <ifXtype><iface_list> [<ifXtype><iface_list>]load-balance
{src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport| dst-tcpport |
src-udpport | dst-udpport}}] [sub-action {none | modify-vlan<short (1-4094)>
| nested-vlan <short (1 -4094)>}]
```

|                           |                                                                    |   |                                                                                                                                                                                                                                                                 |
|---------------------------|--------------------------------------------------------------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>tcp</b>                                                         | - | Transport Control Protocol                                                                                                                                                                                                                                      |
| <b>n</b>                  | any  host<br><src-ip-address> <br><src-ip-address> <<br>src-mask > | - | Source IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the dotted decimal address OR</li> <li>• the IP address of the network or the host that the packet is from and the network mask to use with the source address</li> </ul> |
|                           | port-number                                                        | - | Port Number. The input for the source and the                                                                                                                                                                                                                   |

- destination port-number is prefixed with one of the following operators.
- eq=equal
  - lt=less than
  - gt=greater than
  - range=a range of ports; two different port numbers must be specified
- any|host**
- `<dest-ip-address>`  
`|<dest-ip-address>`  
`< dest-mask >`
- Destination IP address can be
    - 'any' or
    - the dotted decimal address or
    - the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address
- ack**
- TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3).
- rst**
- TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3).
- tos**
- Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7.
- dscp**
- Differentiated services code point provides the quality of service control. The various options available are:
    - 0-63 - Differentiated services code point value

The parameters newly added in the existing commands for industry standard CLI are:

    - af11 - Matches packets with AF11 DSCP (001010)
    - af12 - Matches packets with AF12 DSCP (001100)
    - af13 - Matches packets with AF13 DSCP (001110)
    - af21 - Matches packets with AF21 DSCP (010010)
    - af22 - Matches packets with AF22 DSCP (010100)
    - af23 - Matches packets with AF23 DSCP (010110)
    - af31 - Matches packets with AF31 DSCP (011010)
    - af32 - Matches packets with AF32 DSCP (011100)
    - af33 - Matches packets with AF33 DSCP (011110)
    - af41 - Matches packets with AF41 DSCP (100010)
    - af42 - Matches packets with AF42 DSCP (100100)

- af43 - Matches packets with AF43 DSCP (100110)
- cs1 - Matches packets with CS1 (precedence 1) DSCP (001000)
- cs2 - Matches packets with CS2 (precedence 2) DSCP (010000)
- cs3 - Matches packets with CS3 (precedence 3) DSCP (011000)
- cs4 - Matches packets with CS4 (precedence 4) DSCP (100000)
- cs5 - Matches packets with CS5 (precedence 5) DSCP (101000)
- cs6 - Matches packets with CS6 (precedence 6) DSCP (110000)
- cs7 - Matches packets with CS7 (precedence 7) DSCP (111000)
- default - Default DSCP (000000)
- ef - Matches packets with EF DSCP (101110)

- priority** - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
- svlan-id** - Service VLAN value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.
- ForQoS** - The configuration done is made available for the QoS rules also.
- precedence<sup>1</sup>** - Precedence level to be used for filtering packets. This parameter is newly added in the existing

command for industry standard CLI.

The values are:

- 0 - Matches packets with routine precedence.
- 1 - Matches packets with priority precedence.
- 2 - Matches packets with immediate precedence.
- 3 - Matches packets with flash precedence.
- 4 - Matches packets with flash override precedence.
- 5 - Matches packets with critical precedence.
- 6 - Matches packets with internetwork control precedence.
- 7 - Matches packets with network control precedence.

#### **fragments**

- Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

#### **log**

- Creates informational logging message about the packets that match the entry to be sent to the console.  
This message includes the access list number, whether the packet is permitted or denied; the protocol, whether the protocol is TCP (Transport Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), or a number; and if appropriate, the source and destination addresses and source and destination port numbers.  
This message is generated for the first packet that matches a flow. This message is then generated at 5-minute intervals with the number of packets permitted or denied in the prior 5-minute interval.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

#### **log-input**

- Creates information logging message along with the information about the input interface.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

#### **reflect**

- Name of the reflexive access list.  
This feature has been included to adhere to the

---

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | Industry Standard CLI syntax. This feature is currently not supported.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>time-range</b>   | <ul style="list-style-type: none"> <li>- Name of the time range to be applied.</li> </ul> <p>Time range defines the time when the permit or deny statements of the Access Control List are in effect.</p> <p>This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.</p>                                                                                                                                                |
| <b>redirect</b>     | <ul style="list-style-type: none"> <li>- Redirects the action to the destination interface or set of interfaces. <ul style="list-style-type: none"> <li>• ifXtype – Specifies the interface type</li> <li>• ifnum – Specifies the interface number</li> <li>• iface_list – Specifies the list of interfaces</li> </ul> </li> </ul>                                                                                                                                                     |
| <b>load-balance</b> | <ul style="list-style-type: none"> <li>- Specifies the parameters based on which the traffic distribution needs to be done. Options are: <ul style="list-style-type: none"> <li>• src-ip</li> <li>• dst-ip</li> <li>• src-mac</li> <li>• dst-mac</li> <li>• vlanid</li> <li>• src-tcpport</li> <li>• dst-tcpport</li> <li>• src-udpport</li> <li>• dst-udpport</li> </ul> </li> </ul>                                                                                                  |
| <b>sub-action</b>   | <ul style="list-style-type: none"> <li>- Specifies the VLAN specific sub action to be performed on the packet - <ul style="list-style-type: none"> <li>• none – Actions relating to the VLAN ID will not be considered.</li> <li>• modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</li> <li>• nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.</li> </ul> </li> </ul> |
| <b>Mode</b>         | ACL Extended Access List Configuration Mode                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Package</b>      | Workgroup, Enterprise and Metro                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                 |                         |   |                                                                                     |
|-----------------|-------------------------|---|-------------------------------------------------------------------------------------|
| <b>Defaults</b> | tos-value               | - | 0                                                                                   |
|                 | ack                     | - | 'any' (3) [indicates that the TCP ACK bit will not be checked to decide the action] |
|                 | rst                     | - | 'any' (3) [indicates that the TCP RST bit will not be checked to decide the action] |
|                 | dscp                    | - | -1                                                                                  |
|                 | priority                | - | 1                                                                                   |
|                 | svlan-id                | - | 0                                                                                   |
|                 | svlan-priority          | - | -1                                                                                  |
|                 | cvlan-id                | - | 0                                                                                   |
|                 | cvlan-priority          | - | -1                                                                                  |
|                 | single-tag   double-tag | - | Single tag                                                                          |
|                 | precedence              | - | 1                                                                                   |

**Example** `iss(config-ext-nacl)# permit tcp any 10.0.0.1 load-balance scr-ip`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `deny tcp` - Specifies the TCP packets to be rejected based on the associated parameters
- `show access-lists` - Displays the access list configuration

## 65.1.18 deny tcp

This command specifies the TCP packets to be rejected based on the associated parameters.

```
deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }[[gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>]]{ any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> }[[gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range
<port-number (1-65535)> <port-number (1-65535)>]]{{ ack | rst }}[[tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp {<value
(0-63)> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41
| af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef} }} [
priority <short (1-255)>] [{precedence (0-7)> | fragments | log | log-input |
reflect <access-list> | time-range <value> }]
```

### For Metro

```
deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }[[gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>]]{ any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> }[[gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range
<port-number (1-65535)> <port-number (1-65535)>]]{{ ack | rst }}[[tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value
(0-63)>]] [ priority <short (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-
priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value
(0-7)>] [ { single-tag | double-tag } ]
```

|                    |                                                                                                       |   |                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | tcp                                                                                                   | - | Transmission control protocol                                                                                                                                                                                                                                                                       |
| <b>Description</b> | <p>any  host</p> <p>&lt;src-ip-address&gt; </p> <p>&lt;src-ip-address&gt;</p> <p>&lt;src-mask&gt;</p> | - | <p>Source IP address can be</p> <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul>                  |
|                    | port-number                                                                                           | - | <p>Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.</p> <ul style="list-style-type: none"> <li>• eq=equal</li> <li>• lt=less than</li> <li>• gt=greater than</li> <li>• range=a range of ports; two different port</li> </ul> |

numbers must be specified

- any|host** - Destination IP address can be
- <dest-ip-address>|**
- <dest-ip-address>**
- <dest-mask>**
- 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is destined for and the network mask to use with the destination address
- ack** - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3)
- rst** - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3)
- tos** - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7.
- dscp** - Differentiated services code point provides the quality of service control. The various options available are:
- 0-63 - Differentiated services code point value
- The parameters newly added in the existing commands for industry standard CLI are:
- af11 - Matches packets with AF11 DSCP (001010)
  - af12 - Matches packets with AF12 DSCP (001100)
  - af13 - Matches packets with AF13 DSCP (001110)
  - af21 - Matches packets with AF21 DSCP (010010)
  - af22 - Matches packets with AF22 DSCP (010100)
  - af23 - Matches packets with AF23 DSCP (010110)
  - af31 - Matches packets with AF31 DSCP (011010)
  - af32 - Matches packets with AF32 DSCP (011100)
  - af33 - Matches packets with AF33 DSCP (011110)
  - af41 - Matches packets with AF41 DSCP

- (100010)
- af42 - Matches packets with AF42 DSCP (100100)
  - af43 - Matches packets with AF43 DSCP (100110)
  - cs1 - Matches packets with CS1 (precedence 1) DSCP (001000)
  - cs2 - Matches packets with CS2 (precedence 2) DSCP (010000)
  - cs3 - Matches packets with CS3 (precedence 3) DSCP (011000)
  - cs4 - Matches packets with CS4 (precedence 4) DSCP (100000)
  - cs5 - Matches packets with CS5 (precedence 5) DSCP (101000)
  - cs6 - Matches packets with CS6 (precedence 6) DSCP (110000)
  - cs7 - Matches packets with CS7 (precedence 7) DSCP (111000)
  - default - Default DSCP (000000)
  - ef - Matches packets with EF DSCP (101110)
- priority** - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
- svlan-id** - Service VLAN value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

- precedence<sup>1</sup>**
- Precedence level to be used for filtering packets. This parameter is newly added in the existing command for industry standard CLI. The values are:
    - 0 - Matches packets with routine precedence.
    - 1 - Matches packets with priority precedence.
    - 2 - Matches packets with immediate precedence.
    - 3 - Matches packets with flash precedence.
    - 4 - Matches packets with flash override precedence.
    - 5 - Matches packets with critical precedence.
    - 6 - Matches packets with internetwork control precedence.
    - 7 - Matches packets with network control precedence.
- fragments**
- Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- log**
- Creates informational logging message about the packets that match the entry to be sent to the console. This message includes the access list number, whether the packet is permitted or denied; the protocol, whether the protocol is TCP (Transport Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), or a number; and if appropriate, the source and destination addresses and source and destination port numbers. This message is generated for the first packet that matches a flow. This message is then generated at 5-minute intervals with the number of packets permitted or denied in the prior 5-minute interval. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- log-input**
- Creates information logging message along with the information about the input interface. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is

currently not supported.

**reflect**

- Name of the reflexive access list.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

**time-range**

- Name of the time range to be applied.  
Time range defines the time when the permit or deny statements of the Access Control List are in effect.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

|                 |                         |   |                                                                                 |
|-----------------|-------------------------|---|---------------------------------------------------------------------------------|
| <b>Defaults</b> | tos-value               | - | 0                                                                               |
|                 | ack                     | - | 'any' (3) [indicates that TCP ACK bit will not be checked to decide the action] |
|                 | rst                     | - | 'any' (3) [indicates that TCP RST bit will not be checked to decide the action] |
|                 | dscp                    | - | -1                                                                              |
|                 | priority                | - | 1                                                                               |
|                 | svlan-id                | - | 0                                                                               |
|                 | svlan-priority          | - | -1                                                                              |
|                 | cvlan-id                | - | 0                                                                               |
|                 | cvlan-priority          | - | -1                                                                              |
|                 | single-tag   double-tag | - | Single tag                                                                      |
|                 | precedence              | - | 1                                                                               |

**Example**    `iss(config-ext-nacl)# deny tcp 100.0.0.10 255.255.255.0 eq 20  
any`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

**Related  
Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters
- **show access-lists** - Displays the access list configuration

## 65.1.19 copy-to-cpu tcp

This command copies the TCP control packets to control plane CPU with or without switching of packets based on the configured parameters.

```
copy-to-cpu tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }
[<gt; <port-number (1-65535)> | <lt;port-number (1-65535)> | <eq <port-number (1-
65535)> | <range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [<gt; <port-number (1-
65535)> | <lt;port-number (1-65535)> | <eq <port-number (1-65535)> | <range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value (0-7)>}|dscp <value (0-
63)>}] [ priority <short(1-255)>] [noswitching]
```

### For Metro

```
copy-to-cpu tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }
[<gt; <port-number (1-65535)> | <lt;port-number (1-65535)> | <eq <port-number (1-
65535)> | <range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [<gt; <port-number (1-
65535)> | <lt;port-number (1-65535)> | <eq <port-number (1-65535)> | <range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value (0-7)>}| dscp <value
(0-63)>}] [ priority <short(1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-
priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value
(0-7)>] [ { single-tag | double-tag } ] [noswitching]
```

|                           |                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <pre>any   host &lt;src- ip-address&gt;   &lt;src-ip-address&gt; &lt;src-mask&gt;</pre> | <ul style="list-style-type: none"> <li>- Copies the TCP control packets to control plane CPU with or without switching of packets based on the following source address configuration: <ul style="list-style-type: none"> <li>• any - Copies all control packets. Does not check for the source IP address in the packets.</li> <li>• host - Copies only the control packets having the specified unicast host network IP address as the source address.</li> <li>• &lt;src-ip-address&gt; &lt;src-mask&gt; - Copies only the control packets having the specified unicast source IP address and mask.</li> </ul> </li> </ul> |
| <b>gt</b>                 |                                                                                         | <ul style="list-style-type: none"> <li>- Copies only the TCP control packets having the TCP source / destination port numbers greater than the specified port number.<br/>This value ranges between 1 and 65535.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>lt</b>                 |                                                                                         | <ul style="list-style-type: none"> <li>- Copies only the TCP control packets having the TCP source / destination port numbers lesser than the specified port number.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                               |

- This value ranges between 1 and 65535.
- eq** - Copies only the TCP control packets having the specified TCP source / destination port numbers. This value ranges between 1 and 65535.
- range** - Copies only the TCP control packets having the TCP source / destination port numbers within the specified range. This value ranges between 1 and 65535. This value specifies the minimum port number and the maximum port number values.
- any | host <dest-ip-address> | <dest-ip-address> <dest-mask>** - Copies the TCP control packets to control plane CPU with or without switching of packets based on the following destination address configuration:
- any - Copies all control packets. Does not check for the destination IP address in the packets.
  - host - Copies only the control packets having the specified host network IP address as the destination address.
  - <dest-ip-address> <dest-mask> - Copies only the control packets having the specified destination IP address and mask.
- ack | rst** - Copies the TCP control packets to control plane CPU with or without switching of packets based on the following configuration:
- ack - Copies only the control packets having the ACK bit set.
  - rst - Copies only the control packets having the RST bit set.
- tos** - Copies the TCP control packets to control plane CPU with or without switching of packets based on the following type of service configuration:
- max-reliability - Copies only the control packets having TOS field set as high reliability.
  - max-throughput - Copies only the control packets having TOS field set as high throughput.
  - min-delay - Copies only the control packets having TOS field set as low delay.
  - normal - Copies all control packets. Does not check for the TOS field in the packets.
  - <value (0-7)> - Copies the control packets based on the TOS value set. The value ranges between 0 and 7. This value represents different

combination of TOS.

- 0 - Copies all control packets. Does not check for the TOS field in the packets.
- 1 - Copies only the control packets having TOS field set as high reliability.
- 2 - Copies only the control packets having TOS field set as high throughput.
- 3 - Copies the control packets having TOS field set either as high reliability or high throughput.
- 4 - Copies only the control packets having TOS field set as low delay.
- 5 - Copies the control packets having TOS field set either as low delay or high reliability.
- 6 - Copies the control packets having TOS field set either as low delay or high throughput.
- 7 - Copies the control packets having TOS field set either as low delay or high reliability or high throughput.

- dscp** - Copies only the TCP control packets having the specified DSCP value.  
This value ranges between 0 and 63.
- priority** - Copies only the TCP control packets having the specified L2 priority value.  
This value ranges between 1 and 255.
- svlan-id** - Copies only the TCP control packets having the specified service VLAN ID / outer VLAN ID / VLAN ID provided in outer tag.  
This value ranges between 1 and 4094.
- svlan-priority** - Copies only the TCP control packets having the specified service VLAN priority / outer VLAN priority / VLAN priority provided in outer tag.  
This value ranges between 0 and 7.
- cvlan-id** - Copies only the TCP control packets having the specified customer VLAN ID / inner VLAN ID / VLAN ID provided in inner tag.  
This value ranges between 1 and 4094.

- cvlan-priority** - Copies only the TCP control packets having the specified customer VLAN priority / inner VLAN priority / VLAN priority provided in inner tag. This value ranges between 0 and 7.
  
- single-tag** | - Copies the TCP control packets to control plane CPU with or without switching of packets based on the following packet tag type configuration:
  - **single-tag** - Copies only the single VLAN tagged packets.
  - **double-tag** - Copies only the double VLAN tagged packets.

The tag type is set as double-tag and cannot be configured, if any one of the parameter service VLAN ID, service VLAN priority or customer VLAN priority is configured.
- double-tag**
  
- noswitching** - Copies the TCP control packets to control plane CPU without switching of packets.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

- Defaults**
- any | host <src-ip-address> | <src-ip-address> <src-mask> - any
  
  - gt - 0 (that is, the packets are not checked for TCP port number)
  
  - lt - 0 (that is, the packets are not checked for TCP port number)
  
  - eq - 0 (that is, the packets are not checked for TCP port number)
  
  - range - 0 for minimum port number.  
65535 for maximum port number.
  
  - ack - any (that is, the packets are not checked for ACK bit)
  
  - rst - any (that is, the packets are not checked for RST bit)
  
  - any | host <dest-ip-

|                                          |   |                                                                       |
|------------------------------------------|---|-----------------------------------------------------------------------|
| address>   <dest-ip-address> <dest-mask> |   |                                                                       |
| dscp                                     | - | -1 (that is, the packets are not checked for DSCP value)              |
| priority                                 | - | 1                                                                     |
| svlan-id                                 | - | 0 (that is, the packets are not checked for service VLAN identifier)  |
| svlan-priority                           | - | -1 (that is, the packets are not checked for service VLAN priority)   |
| cvlan-id                                 | - | 0 (that is, the packets are not checked for customer VLAN identifier) |
| cvlan-priority                           | - | -1 (that is, the packets are not checked for customer VLAN priority)  |
| single-tag   double-tag                  | - | single-tag                                                            |

**Example**

```
iss(config-ext-nacl)# copy-to-cpu tcp any eq 300 any tos 1
priority 2 noswitching
```



- This command is available, only if the switch NPAPI\_WANTED or QOSX\_WANTED is set as yes during compilation of the exe.
- The TCP port number details can be set either for source or destination. The default value is applied for destination TCP port number, if the source TCP port number is configured or vice-versa.

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access lists configuration.

## 65.1.20 permit udp

This command specifies the UDP packets to be forwarded based on the associated parameters.

```
permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [ { gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)> } ] [ { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } ] [ { gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-
number (1-65535)> <port-number (1-65535)> } ] [ { tos { max-reliability | max-
throughput | min-delay | normal | <tos-value (0-7)> } | dscp { <value (0-63)> | af11 |
af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 |
cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef } } ] [ priority <(1-
255)> ] [ ForQoS ] [ { precedence (0-7) } | fragments | log | log-input | reflect
<access-list> | time-range <value> } ] [ redirect { interface <ifXtype> <ifnum> |
<ifXtype><iface_list> [ <ifXtype><iface_list> ] load-balance { src-ip | dst-ip |
src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport | src-udpport | dst-
udpport } } ] [ sub-action { none | modify-vlan <short (1-4094)> | nested-vlan
<short (1 -4094)> } ]
```

### For Metro

```
permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [ { gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)> } ] [ { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } ] [ { gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-
number (1-65535)> <port-number (1-65535)> } ] [ { tos { max-reliability | max-
throughput | min-delay | normal | <tos-value (0-7)> } | dscp <value (0-63)> } ] [
priority < short (1-255)> ] [ svlan-id <vlan-id (1-4094)> ] [ svlan-priority
<value (0-7)> ] [ cvlan-id <vlan-id (1-4094)> ] [ cvlan-priority <value (0-7)> ]
[ { single-tag | double-tag } ] [ ForQoS ] [ redirect { interface <ifXtype>
<ifnum> | <ifXtype><iface_list> [ <ifXtype><iface_list> ] load-balance { src-ip |
dst-ip | src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport | src-udpport |
dst-udpport } } ] [ sub-action { none | modify-vlan <short (1-4094)> | nested-vlan
<short (1 -4094)> } ]
```

|                           |                                                                              |   |                                                                                                                                                                                                                                                                             |
|---------------------------|------------------------------------------------------------------------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>udp</b>                                                                   | - | User Datagram Protocol                                                                                                                                                                                                                                                      |
| <b>n</b>                  | any  host<br><br><src-ip-address> <br><br><src-ip-address><br><br><src-mask> | - | Source IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul> |
|                           | port-number                                                                  | - | Port Number. The input for the source and the                                                                                                                                                                                                                               |

- destination port-number is prefixed with one of the following operators.
- eq=equal
  - lt=less than
  - gt=greater than
  - range=a range of ports; two different port numbers must be specified
- any | host**
- <dest-ip-address> |**
- <dest-ip-address>**
- <dest-mask>**
- Destination IP address can be
    - 'any' or
    - the word 'host' and the dotted decimal address or
    - number of the network or the host that the packet is destined for and the network mask to use with the destination address
- tos**
- {max-reliability |**
- max-throughput |**
- min-delay | normal**
- | <value (0-7)> |**
- dscp <value (0-**
- 63)>}**
- Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7.
- dscp**
- Differentiated services code point provides the quality of service control. The various options available are:
    - 0-63 - Differentiated services code point value

The parameters newly added in the existing commands for industry standard CLI are:

    - **af11** - Matches packets with AF11 DSCP (001010)
    - **af12** - Matches packets with AF12 DSCP (001100)
    - **af13** - Matches packets with AF13 DSCP (001110)
    - **af21** - Matches packets with AF21 DSCP (010010)
    - **af22** - Matches packets with AF22 DSCP (010100)
    - **af23** - Matches packets with AF23 DSCP (010110)
    - **af31** - Matches packets with AF31 DSCP (011010)
    - **af32** - Matches packets with AF32 DSCP (011100)
    - **af33** - Matches packets with AF33 DSCP (011110)
    - **af41** - Matches packets with AF41 DSCP (100010)
    - **af42** - Matches packets with AF42 DSCP (100100)
    - **af43** - Matches packets with AF43 DSCP (100110)
    - **cs1** - Matches packets with CS1 (precedence 1) DSCP (001000)

- cs2 - Matches packets with CS2 (precedence 2) DSCP (010000)
  - cs3 - Matches packets with CS3 (precedence 3) DSCP (011000)
  - cs4 - Matches packets with CS4 (precedence 4) DSCP (100000)
  - cs5 - Matches packets with CS5 (precedence 5) DSCP (101000)
  - cs6 - Matches packets with CS6 (precedence 6) DSCP (110000)
  - cs7 - Matches packets with CS7 (precedence 7) DSCP (111000)
  - default - Default DSCP (000000)
  - ef - Matches packets with EF DSCP (101110)
- priority** - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
- svlan-id** - Service VLAN value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.
- ForQoS** - The configuration done is made available for the QoS rules also.
- precedence<sup>1</sup>** - Precedence level to be used for filtering packets.  
 This parameter is newly added in the existing command for industry standard CLI.  
 The values are:
- 0 - Matches packets with routine precedence.

- 1 - Matches packets with priority precedence.
- 2 - Matches packets with immediate precedence.
- 3 - Matches packets with flash precedence.
- 4 - Matches packets with flash override precedence.
- 5 - Matches packets with critical precedence.
- 6 - Matches packets with internetwork control precedence.
- 7 - Matches packets with network control precedence.

**fragments**

- Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

**log**

- Creates informational logging message about the packets that match the entry to be sent to the console.  
This message includes the access list number, whether the packet is permitted or denied; the protocol, whether the protocol is TCP (Transport Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), or a number; and if appropriate, the source and destination addresses and source and destination port numbers.  
This message is generated for the first packet that matches a flow. This message is then generated at 5-minute intervals with the number of packets permitted or denied in the prior 5-minute interval.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

**log-input**

- Creates information logging message along with the information about the input interface.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

**reflect**

- Name of the reflexive access list.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

**time-range**

- Name of the time range to be applied.

Time range defines the time when the permit or deny statements of the Access Control List are in effect.

This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- redirect**
- Redirects the action to the destination interface or set of interfaces.
    - ifXtype – Specifies the interface type
    - ifnum – Specifies the interface number
    - iface\_list – Specifies the list of interfaces
- load-balance**
- Specifies the parameters based on which the traffic distribution needs to be done. Options are:
    - src-ip
    - dst-ip
    - src-mac
    - dst-mac
    - vlanid
    - src-tcpport
    - dst-tcpport
    - src-udpport
    - dst-udpport
- sub-action**
- Specifies the VLAN specific sub action to be performed on the packet -
    - none – Actions relating to the VLAN ID will not be considered.
    - modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
    - nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** dscp - -1

priority - 1

|                         |   |            |
|-------------------------|---|------------|
| svlan-id                | - | 0          |
| svlan-priority          | - | -1         |
| cvlan-id                | - | 0          |
| cvlan-priority          | - | -1         |
| single-tag   double-tag | - | Single tag |
| precedence              | - | 1          |

**Example** `iss(config-ext-nacl)# permit udp any 100.0.0.10 load-balance src-ip`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related  
Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters
- **show access-lists** - Displays the access list configuration

## 65.1.21 deny udp

This command specifies the UDP packets to be rejected based on the associated parameters.

```
deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [ { gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)> } ] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [ { gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-
number (1-65535)> <port-number (1-65535)> } ] [ { tos { max-reliability | max-
throughput | min-delay | normal | <tos-value (0-7)> } | dscp { <value (0-63)> | af11 |
af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 |
cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef } } ] [ priority <(1-255)> ]
[ { precedence (0-7)> | fragments | log | log-input | reflect <access-list> |
time-range <value> } ]
```

### For Metro

```
deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [ { gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)> } ] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [ { gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-
number (1-65535)> <port-number (1-65535)> } ] [ { tos { max-reliability | max-
throughput | min-delay | normal | <tos-value (0-7)> } | dscp <value (0-63)> } ] [
priority < short (1-255)> ] [ svlan-id <vlan-id (1-4094)> ] [ svlan-priority
<value (0-7)> ] [ cvlan-id <vlan-id (1-4094)> ] [ cvlan-priority <value (0-7)> ]
[ { single-tag | double-tag } ]
```

|                           |                                                                                                                |                                                                                                                                                                                                                                                                                                        |
|---------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>udp</b>                                                                                                     | - User Datagram Protocol                                                                                                                                                                                                                                                                               |
| <b>n</b>                  | <b>any  host</b><br><b>&lt;src-ip-address&gt; </b><br><b>&lt;src-ip-address&gt;</b><br><b>&lt;src-mask&gt;</b> | - Source IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul>                          |
|                           | <b>port-number</b>                                                                                             | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators. <ul style="list-style-type: none"> <li>• eq=equal</li> <li>• lt=less than</li> <li>• gt=greater than</li> <li>• range=a range of ports; two different port numbers</li> </ul> |

must be specified

- any | host**
- <dest-ip-address>**
- | <dest-ip-address>**
- <dest-mask>**
- Destination IP address can be
    - 'any' or
    - the word 'host' and the dotted decimal address or
    - number of the network or the host that the packet is destined for and the network mask to use with the destination address
- tos**
- Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.
- dscp**
- Differentiated services code point provides the quality of service control. The various options available are:
    - 0-63 - Differentiated services code point valueThe parameters newly added in the existing commands for industry standard CLI are:
    - af11 - Matches packets with AF11 DSCP (001010)
    - af12 - Matches packets with AF12 DSCP (001100)
    - af13 - Matches packets with AF13 DSCP (001110)
    - af21 - Matches packets with AF21 DSCP (010010)
    - af22 - Matches packets with AF22 DSCP (010100)
    - af23 - Matches packets with AF23 DSCP (010110)
    - af31 - Matches packets with AF31 DSCP (011010)
    - af32 - Matches packets with AF32 DSCP (011100)
    - af33 - Matches packets with AF33 DSCP (011110)
    - af41 - Matches packets with AF41 DSCP (100010)
    - af42 - Matches packets with AF42 DSCP (100100)
    - af43 - Matches packets with AF43 DSCP (100110)
    - cs1 - Matches packets with CS1 (precedence 1) DSCP (001000)
    - cs2 - Matches packets with CS2 (precedence 2) DSCP (010000)
    - cs3 - Matches packets with CS3 (precedence 3) DSCP (011000)
    - cs4 - Matches packets with CS4 (precedence 4) DSCP (100000)
    - cs5 - Matches packets with CS5 (precedence 5) DSCP (101000)

- cs6 - Matches packets with CS6 (precedence 6) DSCP (110000)
  - cs7 - Matches packets with CS7 (precedence 7) DSCP (111000)
  - default - Default DSCP (000000)
  - ef - Matches packets with EF DSCP (101110)
- priority** - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
- svlan-id** - Service VLAN value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.
- precedence<sup>1</sup>** - Precedence level to be used for filtering packets.  
 This parameter is newly added in the existing command for industry standard CLI.  
 The values are:
- 0 - Matches packets with routine precedence.
  - 1 - Matches packets with priority precedence.
  - 2 - Matches packets with immediate precedence.
  - 3 - Matches packets with flash precedence.
  - 4 - Matches packets with flash override precedence.
  - 5 - Matches packets with critical precedence.
  - 6 - Matches packets with internetwork control precedence.
  - 7 - Matches packets with network control precedence.

- fragments**
- Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- log**
- Creates informational logging message about the packets that match the entry to be sent to the console.  
This message includes the access list number, whether the packet is permitted or denied; the protocol, whether the protocol is TCP (Transport Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), or a number; and if appropriate, the source and destination addresses and source and destination port numbers.  
This message is generated for the first packet that matches a flow. This message is then generated at 5-minute intervals with the number of packets permitted or denied in the prior 5-minute interval.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- log-input**
- Creates information logging message along with the information about the input interface.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- reflect**
- Name of the reflexive access list.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- time-range**
- Name of the time range to be applied.  
Time range defines the time when the permit or deny statements of the Access Control List are in effect.  
This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** dscp - -1

|                         |   |            |
|-------------------------|---|------------|
| priority                | - | 1          |
| svlan-id                | - | 0          |
| svlan-priority          | - | -1         |
| cvlan-id                | - | 0          |
| cvlan-priority          | - | -1         |
| single-tag   double-tag | - | Single tag |
| precedence              | - | 1          |

**Example** `iss(config-ext-nacl)# deny udp host 10.0.0.1 any eq 20`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit udp` - Specifies the UDP packets to be forwarded based on the associated parameters
- `show access-lists` - Displays the access list configuration

## 65.1.22 copy-to-cpu udp

This command copies the UDP control packets to control plane CPU with or without switching of packets based on the configured parameters.

```
copy-to-cpu udp { any | host <src-ip-address> | <src-ip-address> <src-mask>}
[<gt; <port-number (1-65535)> | <lt;port-number (1-65535)> | eq <port-number
(1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any |
host <dest-ip-address> | <dest-ip-address> <dest-mask> } [{ <gt; <port-number
(1-65535)> | <lt;port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{<tos{max-reliability|max-
throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [
priority <(1-255)>] [noswitching]
```

### For Metro

```
copy-to-cpu udp { any | host <src-ip-address> | <src-ip-address> <src-mask>}
[<gt; <port-number (1-65535)> | <lt;port-number (1-65535)> | eq <port-number
(1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any |
host <dest-ip-address> | <dest-ip-address> <dest-mask> } [{ <gt; <port-number
(1-65535)> | <lt;port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{<tos{max-reliability|max-
throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [
priority < short (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-priority
<value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value (0-7)>]
[ { single-tag | double-tag } ] [noswitching]
```

|                           |                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <pre>any   host &lt;src- ip-address&gt;        &lt;src-ip-address&gt; &lt;src-mask&gt;</pre> | <ul style="list-style-type: none"> <li>- Copies the UDP control packets to control plane CPU with or without switching of packets based on the following source address configuration: <ul style="list-style-type: none"> <li>• any - Copies all control packets. Does not check for the source IP address in the packets.</li> <li>• host - Copies only the control packets having the specified unicast host network IP address as the source address.</li> <li>• &lt;src-ip-address&gt; &lt;src-mask&gt; - Copies only the control packets having the specified unicast source IP address and mask.</li> </ul> </li> </ul> |
| <b>gt</b>                 |                                                                                              | <ul style="list-style-type: none"> <li>- Copies only the UDP control packets having the UDP source / destination port numbers greater than the specified port number.<br/>This value ranges between 1 and 65535.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>lt</b>                 |                                                                                              | <ul style="list-style-type: none"> <li>- Copies only the UDP control packets having the UDP source / destination port numbers lesser than the specified port number.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                               |

- This value ranges between 1 and 65535.
- eq** - Copies only the UDP control packets having the specified UDP source / destination port numbers. This value ranges between 1 and 65535.
- range** - Copies only the UDP control packets having the UDP source / destination port numbers within the specified range. This value ranges between 1 and 65535. This value specifies the minimum port number and the maximum port number values.
- any | host <dest-ip-address> | <dest-ip-address> <dest-mask>** - Copies the UDP control packets to control plane CPU with or without switching of packets based on the following destination address configuration:
- any - Copies all control packets. Does not check for the destination IP address in the packets.
  - host - Copies only the control packets having the specified host network IP address as the destination address.
  - <dest-ip-address> <dest-mask> - Copies only the control packets having the specified destination IP address and mask.
- ack | rst** - Copies the UDP control packets to control plane CPU with or without switching of packets based on the following configuration:
- ack - Copies only the control packets having the ACK bit set.
  - rst - Copies only the control packets having the RST bit set.
- tos** - Copies the UDP control packets to control plane CPU with or without switching of packets based on the following type of service configuration:
- max-reliability - Copies only the control packets having TOS field set as high reliability.
  - max-throughput - Copies only the control packets having TOS field set as high throughput.
  - min-delay - Copies only the control packets having TOS field set as low delay.
  - normal - Copies all control packets. Does not check for the TOS field in the packets.
  - <value (0-7)> - Copies the control packets based on the TOS value set. The value ranges between

0 and 7. This value represents different combination of TOS.

- 0 - Copies all control packets. Does not check for the TOS field in the packets.
- 1 - Copies only the control packets having TOS field set as high reliability.
- 2 - Copies only the control packets having TOS field set as high throughput.
- 3 - Copies the control packets having TOS field set either as high reliability or high throughput.
- 4 - Copies only the control packets having TOS field set as low delay.
- 5 - Copies the control packets having TOS field set either as low delay or high reliability.
- 6 - Copies the control packets having TOS field set either as low delay or high throughput.
- 7 - Copies the control packets having TOS field set either as low delay or high reliability or high throughput.

- dscp** - Copies only the UDP control packets having the specified DSCP value.  
This value ranges between 0 and 63.
- priority** - Copies only the UDP control packets having the specified L2 priority value.  
This value ranges between 1 and 255.
- svlan-id** - Copies only the UDP control packets having the specified service VLAN ID / outer VLAN ID / VLAN ID provided in outer tag.  
This value ranges between 1 and 4094.
- svlan-priority** - Copies only the UDP control packets having the specified service VLAN priority / outer VLAN priority / VLAN priority provided in outer tag.  
This value ranges between 0 and 7.
- cvlan-id** - Copies only the UDP control packets having the specified customer VLAN ID / inner VLAN ID / VLAN ID provided in inner tag.  
This value ranges between 1 and 4094.

- cvlan-priority** - Copies only the UDP control packets having the specified customer VLAN priority / inner VLAN priority / VLAN priority provided in inner tag. This value ranges between 0 and 7.
- single-tag** | **double-tag** - Copies the UDP control packets to control plane CPU with or without switching of packets based on the following packet tag type configuration:
- **single-tag** - Copies only the single VLAN tagged packets.
  - **double-tag** - Copies only the double VLAN tagged packets.
- The tag type is set as double-tag and cannot be configured, if any one of the parameter service VLAN ID, service VLAN priority or customer VLAN priority is configured.
- noswitching** - Copies the UDP control packets to control plane CPU without switching of packets.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

- Defaults** any | host <src-ip-address> | <src-ip-address> <src-mask> - any
- gt - 0 (that is, the packets are not checked for UDP port number)
- lt - 0 (that is, the packets are not checked for UDP port number)
- eq - 0 (that is, the packets are not checked for UDP port number)
- range - 0 for minimum port number.  
65535 for maximum port number.
- any | host <dest-ip-address> | <dest-ip-address> <dest-mask> - any

|                         |   |                                                                       |
|-------------------------|---|-----------------------------------------------------------------------|
| dscp                    | - | -1 (that is, the packets are not checked for DSCP value)              |
| priority                | - | 1                                                                     |
| svlan-id                | - | 0 (that is, the packets are not checked for service VLAN identifier)  |
| svlan-priority          | - | -1 (that is, the packets are not checked for service VLAN priority)   |
| cvlan-id                | - | 0 (that is, the packets are not checked for customer VLAN identifier) |
| cvlan-priority          | - | -1 (that is, the packets are not checked for customer VLAN priority)  |
| single-tag   double-tag | - | single-tag                                                            |

**Example**

```
iss(config-ext-nacl)# copy-to-cpu udp any eq 300 any tos 1
priority 2 noswitching
```



- This command is available, only if the switch NPAPI\_WANTED or QOSX\_WANTED is set as yes during compilation of the exe.
- The UDP port number details can be set either for source or destination. The default value is applied for destination UDP port number, if the source UDP port number is configured or vice-versa.

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access lists configuration.

## 65.1.23 permit icmp

This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.

```
permit icmp {any | host <src-ip-address>|<src-ip-address> <mask>}{any | host
<dest-ip-address> | <dest-ip-address> <mask> }[<message-type (0-255)>]
[<message-code (0-255)>] [ priority <(1-255)>] [ForQoS] [redirect {interface
<ifXtype> <ifnum> | <ifXtype><iface_list>[<ifXtype><iface_list>] load-balance
{src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport |
src-udpport | dst-udpport}}] [sub-action {none | modify-vlan<short (1-4094)>
| nested-vlan <short (1 -4094)>}]
```

### For Metro

```
permit icmp {any | host <src-ip-address>|<src-ip-address> <mask>}{any | host
<dest-ip-address> | <dest-ip-address> <mask> }[<message-type (0-255)>]
[<message-code (0-255)>] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-
4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-
priority <value (0-7)>] [ { single-tag | double-tag } ] [ForQoS] [redirect
{interface <ifXtype> <ifnum> | <ifXtype><iface_list>[<ifXtype><iface_list>]
load-balance {src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport |
dst-tcpport | src-udpport | dst-udpport}}] [sub-action {none | modify-
vlan<short (1-4094)> | nested-vlan <short (1 -4094)>}]
```

|                           |                                 |                                                                                                                              |
|---------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>icmp</b>                     | - Internet Control Message Protocol                                                                                          |
|                           | <b>any  host</b>                | - Source IP address can be                                                                                                   |
|                           | <b>&lt;src-ip-address&gt;</b>   | • 'any' or                                                                                                                   |
|                           | <b> &lt;src-ip-address&gt;</b>  | • the word 'host' and the dotted decimal address or                                                                          |
|                           | <b>&lt;mask&gt;</b>             | • number of the network or the host that the packet is from and the network mask to use with the source address              |
|                           | <b>any host</b>                 | - Destination IP address can be                                                                                              |
|                           | <b>&lt;dest-ip-address&gt; </b> | • 'any' or                                                                                                                   |
|                           | <b>&lt;dest-ip-address&gt;</b>  | • the word 'host' and the dotted decimal address or                                                                          |
|                           | <b>&lt;mask&gt;</b>             | • number of the network or the host that the packet is destined for and the network mask to use with the destination address |
|                           | <b>message-type</b>             | - Message type                                                                                                               |

---

|                       |                                                                                                                                                                                                                                                                                                    |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>message-code</b>   | - ICMP Message code                                                                                                                                                                                                                                                                                |
| <b>priority</b>       | - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.                                                                                                  |
| <b>svlan-id</b>       | - Service VLAN value to match against incoming packets.                                                                                                                                                                                                                                            |
| <b>svlan-priority</b> | - Service VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                   |
| <b>cvlan-id</b>       | - Customer VLAN value to match against incoming packets.                                                                                                                                                                                                                                           |
| <b>cvlan-priority</b> | - Customer VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                  |
| <b>single-tag</b>     | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                                                                                                                              |
| <b>double-tag</b>     | - Filter to be applied on double VLAN tagged packets.                                                                                                                                                                                                                                              |
| <b>ForQoS</b>         | - The configuration done is made available for the QoS rules also.                                                                                                                                                                                                                                 |
| <b>redirect</b>       | - Redirects the action to the destination interface or set of interfaces. <ul style="list-style-type: none"><li>• ifXtype – Specifies the interface type</li><li>• ifnum – Specifies the interface number</li><li>• iface_list – Specifies the list of interfaces</li></ul>                        |
| <b>load-balance</b>   | - Specifies the parameters based on which the traffic distribution needs to be done. Options are: <ul style="list-style-type: none"><li>• src-ip</li><li>• dst-ip</li><li>• src-mac</li><li>• dst-mac</li><li>• vlanid</li><li>• src-tcpport</li><li>• dst-tcpport</li><li>• src-udpport</li></ul> |

- dst-udpport

- sub-action**
- Specifies the VLAN specific sub action to be performed on the packet -
    - none – Actions relating to the VLAN ID will not be considered.
    - modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
    - nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults**

|                           |   |            |
|---------------------------|---|------------|
| message-type/message code | - | 255        |
| priority                  | - | 1          |
| svlan-id                  | - | 0          |
| svlan-priority            | - | -1         |
| cvlan-id                  | - | 0          |
| cvlan-priority            | - | -1         |
| single-tag   double-tag   | - | Single tag |

**Example** `iss(config-ext-nacl)# permit icmp any 10.0.0.1 load balance src-ip`



- The ICMP message type can be one of the following:

| Value | ICMP type               |
|-------|-------------------------|
| 0     | Echo reply              |
| 3     | Destination unreachable |
| 4     | Source quench           |
| 5     | Redirect                |
| 8     | Echo request            |
| 11    | Time exceeded           |
| 12    | Parameter problem       |

|     |                      |
|-----|----------------------|
| 13  | Timestamp request    |
| 14  | Timestamp reply      |
| 15  | Information request  |
| 16  | Information reply    |
| 17  | Address mask request |
| 18  | Address mask reply   |
| 155 | No ICMP type         |

- The ICMP code can be any of the following:

| Value | ICMP code                                       |
|-------|-------------------------------------------------|
| 0     | Network unreachable                             |
| 1     | Host unreachable                                |
| 2     | Protocol unreachable                            |
| 3     | Port unreachable                                |
| 4     | Fragment need                                   |
| 5     | Source route fail                               |
| 6     | Destination network unknown                     |
| 7     | Destination host unknown                        |
| 8     | Source host isolated                            |
| 9     | Destination network administratively prohibited |
| 10    | Destination host administratively prohibited    |
| 11    | Network unreachable TOS                         |
| 12    | Host unreachable TOS                            |
| 255   | No ICMP code                                    |

- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

#### Related Commands

- **ip access-list** - Created IP ACLs and enters the IP Access-list configuration mode
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- **show access-lists** - Displays the access list configuration

## 65.1.24 deny icmp

This command specifies the ICMP packets to be rejected based on the IP address and associated parameters.

```
deny icmp {any | host <src-ip-address>|<src-ip-address> <mask>}{any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
 [<message-code (0-255)>] [ priority <(1-255)>]
```

### For Metro

```
deny icmp {any | host <src-ip-address>|<src-ip-address> <mask>}{any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
 [<message-code (0-255)>] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-
4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-
priority <value (0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                                                               |                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>icmp</b>                                                                   | - Internet Control Message Protocol                                                                                                                                                                                                                                                                                                                                   |
|                           | <b>any  host &lt;src-ip-address&gt;  &lt;src-ip-address&gt; &lt;mask&gt;</b>  | <ul style="list-style-type: none"> <li>- Source IP address can be           <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address</li> <li>or</li> <li>- number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul> </li> </ul>                   |
|                           | <b>any host &lt;dest-ip-address&gt;  &lt;dest-ip-address&gt; &lt;mask&gt;</b> | <ul style="list-style-type: none"> <li>- Destination IP address can be           <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address</li> <li>or</li> <li>- number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> </li> </ul> |
|                           | <b>message-type</b>                                                           | - Message type                                                                                                                                                                                                                                                                                                                                                        |
|                           | <b>message-code</b>                                                           | - ICMP Message code                                                                                                                                                                                                                                                                                                                                                   |
|                           | <b>priority</b>                                                               | - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a                                                                                                                                                                                      |

|                       |   |                                                                 |
|-----------------------|---|-----------------------------------------------------------------|
|                       |   | higher priority.                                                |
| <b>svlan-id</b>       | - | Service VLAN value to match against incoming packets.           |
| <b>svlan-priority</b> | - | Service VLAN priority value to match against incoming packets.  |
| <b>cvlan-id</b>       | - | Customer VLAN value to match against incoming packets.          |
| <b>cvlan-priority</b> | - | Customer VLAN priority value to match against incoming packets. |
| <b>single-tag</b>     | - | Filter to be applied on Single VLAN tagged packets.             |
| <b>double-tag</b>     | - | Filter to be applied on double VLAN tagged packets.             |

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

|                 |                               |   |            |
|-----------------|-------------------------------|---|------------|
| <b>Defaults</b> | message-type/<br>message code | - | 255        |
|                 | priority                      | - | 1          |
|                 | svlan-id                      | - | 0          |
|                 | svlan-priority                | - | -1         |
|                 | cvlan-id                      | - | 0          |
|                 | cvlan-priority                | - | -1         |
|                 | single-tag   double-tag       | - | Single tag |

**Example**

```
iss(config-ext-nacl)# deny icmp host 100.0.0.10 10.0.0.1
255.255.255.255
```



- The ICMP message type can be one of the following:

| Value | ICMP type |
|-------|-----------|
|-------|-----------|

|     |                         |
|-----|-------------------------|
| 0   | Echo reply              |
| 3   | Destination unreachable |
| 4   | Source quench           |
| 5   | Redirect                |
| 8   | Echo request            |
| 11  | Time exceeded           |
| 12  | Parameter problem       |
| 13  | Timestamp request       |
| 14  | Timestamp reply         |
| 15  | Information request     |
| 16  | Information reply       |
| 17  | Address mask request    |
| 18  | Address mask reply      |
| 155 | No ICMP type            |

- The ICMP code can be any of the following:

| Value | ICMP code                                       |
|-------|-------------------------------------------------|
| 0     | Network unreachable                             |
| 1     | Host unreachable                                |
| 2     | Protocol unreachable                            |
| 3     | Port unreachable                                |
| 4     | Fragment need                                   |
| 5     | Source route fail                               |
| 6     | Destination network unknown                     |
| 7     | Destination host unknown                        |
| 8     | Source host isolated                            |
| 9     | Destination network administratively prohibited |
| 10    | Destination host administratively prohibited    |
| 11    | Network unreachable TOS                         |
| 12    | Host unreachable TOS                            |
| 255   | No ICMP code                                    |

- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

**Related Commands**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit icmp` - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters

- `show access-lists` - Displays the access list configuration

## 65.1.25 copy-to-cpu icmp

This command copies the ICMP control packets to control plane CPU with or without switching of packets based on the configured parameters.

```
copy-to-cpu icmp {any |host <src-ip-address>|<src-ip-address> <mask>} {any |
host <dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
[<message-code (0-255)>] [priority <(1-255)>] [noswitching]
```

### For Metro

```
copy-to-cpu icmp {any |host <src-ip-address>|<src-ip-address> <mask>} {any |
host <dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
[<message-code (0-255)>] [priority <value (1-255)>] [ svlan-id <vlan-id (1-
4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-
priority <value (0-7)>] [ { single-tag | double-tag } ] [noswitching]
```

|                           |                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <pre>any  host &lt;src- ip-address&gt; &lt;src- ip-address&gt; &lt;mask&gt;</pre>     | <ul style="list-style-type: none"> <li>- Copies the ICMP control packets to control plane CPU with or without switching of packets based on the following source address configuration: <ul style="list-style-type: none"> <li>• any - Copies all control packets. Does not check for the source IP address in the packets.</li> <li>• host - Copies only the control packets having the specified unicast host network IP address as the source address.</li> <li>• &lt;src-ip-address&gt; &lt;mask&gt; - Copies only the control packets having the specified unicast source IP address and mask.</li> </ul> </li> </ul>      |
| <b>Syntax Description</b> | <pre>any   host &lt;dest- ip-address&gt;   &lt;dest-ip-address&gt; &lt;mask&gt;</pre> | <ul style="list-style-type: none"> <li>- Copies the ICMP control packets to control plane CPU with or without switching of packets based on the following destination address configuration: <ul style="list-style-type: none"> <li>• any - Copies all control packets. Does not check for the destination IP address in the packets.</li> <li>• host - Copies only the control packets having the specified host network IP address as the destination address.</li> <li>• &lt;dest-ip-address&gt; &lt;mask&gt; - Copies only the control packets having the specified destination IP address and mask.</li> </ul> </li> </ul> |
| <b>Syntax Description</b> | <pre>&lt;message-type (0- 255)&gt;</pre>                                              | <ul style="list-style-type: none"> <li>- Copies only the ICMP control packets having the specified message type.<br/>This value ranges between 0 and 255.<br/>The value can be one of the following:</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Value | ICMP Type               |
|-------|-------------------------|
| 0     | Echo reply              |
| 3     | Destination unreachable |
| 4     | Source quench           |
| 5     | Redirect                |
| 8     | Echo request            |
| 11    | Time exceeded           |
| 12    | Parameter problem       |
| 13    | Timestamp request       |
| 14    | Timestamp reply         |
| 15    | Information request     |
| 16    | Information reply       |
| 17    | Address mask request    |
| 18    | Address mask reply      |

**<message-code (0-255) >** - Copies only the ICMP control packets having the specified message code.

This value ranges between 0 and 255.

The value can be one of the following:

| Value | ICMP Code                                       |
|-------|-------------------------------------------------|
| 0     | Network unreachable                             |
| 1     | Host unreachable                                |
| 2     | Protocol unreachable                            |
| 3     | Port unreachable                                |
| 4     | Fragment need                                   |
| 5     | Source route failed                             |
| 6     | Destination network unknown                     |
| 7     | Destination host unknown                        |
| 8     | Source host isolated                            |
| 9     | Destination network administratively prohibited |
| 10    | Destination host administratively prohibited    |
| 11    | Network unreachable TOS                         |
| 12    | Host unreachable TOS                            |
| 255   | No ICMP codes to be filtered                    |

**priority <(1-255) >** - Copies only the ICMP control packets having the specified L2 priority value.

This value ranges between 1 and 255.

- svlan-id** - Copies only the ICMP control packets having the specified service VLAN ID / outer VLAN ID / VLAN ID provided in outer tag.  
This value ranges between 1 and 4094.
  
- svlan-priority** - Copies only the ICMP control packets having the specified service VLAN priority / outer VLAN priority / VLAN priority provided in outer tag.  
This value ranges between 0 and 7.
  
- cvlan-id** - Copies only the ICMP control packets having the specified customer VLAN ID / inner VLAN ID / VLAN ID provided in inner tag.  
This value ranges between 1 and 4094.
  
- cvlan-priority** - Copies only the ICMP control packets having the specified customer VLAN priority / inner VLAN priority / VLAN priority provided in inner tag.  
This value ranges between 0 and 7.
  
- single-tag** | **double-tag** - Copies the ICMP control packets to control plane CPU with or without switching of packets based on the following packet tag type configuration:
  - single-tag - Copies only the single VLAN tagged packets.
  - double-tag - Copies only the double VLAN tagged packets.

The tag type is set as double-tag and cannot be configured, if any one of the parameter service VLAN ID, service VLAN priority or customer VLAN priority is configured.
  
- noswitching** - Copies the UDP control packets to control plane CPU without switching of packets.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** any | host <src-ip-address> | <src-ip-address> <mask> - any

any | host <dest-ip-address> | <dest-ip-address> <mask> - any

|                         |   |                                                                       |
|-------------------------|---|-----------------------------------------------------------------------|
| priority                | - | 1                                                                     |
| svlan-id                | - | 0 (that is, the packets are not checked for service VLAN identifier)  |
| svlan-priority          | - | -1 (that is, the packets are not checked for service VLAN priority)   |
| cvlan-id                | - | 0 (that is, the packets are not checked for customer VLAN identifier) |
| cvlan-priority          | - | -1 (that is, the packets are not checked for customer VLAN priority)  |
| single-tag   double-tag | - | single-tag                                                            |

**Example**

```
iss(config-ext-nacl)# copy-to-cpu icmp any any 11 7
noswitching
```



This command is available, only if the switch NPAPI\_WANTED or QOSX\_WANTED is set as yes during compilation of the exe.

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access lists configuration.

## 65.1.26 ip access-group

This command enables access control for the packets on the interface. It controls access to a Layer 2 or Layer 3 interface. The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out.

```
ip access-group <access-list-number (1-65535)> {in | out}
```

```
no ip access-group [<access-list-number (1-65535)>] {in | out}
```

|                           |                           |   |                               |
|---------------------------|---------------------------|---|-------------------------------|
| <b>Syntax Description</b> | <b>access-list-number</b> | - | IP access control list number |
|                           | <b>in</b>                 | - | Inbound packets               |
|                           | <b>out</b>                | - | Outbound packets              |

**Mode** Interface Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss(config-if)# ip access-group 1 in



- IP access list must have been created.
- Following are the limitations for this command to be applicable to Layer 2 interfaces.
  - The out keyword is not supported by Layer 2 interfaces.
  - An IP ACL applied to a Layer 2 interface filters only the IP packets. MAC access-group interface configuration command with MAC extended ACLs must be used to filter non-IP packets.

- Related Commands**
- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
  - **show access-lists** - Displays the access list configuration

## 65.1.27 mac access-group

This command applies a MAC access control list (ACL) to a Layer 2 interface. The no form of this command can be used to remove the MAC ACLs from the interface.

```
mac access-group <access-list-number (1-65535)> in
```

```
no mac access-group [<access-list-number (1-65535)>] in
```

### For Metro

```
mac access-group <access-list-number (1-65535)> {in | out}
```

```
no mac access-group [<access-list-number (1-65535)>] {in | out}
```

|                           |                           |   |                    |
|---------------------------|---------------------------|---|--------------------|
| <b>Syntax Description</b> | <b>access-list-number</b> | - | Access List Number |
|                           | <b>in</b>                 | - | Inbound packets    |
|                           | <b>out</b>                | - | Outbound packets   |

**Mode** Interface Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config-if)# mac access-group 5 in`



MAC access list must have been created.

- Related Commands**
- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
  - **permit - MAC** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
  - **deny - MAC** - Specifies the packets to be rejected based on the MAC address and the associated parameters.
  - **show access-lists** - Displays the access list statistics

## 65.1.28 user-defined access-group

This command applies a user defined access list (ACL) to an interface. The no form of this command removes the User defined ACLs from the interface.

```
user-defined access-group <access-list-number (1-65535)> in
```

```
no user-defined access-group [<access-list-number (1-65535)>] in
```

### For Metro

```
user-defined access-group <access-list-number (1-65535)> {in | out}
```

```
no user-defined access-group [<access-list-number (1-65535)>] {in | out}
```

|                           |                           |                                 |
|---------------------------|---------------------------|---------------------------------|
| <b>Syntax Description</b> | <b>access-list-number</b> | - IP access control list number |
|                           | <b>in</b>                 | - Inbound packets               |
|                           | <b>out</b>                | - Outbound packets              |

**Mode** Interface Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss(config-if)# user-defined access-group 5 in



User defined access list should be created already, before executing this command.

- Related Commands**
- **user-defined access-list** - Creates the user defined access-list.
  - **show access-lists** - Displays the access list statistics

## 65.1.29 permit - MAC

This command specifies the packets to be forwarded based on the MAC address and the associated parameters, that is, this command allows non-IP traffic to be forwarded if the conditions are matched.

```
permit { any | host <src-mac-address> } { any | host <dest-mac-address> } [ aarp |
amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 |
lat | larc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo
| vines-ip | xns-id | <protocol (0-65535)> | type <0-65535> <0-65535> | lsap
<0-65535> <0-65535> ] [ encaps-type <value (1-65535)> ] [ Vlan <vlan-id (1-
4094)> ] [ priority <value (1-255)> ] [ ForQoS ] [ redirect { interface <ifXtype>
<ifnum> | <ifXtype><iface_list> [ <ifXtype><iface_list> ] load-balance { src-ip |
dst-ip | src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport | src-udpport
| dst-udpport } } ] [ sub-action { none | modify-vlan <short (1-4094)> | nested-vlan
<short (1 -4094)> | strip-ether-hdr } } ] [ next-filter-type { 12 | 13 | user-
defined } next-filter-id <short (1-65535)> ]
```

### For Metro

```
permit { any | host <src-mac-address> } { any | host <dest-mac-address> } [ { aarp
| amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-
8042 | lat | larc-sca | mop-console | mop-dump | msdos | mumps | netbios |
vines-echo | vines-ip | xns-id | <short (0-65535)> } ] [ encaps-type <integer
(1-65535)> ] [ Vlan <vlan-id (1-4094)> ] [ priority <short (1-255)> ] [
outerEtherType < integer (1-65535)> ] [ svlan-id <vlan-id (1-4094)> ] [ cvlan-
priority <value (0-7)> ] [ svlan-priority <value (0-7)> ] [ { single-tag |
double-tag } ] [ ForQoS ] [ redirect { interface <ifXtype> <ifnum> |
<ifXtype><iface_list> [ <ifXtype><iface_list> ] load-balance { src-ip | dst-ip |
src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport | src-udpport | dst-
udpport } } ] [ sub-action { none | modify-vlan <short (1-4094)> | nested-vlan
<short (1 -4094)> | strip-ether-hdr } } ] [ next-filter-type { 12 | 13 | user-
defined } next-filter-id <short (1-65535)> ]
```

|                           |                                |   |                                                                                                    |
|---------------------------|--------------------------------|---|----------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | any   host <src-mac-address >  | - | Source MAC address to be matched with the packet                                                   |
|                           | any   host <dest-mac-address > | - | Destination MAC address to be matched with the packet                                              |
|                           | aarp                           | - | EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address |
|                           | amber                          | - | EtherType DEC-Amber                                                                                |
|                           | dec-spanning                   | - | EtherType Digital Equipment Corporation (DEC) spanning tree                                        |

---

|                                   |                                                                                                                                                                |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>decnet-iv</b>                  | - EtherType DECnet Phase IV protocol                                                                                                                           |
| <b>diagnostic</b>                 | - EtherType DEC-Diagnostic                                                                                                                                     |
| <b>dsm</b>                        | - EtherType DEC-DSM/DDP                                                                                                                                        |
| <b>etype-6000</b>                 | - EtherType 0x6000                                                                                                                                             |
| <b>etype-8042</b>                 | - EtherType 0x8042                                                                                                                                             |
| <b>lat</b>                        | - EtherType DEC-LAT                                                                                                                                            |
| <b>lavc-sca</b>                   | - EtherType DEC-LAVC-SCA                                                                                                                                       |
| <b>mop-console</b>                | - EtherType DEC-MOP Remote Console                                                                                                                             |
| <b>mop-dump</b>                   | - EtherType DEC-MOP Dump                                                                                                                                       |
| <b>msdos</b>                      | - EtherType DEC-MSDOS                                                                                                                                          |
| <b>mumps</b>                      | - EtherType DEC-MUMPS                                                                                                                                          |
| <b>netbios</b>                    | - EtherType DEC- Network Basic Input/Output System (NETBIOS)                                                                                                   |
| <b>vines-echo</b>                 | - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems                                                                                |
| <b>vines-ip</b>                   | - EtherType VINES IP                                                                                                                                           |
| <b>xns-id</b>                     | - EtherType Xerox Network Systems (XNS) protocol suite                                                                                                         |
| <b>&lt;protocol (0-65535)&gt;</b> | - Specifies the non-IP protocol type to be filtered. The value ranges between 0 and 65535. The value 0 represents that filter is applicable for all protocols. |
| <b>type</b>                       | - Specifies the ether type value and its mask. The value ranges between 0 and 65535 for type                                                                   |

- value and mask.
- . The mask feature is currently not supported.
- lsap**
- Specifies the LSAP value and its mask.  
The value ranges between 0 and 65535 for type value and mask.
  - . The mask feature is currently not supported.
- encaptype**
- Encapsulation Type
- outerEtherType**
- EtherType value to match on Service vlan tag
- svlan-id**
- Service VLAN value to match against incoming packets.
- cvlan-priority**
- Customer VLAN priority value to match against incoming packets.
- svlan-priority**
- Service VLAN priority value to match against incoming packets.
- single-tag**
- Filter to be applied on Single VLAN tagged packets.
- double-tag**
- Filter to be applied on double VLAN tagged packets.
- ForQoS**
- The configuration done is made available for the QoS rules also.
- redirect**
- Redirects the action to the destination interface or set of interfaces.
    - ifXtype – Specifies the interface type
    - ifnum – Specifies the interface number
    - iface\_list – Specifies the list of interfaces
- load-balance**
- Specifies the parameters based on which the traffic distribution needs to be done. Options are:
    - src-ip
    - dst-ip
    - src-mac
    - dst-mac

|                         |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         |                      | <ul style="list-style-type: none"> <li>• vlanid</li> <li>• src-tcpport</li> <li>• dst-tcpport</li> <li>• src-udpport dst-udpport</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>sub-action</b>       | -                    | <p>Specifies the VLAN specific sub action to be performed on the packet -</p> <ul style="list-style-type: none"> <li>• none – Actions relating to the VLAN ID will not be considered.</li> <li>• modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</li> <li>• nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.</li> <li>• strip-ether-hdr – Used to strip outer Ethernet header for MPLS packets.</li> </ul> |
| <b>next-filter-type</b> | -                    | <p>Specifies the type of next access-control list. The options are:</p> <ul style="list-style-type: none"> <li>• I2 - Filtering done for MAC-based ACL.</li> <li>• I3 - Filtering done for IP-based ACL.</li> <li>• user-defined - Filtering done based on user-defined filters.</li> </ul>                                                                                                                                                                                                                                 |
| <b>next-filter-id</b>   | -                    | <p>Specifies the next filter rule number to be matched for traffic matching the current ACL / QoS rule. This value ranges between 1 and 65535.</p>                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Mode</b>             |                      | ACL MAC Configuration Mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Package</b>          |                      | Workgroup, Enterprise and Metro                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Defaults</b>         | <protocol (0-65535)> | - 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                         | sub-action           | - none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                         | vlan-id              | - 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                         | priority             | - 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                         | outerEtherType       | - 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

---

|                         |   |            |
|-------------------------|---|------------|
| svlan-id                | - | 0          |
| cvlan-priority          | - | -1         |
| svlan-priority          | - | -1         |
| single-tag   double-tag | - | Single tag |

**Example** `iss(config-ext-macl)# permit host 00:11:22:33:44:55 any load-balance src-ip vlan-action modify lan 526`



- MAC access list must have been created.
- OuterEtherType, Service Vlan, Service Vlan Priority and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

**Related Commands**

- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **user-defined access-list** - Creates the user defined access-list.
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **deny - MAC** - Specifies the packets to be rejected based on the MAC address and the associated parameters
- **show access-lists** - Displays the access list statistics

## 65.1.30 deny - MAC

This command specifies the packets to be rejected based on the MAC address and the associated parameters.

```
deny { any | host <src-mac-address> } { any | host <dest-mac-address> } [ aarp |
amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 |
lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo
| vines-ip | xns-id | <protocol (0-65535)> | type <(0-65535)> <(0-65535)> |
lsap <(0-65535)> <(0-65535)> ] [ encapsype <value (1-65535)> ] [ Vlan <vlan-id
(1-4094)> ] [ priority <value (1-255)> ]
```

### For Metro

```
deny { any | host <src-mac-address> } { any | host <dest-mac-address> } [ { aarp
| amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-
8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios |
vines-echo | vines-ip | xns-id | <short (0-65535)> } ] [ encapsype <integer
(1-65535)> ] [ Vlan <vlan-id (1-4094)> ] [ priority <short (1-255)> ] [
outerEtherType < integer (1-65535)> ] [ svlan-id <vlan-id (1-4094)> ] [ cvlan-
priority <priority (0-7)> ] [ svlan-priority <value (0-7)> ] [ { single-tag |
double-tag } ]
```

|                           |                                             |   |                                                                                                    |
|---------------------------|---------------------------------------------|---|----------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>any   host &lt;src-mac-address &gt;</b>  | - | Source MAC address to be matched with the packet                                                   |
|                           | <b>any   host &lt;dest-mac-address &gt;</b> | - | Destination MAC address to be matched with the packet                                              |
|                           | <b>aarp</b>                                 | - | EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address |
|                           | <b>amber</b>                                | - | EtherType DEC-Amber                                                                                |
|                           | <b>dec-spanning</b>                         | - | EtherType Digital Equipment Corporation (DEC) spanning tree                                        |
|                           | <b>decnet-iv</b>                            | - | EtherType DECnet Phase IV protocol                                                                 |
|                           | <b>diagnostic</b>                           | - | EtherType DEC-Diagnostic                                                                           |
|                           | <b>dsm</b>                                  | - | EtherType DEC-DSM/DDP                                                                              |

---

|                               |     |                                                                                                                                                                |
|-------------------------------|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>etype-6000</b>             | -   | EtherType 0x6000                                                                                                                                               |
| <b>etype-8042</b>             | -   | EtherType 0x8042                                                                                                                                               |
| <b>lat</b>                    | -   | EtherType DEC-LAT                                                                                                                                              |
| <b>lavc-sca</b>               | -   | EtherType DEC-LAVC-SCA                                                                                                                                         |
| <b>mop-console</b>            | -   | EtherType DEC-MOP Remote Console                                                                                                                               |
| <b>mop-dump</b>               | -   | EtherType DEC-MOP Dump                                                                                                                                         |
| <b>msdos</b>                  | -   | EtherType DEC-MSDOS                                                                                                                                            |
| <b>mumps</b>                  | -   | EtherType DEC-MUMPS                                                                                                                                            |
| <b>netbios</b>                | -   | EtherType DEC- Network Basic Input/Output System (NETBIOS)                                                                                                     |
| <b>vines-echo</b>             | -   | EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems                                                                                  |
| <b>vines-ip</b>               | -   | EtherType VINES IP                                                                                                                                             |
| <b>xns-id</b>                 | -   | EtherType Xerox Network Systems (XNS) protocol suite                                                                                                           |
| <b>&lt;protocol 65535&gt;</b> | (0- | - Specifies the non-IP protocol type to be filtered. The value ranges between 0 and 65535. The value 0 represents that filter is applicable for all protocols. |
| <b>type</b>                   | -   | Specifies the ether type value and its mask. The value ranges between 0 and 65535 for type value and mask.<br>. The mask feature is currently not supported.   |
| <b>lsap</b>                   | -   | Specifies the LSAP value and its mask. The value ranges between 0 and 65535 for type value and mask.<br>. The mask feature is currently not supported.         |

|                       |   |                                                                                                                                                                                                       |
|-----------------------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>encaptype</b>      | - | Encapsulation Type                                                                                                                                                                                    |
| <b>vlan</b>           | - | VLAN ID to be filtered                                                                                                                                                                                |
| <b>priority</b>       | - | The priority of the L2 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. |
| <b>outerEtherType</b> | - | EtherType value to match on Service vlan tag                                                                                                                                                          |
| <b>svlan-id</b>       | - | Service VLAN value to match against incoming packets.                                                                                                                                                 |
| <b>cvlan-priority</b> | - | Customer VLAN priority value to match against incoming packets.                                                                                                                                       |
| <b>svlan-priority</b> | - | Service VLAN priority value to match against incoming packets.                                                                                                                                        |
| <b>single-tag</b>     | - | Filter to be applied on Single VLAN tagged packets.                                                                                                                                                   |
| <b>double-tag</b>     | - | Filter to be applied on double VLAN tagged packets.                                                                                                                                                   |

**Mode** ACL MAC Configuration Mode

**Package** Workgroup, Enterprise and Metro

|                 |                         |   |            |
|-----------------|-------------------------|---|------------|
| <b>Defaults</b> | <protocol (0-65535)>    | - | 0          |
|                 | vlan-id                 | - | 0          |
|                 | priority                | - | 1          |
|                 | outerEtherType          | - | 0          |
|                 | svlan-id                | - | 0          |
|                 | cvlan-priority          | - | -1         |
|                 | svlan-priority          | - | -1         |
|                 | single-tag   double-tag | - | Single tag |

**Example**    `iss(config-ext-macl)# deny any host 00:11:22:33:44:55 priority 200`



- MAC access list must have been created.
- OuterEtherType, Service Vlan, Service Vlan Priority and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **user-defined access-list** - Creates the user defined access-list.
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **permit - MAC** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **show access-lists** - Displays the access list statistics

## 65.1.31 copy-to-cpu - MAC

This command copies the MAC protocol control packets to control plane CPU with or without switching of packets based on the configured parameters.

```
copy-to-cpu { any | host <src-mac-address>}{ any | host <dest-mac-address> }
[aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000
|etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps |
netbios | vines-echo | vines-ip | xns-id | <protocol (0-65535)> | type <(0-
65535)> <(0-65535)> | lsap <(0-65535)> <(0-65535)>] [ encapsytype <value (1-
65535)>][ Vlan <vlan-id (1-4094)>] [priority <value (1-255)>] [noswitching]
```

### For Metro

```
copy-to-cpu { any | host <src-mac-address>}{ any | host <dest-mac-address> } [
{ aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |
etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios
| vines-echo | vines-ip | xns-id | <short (0-65535)> } ] [ encapsytype <integer
(1-65535)> ] [ Vlan <vlan-id (1-4094)>] [priority <short (1-255)>] [
outerEtherType < integer (1-65535)> ] [ svlan-id <vlan-id (1-4094)>] [cvlan-
priority <priority (0-7)>] [ svlan-priority <value (0-7)>] [ { single-tag |
double-tag } ] [noswitching]
```

|                           |                                            |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>any   host &lt;src-mac-address&gt;</b>  | - Copies the MAC protocol control packets to control plane CPU with or without switching of packets based on the following source address configuration: <ul style="list-style-type: none"> <li>• any - Copies all control packets. Does not check for the source MAC address in the packets.</li> <li>• host - Copies only the control packets having the specified source MAC address.</li> </ul>                |
|                           | <b>any   host &lt;dest-mac-address&gt;</b> | - Copies the MAC protocol control packets to control plane CPU with or without switching of packets based on the following destination address configuration: <ul style="list-style-type: none"> <li>• any - Copies all control packets. Does not check for the destination MAC address in the packets.</li> <li>• host - Copies only the control packets having the specified destination MAC address.</li> </ul> |
|                           | <b>aarp</b>                                | - Copies only the MAC protocol control packets having the protocol type as AARP.                                                                                                                                                                                                                                                                                                                                   |
|                           | <b>amber</b>                               | - Copies only the MAC protocol control packets having the protocol type as DEC-Amber.                                                                                                                                                                                                                                                                                                                              |

---

|                     |                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------|
| <b>dec-spanning</b> | - Copies only the MAC protocol control packets having the protocol type as DEC spanning tree.      |
| <b>decnet-iv</b>    | - Copies only the MAC protocol control packets having the protocol type as DECnet Phase IV.        |
| <b>diagnostic</b>   | - Copies only the MAC protocol control packets having the protocol type as DEC-diagnostic.         |
| <b>dsm</b>          | - Copies only the MAC protocol control packets having the protocol type as DEC-DSM / DDP.          |
| <b>etype-6000</b>   | - Copies only the MAC protocol control packets having the protocol type as EtherType 0x6000.       |
| <b>etype-8042</b>   | - Copies only the MAC protocol control packets having the protocol type as EtherType 0x8042.       |
| <b>lat</b>          | - Copies only the MAC protocol control packets having the protocol type as DEC-LAT.                |
| <b>lavc-sca</b>     | - Copies only the MAC protocol control packets having the protocol type as DEC-LAVC-SCA.           |
| <b>mop-console</b>  | - Copies only the MAC protocol control packets having the protocol type as DEC-MOP remote console. |
| <b>mop-dump</b>     | - Copies only the MAC protocol control packets having the protocol type as DEC-MOP Dump.           |
| <b>msdos</b>        | - Copies only the MAC protocol control packets having the protocol type as DEC-MSDOS.              |
| <b>mumps</b>        | - Copies only the MAC protocol control packets having the protocol type as DEC-MUMPS.              |
| <b>netbios</b>      | - Copies only the MAC protocol control packets having the protocol type as NETBIOS.                |
| <b>vines-echo</b>   | - Copies only the MAC protocol control packets having the protocol type as VINES Echo.             |
| <b>vines-ip</b>     | - Copies only the MAC protocol control packets having the protocol type as VINES IP.               |

- 
- |                               |     |                                                                                                                                                                                                                    |
|-------------------------------|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>xns-id</b>                 | -   | Copies only the MAC protocol control packets having the protocol type as XNS protocol suite.                                                                                                                       |
| <b>&lt;protocol 65535&gt;</b> | (0- | - Copies only the MAC protocol control packets having the specified non-IP protocol type value. This value ranges between 0 and 65535.                                                                             |
| <b>type</b>                   | -   | - Copies only the MAC protocol control packets having the specified ether type value and mask. The value ranges between 0 and 65535 for type value and mask.<br><br>. The mask feature is currently not supported. |
| <b>lsap</b>                   | -   | - Copies only the MAC protocol control packets having the specified LSAP value and mask. The value ranges between 0 and 65535 for type value and mask.<br><br>. The mask feature is currently not supported.       |
| <b>encaptype</b>              | -   | - Copies only the MAC protocol control packets having the specified Ether Type value. This value ranges between 1 and 65535.                                                                                       |
| <b>vlan</b>                   | -   | - Copies only the MAC protocol control packets having the specified VLAN ID. This value ranges between 1 and 4094.                                                                                                 |
| <b>priority</b>               | -   | - Copies only the MAC protocol control packets having the specified L2 priority value. This value ranges between 1 and 255.                                                                                        |
| <b>outerEtherType</b>         | -   | - Copies only the MAC control packets having the specified Ether type value for the outer VLAN tag. This value ranges between 1 and 65535.                                                                         |
| <b>svlan-id</b>               | -   | - Copies only the MAC control packets having the specified service VLAN ID / outer VLAN ID / VLAN ID provided in outer tag. This value ranges between 1 and 4094.                                                  |
| <b>cvlan-priority</b>         | -   | - Copies only the MAC control packets having the specified customer VLAN priority / inner VLAN priority / VLAN priority provided in inner tag. This value ranges between 0 and 7.                                  |

- svlan-priority** - Copies only the MAC control packets having the specified service VLAN priority / outer VLAN priority / VLAN priority provided in outer tag. This value ranges between 0 and 7.
- single-tag** | **double-tag** - Copies the MAC control packets to control plane CPU with or without switching of packets based on the following packet tag type configuration:
- **single-tag** - Copies only the single VLAN tagged packets.
  - **double-tag** - Copies only the double VLAN tagged packets.
- The tag type is set as double-tag and cannot be configured, if any one of the parameter service VLAN ID, service VLAN priority or customer VLAN priority is configured.
- noswitching** - Copies the MAC protocol control packets to control plane CPU without switching of packets.

**Mode** ACL MAC Configuration Mode

**Package** Workgroup, Enterprise and Metro

- Defaults**
- any | host <src-mac-address> - any
  - any | host <dest-mac-address> - any
  - <protocol (0-65535)> - 0
  - encaptype - 0 (that is, the packets are not checked for Ether Type)
  - Vlan - 0 (that is, the packets are not checked for VLAN ID)
  - priority - 1
  - outerEtherType - 0 (that is, the packets are not checked for outer Ether type)
  - svlan-id - 0 (that is, the packets are not checked for service VLAN identifier)

|                         |   |                                                                      |
|-------------------------|---|----------------------------------------------------------------------|
| cvlan-priority          | - | -1 (that is, the packets are not checked for customer VLAN priority) |
| svlan-priority          | - | -1 (that is, the packets are not checked for service VLAN priority)  |
| single-tag   double-tag | - | single-tag                                                           |

**Example**

```
iss(config-ext-macl)# copy-to-cpu any any aarp encaptype 10
```



This command is available, only if the switch NPAPI\_WANTED or QOSX\_WANTED is set as yes during compilation of the exe.

**Related Commands**

- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **show access-lists** - Displays the access list statistics

## 65.1.32 show access-lists

This command displays the access lists configuration.

```
show access-lists [[{ip | mac | user-defined }] < access-list-number (1-65535)> ]
```

|                           |                     |                            |
|---------------------------|---------------------|----------------------------|
| <b>Syntax Description</b> | <b>ip</b>           | - IP Access List           |
|                           | <b>mac</b>          | - MAC Access List          |
|                           | <b>user-defined</b> | - user defined access list |

**Mode** Privileged/User EXEC Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show access-lists

```
EIP ACCESS LISTS
```

```
-----  
Standard IP Access List 34
```

```
-----  
IP address Type           : IPV4  
Source IP address        : 172.30.3.134  
Source IP address mask   : 255.255.255.255  
Source IP Prefix Length  : 32  
Destination IP address   : 0.0.0.0  
Destination IP address mask : 0.0.0.0  
Destination IP Prefix Length : 0  
Flow Identifier          : 0  
In Port List             : NIL  
Out Port List            : NIL  
Filter Action            : Deny  
Status                   : InActive
```

```
Extended IP Access List 1002
```

```
-----  
Filter Priority           : 1  
Filter Protocol Type     : ANY  
IP address Type          : IPV4  
Source IP address        : 0.0.0.0  
Source IP address mask   : 0.0.0.0  
Source IP Prefix Length  : 0  
Destination IP address   : 0.0.0.0  
Destination IP address mask : 0.0.0.0  
Destination IP Prefix Length : 0  
Flow Identifier          : 0
```

```

In Port List           : NIL
Out Port List         : NIL
Filter TOS             : Invalid combination
Filter DSCP           : NIL
Filter Action         : Permit
Status                : InActive

```

#### Extended IP Access List 10022

```

-----
Filter Priority        : 1
Filter Protocol Type  : ANY
IP address Type       : IPV4
Source IP address     : 0.0.0.0
Source IP address mask : 0.0.0.0
Source IP Prefix Length : 0
Destination IP address : 0.0.0.0
Destination IP address mask : 0.0.0.0
Destination IP Prefix Length : 0
Flow Identifier       : 0
In Port List         : NIL
Out Port List       : NIL
Filter TOS          : Invalid combination
Filter DSCP         : NIL
Filter Action       : Permit
Status             : InActive

```

#### MAC ACCESS LISTS

No MAC Access Lists have been configured

#### Related Commands

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **user-defined access-list** - Creates user defined access-list.
- **traffic-separation control** - Specifies globally the method to be implemented for carrying control packets to CPU
- **userdefined-list** - Creates a user defined access list by applying AND, OR, NOT operation on existing ACL rules
- **permit usr-defined-packet-type** - Permits Packet Based on User Defined Packet Byte
- **deny usr-defined-packet-type** - This command denies packet based on user defined byte.
- **permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters
- **deny - standard mode** - Denies traffic if the conditions defined in the deny

statement are matched

- **copy-to-cpu - standard mode** - Copies the IP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- **permit ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- **permit ipv6** - Specifies IP packets to be forwarded based on protocol and associated parameters.
- **deny ip/ospf/pim/protocol type** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- **copy-to-cpu - ip / ospf / pim / protocol-type** - Copies the IP control packets of all type of protocols to control plane CPU with or without switching of packets based on the configured parameters.
- **deny ipv6** - Specifies IPv6 packets to be rejected based on protocol and associated parameters.
- **copy-to-cpu ipv6** - Copies the IPv6 control packets to control plane CPU with or without switching of packets based on the configured parameters.
- **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters
- **deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters
- **copy-to-cpu tcp** - Copies the TCP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- **permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters
- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters
- **copy-to-cpu udp** - Copies the UDP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- **copy-to-cpu icmp** - Copies the ICMP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- **ip access-group** - Enables access control for the packets on the interface
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **user-defined access-group** - Applies a user defined access list (ACL) to an interface
- **permit - MAC** - Specifies the packets to be forwarded based on the MAC address and the associated parameters

- **deny - MAC** - specifies the packets to be rejected based on the MAC address and the associated parameters
- **copy-to-cpu - MAC** - Copies the MAC protocol control packets to control plane CPU with or without switching of packets based on the configured parameters.

## 65.2 BCM Specific Commands

This section describes the CLI commands executable only in BCM target for configuring ACL feature supported by ISS.

The list of CLI commands for the configuration of ACL is as follows:

- ip access-list
- mac access-list extended
- permit - standard mode
- deny - standard mode
- permit- ip/ospf/pim/protocol type
- permit ipv6
- deny ipv6
- deny - ip/ospf/pim/protocol type
- permit tcp
- deny tcp
- permit udp
- deny udp
- permit icmp
- deny icmp
- ip access-group
- mac access-group
- permit
- deny
- show access-lists

## 65.2.1 ip access-list

This command creates IP ACLs and enters the IP Access-list configuration mode. Standard access lists create filters based on IP address and network mask only (L3 filters only). Extended access lists enables specification of filters based on the type of protocol, range of TCP/UDP ports as well as the IP address and network mask (Layer 4 filters).

Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode.

The no form of the command deletes the IP access-list.

```
ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> }
```

```
no ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> }
```

|                           |                 |   |                             |
|---------------------------|-----------------|---|-----------------------------|
| <b>Syntax Description</b> | <b>standard</b> | - | Standard access-list number |
|                           | <b>extended</b> | - | Extended access-list number |

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config)# ip access-list standard 1`



ACLs on the system perform both access control and Layer 3 field classification. To define Layer 3 fields' access-lists the `ip access-list` command must be used.

**Related Commands**

- `permit - standard mode` - Specifies the packets to be forwarded depending upon the associated parameters
- `deny - standard mode` - Denies traffic if the conditions defined in the deny statement are matched
- `permit- ip/ospf/pim/protocol type` - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- `deny - ip/ospf/pim/protocol type` - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- `permit tcp` - Specifies the TCP packets to be forwarded based on the associated parameters
- `deny tcp` - Specifies the TCP packets to be rejected based on the associated parameters
- `permit udp` - Specifies the UDP packets to be forwarded based on the

associated parameters

- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- **ip access-group** - Enables access control for the packets on the interface
- **show access-lists** - Displays the access list configuration

## 65.2.2 mac access-list extended

This command creates Layer 2 MAC ACLs, that is, this command creates a MAC access-list and returns the MAC-Access list configuration mode to the user. The no form of the command deletes the MAC access-list.

```
mac access-list extended <access-list-number (1-65535)>
```

```
no mac access-list extended <short (1-65535)>
```

**Syntax Description**      **access-**                      -    Access list number  
**list-number**

**Mode**                      Global Configuration Mode

**Package**                  Workgroup, Enterprise and Metro

**Example**                  `iss(config)# mac access-list extended 5`



ACLs on the system perform both access control and layer 2 field classification. To define Layer 2 access lists, the mac access-list command must be used.

**Related Commands**

- **show access-lists** - Displays the access list configuration
- **permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **deny** - Specifies the packets to be rejected based on the MAC address and the associated parameters

## 65.2.3 permit - standard mode

This command specifies the packets to be forwarded depending upon the associated parameters. Standard IP access lists use source addresses for matching operations.

```
permit { any | host <src-ip-address> | < src-ip-address> <mask> } [{ any |
host <dest-ip-address> | < dest-ip-address> <mask> } ]
```

### For Metro

```
permit { any | host <src-ip-address> | <network-src-ip> <mask> } [ { any |
host <dest-ip-address> | <network-dest-ip> <mask> } ]
```

|                    |                                                                                            |                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>any host</b>                                                                            | - Source IP address can be                                                                                                                                                                                                                                                         |
| <b>Description</b> | <b>&lt;src-ip-address&gt; <br/>&lt; src-ip-<br/>address&gt;&lt;mask&gt;</b>                | <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- the host that the packet is from and the network mask to use with the source IP address</li> </ul>                                                       |
|                    | <b>any host<br/>&lt;dest-ip-address&gt; <br/>&lt; dest-ip-<br/>address&gt;&lt;mask&gt;</b> | <ul style="list-style-type: none"> <li>- Destination IP address can be</li> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- the host that the packet is destined for and the network mask to use with the destination IP address</li> </ul> |

**Mode** IP ACL Configuration (standard)

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config-std-nacl)# permit host 100.0.0.10 host 10.0.0.1`

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched
- **show access-lists** - Displays the access list configuration

## 65.2.4 deny - standard mode

This command denies traffic if the conditions defined in the deny statement are matched.

```
deny{ any | host <src-ip-address> | <src-ip-address> <mask> } [ { any | host
<dest-ip-address> | <dest-ip-address> <mask> } ]
```

### For Metro

```
deny{ any | host <src-ip-address> | <network-src-ip> <mask> } [ { any | host
<dest-ip-address> | <network-dest-ip> <mask> } ]
```

|                         |                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                    |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>           | <b>any host</b>                                                                                                                                                                                                                                                                                                                                     | - Source IP address can be                                                                                                                                                                                                                                         |
| <b>Description</b>      | <b>src-ip-address </b><br><b>&lt;src-ip-address&gt;</b><br><b>&lt;mask&gt;</b>                                                                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is from and the network mask to use with the source IP address</li> </ul>              |
|                         | <b>any host</b>                                                                                                                                                                                                                                                                                                                                     | - Destination IP address can be                                                                                                                                                                                                                                    |
|                         | <b>dest-ip-address </b><br><b>&lt;dest-ip-</b><br><b>address&gt;&lt;mask&gt;</b>                                                                                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is destined for and the network mask to use with the destination IP address</li> </ul> |
| <b>Mode</b>             | IP ACL Configuration (standard)                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                    |
| <b>Package</b>          | Workgroup, Enterprise and Metro                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                    |
| <b>Example</b>          | iss(config-std-nacl)# deny host 100.0.0.10 any                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                    |
| <b>Related Commands</b> | <ul style="list-style-type: none"> <li>• <b>ip access-list</b> - Creates IP ACLs and enters the IP Access-list configuration mode</li> <li>• <b>permit - standard mode</b> - Specifies the packets to be forwarded depending upon the associated parameters</li> <li>• <b>show access-lists</b> - Displays the access list configuration</li> </ul> |                                                                                                                                                                                                                                                                    |

## 65.2.5 permit- ip/ospf/pim/protocol type

This command allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.

```
permit { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>} ] [ priority <value (1-255)>]
```

### For Metro

```
permit { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>} ] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value (0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                                               |                                                                                                                                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | ip  ospf pim <br><protocol-type (1-255)>                      | - Type of protocol for the packet. It can also be a protocol number.                                                                                                                                                                                                                            |
|                           | any  host<br><src-ip-address> <br><src-ip-address><br><mask>  | - Source IP address can be <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is from and the network mask to use with the source address.</li> </ul>                  |
|                           | any host<br><dest-ip-address> <br><dest-ip-address><br><mask> | - Destination IP address can be <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> |
|                           | tos                                                           | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                                                              |
|                           | priority                                                      | - The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies                                                                                                            |

a higher priority.

**svlan-id** - Service VLAN value to match against incoming packets.

**svlan-priority** - Service VLAN priority value to match against incoming packets.

**cvlan-id** - Customer VLAN value to match against incoming packets.

**cvlan-priority** - Customer VLAN priority value to match against incoming packets.

**single-tag** - Filter to be applied on Single VLAN tagged packets.

**double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults**

|                         |   |            |
|-------------------------|---|------------|
| protocol-type           | - | 255        |
| priority                | - | 1          |
| svlan-id                | - | 0          |
| svlan-priority          | - | -1         |
| cvlan-id                | - | 0          |
| cvlan-priority          | - | -1         |
| single-tag   double-tag | - | Single tag |

**Example** `iss(config-ext-nacl)# permit 200 host 100.0.0.10 any tos 6`



- Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.
- Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related  
Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **deny - ip/ospf/pim/protocol type** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched

## 65.2.6 permit ipv6

This command specifies IP packets to be forwarded based on protocol and associated parameters.

```
permit ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr>
<integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> }}
```

|                           |                                                           |   |                                             |
|---------------------------|-----------------------------------------------------------|---|---------------------------------------------|
| <b>Syntax Description</b> | <b>flow-label</b>                                         | - | Flow identifier in IPv6 header.             |
|                           | <b>any   host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</b> | - | Source address of the host / any host.      |
|                           | <b>any   host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</b> | - | Destination address of the host / any host. |

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup and Enterprise

**Example**

```
iss(config-ext-nacl)# permit ipv6 host c004::04 28 any
iss(config-ext-nacl)# permit ipv6 flow-label 40
```



Flow label cannot be configured along with either source/destination IP address.

**Related Commands** `show access-lists` - Displays the access lists configuration.

## 65.2.7 deny ipv6

This command specifies IPv6 packets to be rejected based on protocol and associated parameters.

```
deny ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr> <integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> } }
```

|                           |                                                                                      |   |                                             |
|---------------------------|--------------------------------------------------------------------------------------|---|---------------------------------------------|
| <b>Syntax Description</b> | <b>flow-label</b>                                                                    | - | Flow identifier in IPv6 header.             |
|                           | <b>any</b>   <b>host</b><br><b>&lt;ip6_addr&gt;</b><br><b>&lt;integer(0-128)&gt;</b> | - | Source address of the host / any host.      |
|                           | <b>any</b>   <b>host</b><br><b>&lt;ip6_addr&gt;</b><br><b>&lt;integer(0-128)&gt;</b> | - | Destination address of the host / any host. |

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup and Enterprise

**Example**

```
iss(config-ext-nacl)# deny ipv6 host c004::04 28 any
iss(config-ext-nacl)# deny ipv6 flow-label 40
```



Flow label cannot be configured along with either source/destination IP address.

**Related Commands** **show access-lists** - Displays the access lists configuration.

## 65.2.8 deny - ip/ospf/pim/protocol type

This command denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.

```
deny { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>} ] [ priority <value (1-255)>]
```

### For Metro

```
deny { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>} ] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-4094)>] [ svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value (0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                                               |                                                                                                                                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | ip  ospf pim <br><protocol-type<br>(1-255)>                   | - Type of protocol for the packet. It can also be a protocol number.                                                                                                                                                                                                                            |
|                           | any  host<br><src-ip-address> <br><src-ip-address><br><mask>  | - Source IP address can be <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul>                   |
|                           | any host<br><dest-ip-address> <br><dest-ip-address><br><mask> | - Destination IP address can be <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> |
|                           | tos                                                           | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                                                              |
|                           | priority                                                      | - The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority'                                                                                                                    |

implies a higher priority.

- svlan-id** - Service VLAN value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults**

- protocol type - 255
- priority - 1
- svlan-id - 0
- svlan-priority - -1
- cvlan-id - 0
- cvlan-priority - -1
- single-tag | double-tag - Single tag

**Example** `iss(config-ext-nacl)# deny ospf any host 10.0.0.1 tos max-throughput`



- Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.
- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related  
Commands**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit- ip/ospf/pim/protocol type` - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- `show access-lists` - Displays the access list configuration

## 65.2.9 permit tcp

This command specifies the TCP packets to be forwarded based on the associated parameters.

```
permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp <value (0-
63)>}] [ priority <short (1-255)>]
```

### For Metro

```
permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp <value (0-
63)>}] [ priority <short (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-
priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value
(0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                    |                                                                                                                                                                                                                                                                                                                          |
|---------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>tcp</b>                         | - Transport Control Protocol                                                                                                                                                                                                                                                                                             |
|                           | <b>any  host</b>                   | - Source IP address can be                                                                                                                                                                                                                                                                                               |
|                           | <b>&lt;src-ip-address&gt; </b>     | - 'any' or                                                                                                                                                                                                                                                                                                               |
|                           | <b>&lt;src-ip-address&gt; &lt;</b> | - the word 'host' and the dotted decimal address or                                                                                                                                                                                                                                                                      |
|                           | <b>src-mask &gt;</b>               | - number of the network or the host that the packet is from and the network mask to use with the source address                                                                                                                                                                                                          |
|                           | <b>port-number</b>                 | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators. <ul style="list-style-type: none"> <li>- eq=equal</li> <li>- lt=less than</li> <li>- gt=greater than</li> <li>- range=a range of ports; two different port numbers must be specified</li> </ul> |

- any | host** - Destination IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is destined for and the network mask to use with the destination address
- <dest-ip-address> | <dest-ip-address> < dest-mask >**
- ack** - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3).
- rst** - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3).
- tos** - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.
- priority** - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
- svlan-id** - Service VLAN value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

|                 |                         |                                                                                       |
|-----------------|-------------------------|---------------------------------------------------------------------------------------|
| <b>Defaults</b> | tos-value               | - 0                                                                                   |
|                 | ack                     | - 'any' (3) [indicates that the TCP ACK bit will not be checked to decide the action] |
|                 | rst                     | - any' (3) [indicates that the TCP RST bit will not be checked to decide the action]  |
|                 | svlan-id                | - 0                                                                                   |
|                 | svlan-priority          | - -1                                                                                  |
|                 | cvlan-id                | - 0                                                                                   |
|                 | cvlan-priority          | - -1                                                                                  |
|                 | single-tag   double-tag | - Single tag                                                                          |

**Example** `iss(config-ext-nacl)# permit tcp any 10.0.0.1 255.255.255.255`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters

## 65.2.10 deny tcp

This command specifies the TCP packets to be rejected based on the associated parameters.

```
deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}] | dscp <value
(0-63)>}] [ priority <short (1-255)>]
```

### For Metro

```
deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}] | dscp <value
(0-63)>}] [ priority <short (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-
priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value
(0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                |                                                                                                                                                                                                                               |
|---------------------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>tcp</b>                     | - Transmission control protocol                                                                                                                                                                                               |
|                           | <b>any  host</b>               | - Source IP address can be                                                                                                                                                                                                    |
|                           | <b>&lt;src-ip-address&gt; </b> | - 'any' or                                                                                                                                                                                                                    |
|                           | <b>&lt;src-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address or                                                                                                                                                                           |
|                           | <b>&lt;src-mask&gt;</b>        | - number of the network or the host that the packet is from and the network mask to use with the source address                                                                                                               |
|                           | <b>port-number</b>             | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.<br>- eq=equal<br>- lt=less than<br>- gt=greater than<br>- range=a range of ports; two different port |

numbers must be specified

- |                                 |                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>any host</b>                 | - Destination IP address can be                                                                                                                                                                      |
| <b>&lt;dest-ip-address&gt; </b> | - 'any' or                                                                                                                                                                                           |
| <b>&lt;dest-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address or                                                                                                                                                  |
| <b>&lt;dest-mask&gt;</b>        | - number of the network or the host that the packet is destined for and the network mask to use with the destination address                                                                         |
| <b>ack</b>                      | - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3)                                                                                                |
| <b>rst</b>                      | - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3)                                                                                                             |
| <b>tos</b>                      | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.   |
| <b>priority</b>                 | - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. |
| <b>svlan-id</b>                 | - Service VLAN value to match against incoming packets.                                                                                                                                              |
| <b>svlan-priority</b>           | - Service VLAN priority value to match against incoming packets.                                                                                                                                     |
| <b>cvlan-id</b>                 | - Customer VLAN value to match against incoming packets.                                                                                                                                             |
| <b>cvlan-priority</b>           | - Customer VLAN priority value to match against incoming packets.                                                                                                                                    |
| <b>single-tag</b>               | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                                |
| <b>double-tag</b>               | - Filter to be applied on double VLAN tagged packets.                                                                                                                                                |

|                 |                                             |                                                                                   |
|-----------------|---------------------------------------------|-----------------------------------------------------------------------------------|
| <b>Mode</b>     | ACL Extended Access List Configuration Mode |                                                                                   |
| <b>Package</b>  | Workgroup, Enterprise and Metro             |                                                                                   |
| <b>Defaults</b> | tos-value                                   | - 0                                                                               |
|                 | ack                                         | - 'any' (3) [indicates that TCP ACK bit will not be checked to decide the action] |
|                 | rst                                         | - any' (3) [indicates that TCP RST bit will not be checked to decide the action]  |
|                 | svlan-id                                    | - 0                                                                               |
|                 | svlan-priority                              | - -1                                                                              |
|                 | cvlan-id                                    | - 0                                                                               |
|                 | cvlan-priority                              | - -1                                                                              |
|                 | single-tag   double-tag                     | - Single tag                                                                      |

**Example**      `iss(config-ext-nacl)# deny tcp 100.0.0.10 255.255.255.0 eq 20 any`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters

## 65.2.11 permit udp

This command specifies the UDP packets to be forwarded based on the associated parameters.

```
permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [ { gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)> } ] [ { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } ] [ { gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-
number (1-65535)> <port-number (1-65535)> } ] [ { tos { max-reliability | max-
throughput | min-delay | normal | <tos-value (0-7)> } | dscp <value (0-63)> } ] [
priority <(1-255)> ]
```

### For Metro

```
permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [ { gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)> } ] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [ { gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)> } ] [ { tos { max-reliability | max-
throughput | min-delay | normal | <tos-value (0-7)> } | dscp <value (0-63)> } ] [
priority <short (1-255)> ] [ svlan-id <vlan-id (1-4094)> ] [ svlan-priority
<value (0-7)> ] [ cvlan-id <vlan-id (1-4094)> ] [ cvlan-priority <value (0-7)> ]
[ { single-tag | double-tag } ]
```

|                           |                                                                         |                                                                                                                                                                                                                                                                                                |
|---------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>udp</b>                                                              | - User Datagram Protocol                                                                                                                                                                                                                                                                       |
| <b>any   host</b>         | <b>&lt;src-ip-address&gt;   &lt;src-ip-address&gt; &lt;src-mask&gt;</b> | - Source IP address can be <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul>                  |
| <b>port-number</b>        |                                                                         | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators. <ul style="list-style-type: none"> <li>- eq=equal</li> <li>- lt=less than</li> <li>- gt=greater than</li> <li>- range=a range of ports; two different port</li> </ul> |

numbers must be specified

- |                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>any host &lt;dest-ip-address&gt;  &lt;dest-ip-address&gt; &lt;dest-mask&gt;</pre>                                   | <ul style="list-style-type: none"> <li>- Destination IP address can be           <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> </li> </ul> |
| <pre>tos {max-reliability   max-throughput   min-delay   normal   &lt;value (0-7)&gt;   dscp &lt;value (0-63)&gt;}</pre> | <ul style="list-style-type: none"> <li>- Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.</li> </ul>                                                                                                         |
| <pre>priority</pre>                                                                                                      | <ul style="list-style-type: none"> <li>- The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.</li> </ul>                                                                                                       |
| <pre>svlan-id</pre>                                                                                                      | <ul style="list-style-type: none"> <li>- Service VLAN value to match against incoming packets.</li> </ul>                                                                                                                                                                                                                                                    |
| <pre>svlan-priority</pre>                                                                                                | <ul style="list-style-type: none"> <li>- Service VLAN priority value to match against incoming packets.</li> </ul>                                                                                                                                                                                                                                           |
| <pre>cvlan-id</pre>                                                                                                      | <ul style="list-style-type: none"> <li>- Customer VLAN value to match against incoming packets.</li> </ul>                                                                                                                                                                                                                                                   |
| <pre>cvlan-priority</pre>                                                                                                | <ul style="list-style-type: none"> <li>- Customer VLAN priority value to match against incoming packets.</li> </ul>                                                                                                                                                                                                                                          |
| <pre>single-tag</pre>                                                                                                    | <ul style="list-style-type: none"> <li>- Filter to be applied on Single VLAN tagged packets.</li> </ul>                                                                                                                                                                                                                                                      |
| <pre>double-tag</pre>                                                                                                    | <ul style="list-style-type: none"> <li>- Filter to be applied on double VLAN tagged packets.</li> </ul>                                                                                                                                                                                                                                                      |

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

---

|                 |                         |   |            |
|-----------------|-------------------------|---|------------|
| <b>Defaults</b> | svlan-id                | - | 0          |
|                 | svlan-priority          | - | -1         |
|                 | cvlan-id                | - | 0          |
|                 | cvlan-priority          | - | -1         |
|                 | single-tag   double-tag | - | Single tag |

**Example** `iss(config-ext-nacl)# permit udp any gt 65000 any dscp 1`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related  
Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters

## 65.2.12 deny udp

This command specifies the UDP packets to be rejected based on the associated parameters.

```
deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask>} [{gt
<port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{ gt <port-number (1-
65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)>| range <port-
number (1-65535)> <port-number (1-65535)>}] [{tos{max-reliability|max-
throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [
priority <(1-255)>]
```

### For Metro

```
deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask>} [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{ gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{tos{max-reliability|max-
throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [
priority <short (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-priority
<value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value (0-7)>]
[ { single-tag | double-tag } ]
```

|                                |            |                                                                                                                          |
|--------------------------------|------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b>      | <b>udp</b> | - User Datagram Protocol                                                                                                 |
| <b>any  host</b>               |            | - Source IP address can be                                                                                               |
| <b>&lt;src-ip-address&gt; </b> |            | - 'any' or                                                                                                               |
| <b>&lt;src-ip-address&gt;</b>  |            | - the word 'host' and the dotted decimal address                                                                         |
| <b>&lt;src-mask&gt;</b>        |            | or                                                                                                                       |
|                                |            | - number of the network or the host that the packet is from and the network mask to use with the source address          |
| <b>port-number</b>             |            | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators. |
|                                |            | - eq=equal                                                                                                               |
|                                |            | - lt=less than                                                                                                           |
|                                |            | - gt=greater than                                                                                                        |
|                                |            | - range=a range of ports; two different port numbers must be specified                                                   |

|                                 |                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>any host</b>                 | - Destination IP address can be                                                                                                                                                                    |
| <b>&lt;dest-ip-address&gt;</b>  | - 'any' or                                                                                                                                                                                         |
| <b> &lt;dest-ip-address&gt;</b> | - the word 'host' and the dotted decimal address or                                                                                                                                                |
| <b>&lt;dest-mask&gt;</b>        | - number of the network or the host that the packet is destined for and the network mask to use with the destination address                                                                       |
|                                 |                                                                                                                                                                                                    |
| <b>tos</b>                      | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets. |
|                                 |                                                                                                                                                                                                    |
| <b>priority</b>                 | - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.  |
|                                 |                                                                                                                                                                                                    |
| <b>svlan-id</b>                 | - Service VLAN value to match against incoming packets.                                                                                                                                            |
|                                 |                                                                                                                                                                                                    |
| <b>svlan-priority</b>           | - Service VLAN priority value to match against incoming packets.                                                                                                                                   |
|                                 |                                                                                                                                                                                                    |
| <b>cvlan-id</b>                 | - Customer VLAN value to match against incoming packets.                                                                                                                                           |
|                                 |                                                                                                                                                                                                    |
| <b>cvlan-priority</b>           | - Customer VLAN priority value to match against incoming packets.                                                                                                                                  |
|                                 |                                                                                                                                                                                                    |
| <b>single-tag</b>               | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                              |
|                                 |                                                                                                                                                                                                    |
| <b>double-tag</b>               | - Filter to be applied on double VLAN tagged packets.                                                                                                                                              |
|                                 |                                                                                                                                                                                                    |
| <b>Mode</b>                     | ACL Extended Access List Configuration Mode                                                                                                                                                        |
|                                 |                                                                                                                                                                                                    |
| <b>Defaults</b>                 | svlan-id - 0                                                                                                                                                                                       |
|                                 | svlan-priority - -1                                                                                                                                                                                |
|                                 | cvlan-id - 0                                                                                                                                                                                       |

cvlan-priority - -1

single-tag | double-tag - Single tag

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config-ext-nacl)# deny udp host 10.0.0.1 any eq 20`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related  
Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters

## 65.2.13 permit icmp

This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.

```
permit icmp {any | host <src-ip-address> | <src-ip-address> <mask>} {any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
[<message-code (0-255)>] [ priority <(1-255)>]
```

### For Metro

```
permit icmp {any | host <src-ip-address> | <src-ip-address> <mask>} {any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
[<message-code (0-255)>] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-
4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-
priority <value (0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                 |                                                                                                                              |
|---------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>icmp</b>                     | - Internet Control Message Protocol                                                                                          |
|                           | <b>any  host</b>                | - Source IP address can be                                                                                                   |
|                           | <b>&lt;src-ip-address&gt;</b>   | - 'any' or                                                                                                                   |
|                           | <b> &lt;src-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address                                                                             |
|                           | <b>&lt;mask&gt;</b>             | or                                                                                                                           |
|                           |                                 | - number of the network or the host that the packet is from and the network mask to use with the source address              |
|                           | <b>any host</b>                 | - Destination IP address can be                                                                                              |
|                           | <b>&lt;dest-ip-address&gt; </b> | - 'any' or                                                                                                                   |
|                           | <b>&lt;dest-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address                                                                             |
|                           | <b>&lt;mask&gt;</b>             | or                                                                                                                           |
|                           |                                 | - number of the network or the host that the packet is destined for and the network mask to use with the destination address |
|                           | <b>message-type</b>             | - Message type                                                                                                               |
|                           | <b>message-code</b>             | - ICMP Message code                                                                                                          |
|                           | <b>priority</b>                 | - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than           |

one filter rules. Higher value of 'filter priority' implies a higher priority.

- svlan-id** - Service VLAN value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

- Defaults**
- message-type/message code - 255
  - svlan-id - 0
  - svlan-priority - -1
  - cvlan-id - 0
  - cvlan-priority - -1
  - single-tag | double-tag - Single tag

**Example** `iss(config-ext-nacl)# permit icmp any any`



- The ICMP message type can be one of the following:

| Value | ICMP type |
|-------|-----------|
|-------|-----------|

|     |                         |
|-----|-------------------------|
| 0   | Echo reply              |
| 3   | Destination unreachable |
| 4   | Source quench           |
| 5   | Redirect                |
| 8   | Echo request            |
| 11  | Time exceeded           |
| 12  | Parameter problem       |
| 13  | Timestamp request       |
| 14  | Timestamp reply         |
| 15  | Information request     |
| 16  | Information reply       |
| 17  | Address mask request    |
| 18  | Address mask reply      |
| 155 | No ICMP type            |

- The ICMP code can be any of the following:

| - Value | ICMP code                                       |
|---------|-------------------------------------------------|
| - 0     | Network unreachable                             |
| - 1     | Host unreachable                                |
| - 2     | Protocol unreachable                            |
| - 3     | Port unreachable                                |
| - 4     | Fragment need                                   |
| - 5     | Source route fail                               |
| - 6     | Destination network unknown                     |
| - 7     | Destination host unknown                        |
| - 8     | Source host isolated                            |
| - 9     | Destination network administratively prohibited |
| - 10    | Destination host administratively prohibited    |
| - 11    | Network unreachable TOS                         |
| - 12    | Host unreachable TOS                            |
| - 255   | No ICMP code                                    |

- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related**

- `ip access-list` - Created IP ACLs and enters the IP Access-list configuration

**Commands**

mode

- **show access-lists** - Displays the access list configuration
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters

## 65.2.14 deny icmp

This command specifies the ICMP packets to be rejected based on the IP address and associated parameters.

```
deny icmp {any | host <src-ip-address>|<src-ip-address> <mask>}{any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
 [<message-code (0-255)>] [ priority <(1-255)>]
```

### For Metro

```
deny icmp {any | host <src-ip-address>|<src-ip-address> <mask>} {any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
 [<message-code (0-255)>] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-
4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-
priority <value (0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                 |                                                                                                                              |
|---------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>icmp</b>                     | - Internet Control Message Protocol                                                                                          |
|                           | <b>any  host</b>                | - Source IP address can be                                                                                                   |
|                           | <b>&lt;src-ip-address&gt; </b>  | - 'any' or                                                                                                                   |
|                           | <b>&lt;src-ip-address&gt;</b>   | - the word 'host' and the dotted decimal address or                                                                          |
|                           | <b>&lt;mask&gt;</b>             | - number of the network or the host that the packet is from and the network mask to use with the source address              |
|                           | <b>any host</b>                 | - Destination IP address can be                                                                                              |
|                           | <b>&lt;dest-ip-address&gt; </b> | - 'any' or                                                                                                                   |
|                           | <b>&lt;dest-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address or                                                                          |
|                           | <b>&lt;mask&gt;</b>             | - number of the network or the host that the packet is destined for and the network mask to use with the destination address |
|                           | <b>message-type</b>             | - Message type                                                                                                               |
|                           | <b>message-code</b>             | - ICMP Message code                                                                                                          |
|                           | <b>priority</b>                 | - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than           |

one filter rules. Higher value of 'filter priority' implies a higher priority.

- svlan-id** - Service VLAN value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

- Defaults**
- message-type/  
message code - 255
  - svlan-id - 0
  - svlan-priority - -1
  - cvlan-id - 0
  - cvlan-priority - -1
  - single-tag | double-tag - Single tag

**Example** `iss(config-ext-nacl)# deny icmp host 100.0.0.10 10.0.0.1 255.255.255.255`



- The ICMP message type can be one of the following:

| Value | ICMP type |
|-------|-----------|
|-------|-----------|

|     |                         |
|-----|-------------------------|
| 0   | Echo reply              |
| 3   | Destination unreachable |
| 4   | Source quench           |
| 5   | Redirect                |
| 8   | Echo request            |
| 11  | Time exceeded           |
| 12  | Parameter problem       |
| 13  | Timestamp request       |
| 14  | Timestamp reply         |
| 15  | Information request     |
| 16  | Information reply       |
| 17  | Address mask request    |
| 18  | Address mask reply      |
| 155 | No ICMP type            |

- The ICMP code can be any of the following:

| Value | ICMP code                                       |
|-------|-------------------------------------------------|
| 0     | Network unreachable                             |
| 1     | Host unreachable                                |
| 2     | Protocol unreachable                            |
| 3     | Port unreachable                                |
| 4     | Fragment need                                   |
| 5     | Source route fail                               |
| 6     | Destination network unknown                     |
| 7     | Destination host unknown                        |
| 8     | Source host isolated                            |
| 9     | Destination network administratively prohibited |
| 10    | Destination host administratively prohibited    |
| 11    | Network unreachable TOS                         |
| 12    | Host unreachable TOS                            |
| 255   | No ICMP code                                    |

- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

#### Related Commands

- ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

- **show access-lists** - Displays the access list configuration
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters

## 65.2.15 ip access-group

This command enables access control for the packets on the interface. It controls access to a Layer 2 or Layer 3 interface. The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out.

```
ip access-group <access-list-number (1-65535)> {in | out}
```

```
no ip access-group [<access-list-number (1-65535)>] {in | out}
```

**Syntax Description**      **access-list-number** - IP access control list number

**in** - Inbound packets

**out** - Outbound packets

**Mode**                    Interface Configuration Mode

**Package**                Workgroup, Enterprise and Metro

**Example**                iss(config-if)# ip access-group 1 in



- IP access list must have been created.
- Following are the limitations for this command to be applicable to Layer 2 interfaces.
  - The out keyword is not supported by Layer 2 interfaces.
  - An IP ACL applied to a Layer 2 interface filters only the IP packets. MAC access-group interface configuration command with MAC extended ACLs must be used to filter non-IP packets.

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration

## 65.2.16 mac access-group

This command applies a MAC access control list (ACL) to a Layer 2 interface. The no form of this command can be used to remove the MAC ACLs from the interface.

```
mac access-group <access-list-number (1-65535)> {in | out}
```

```
no mac access-group [<access-list-number (1-65535)>] {in | out}
```

### For Metro

```
mac access-group <access-list-number (1-65535)> in
```

```
no mac access-group [<access-list-number (1-65535)>] in
```

|                           |                                                |
|---------------------------|------------------------------------------------|
| <b>Syntax Description</b> | <b>access-list-number</b> - Access List Number |
|                           | <b>in</b> - Inbound packets                    |
|                           | <b>out</b> - Outbound packets                  |

**Mode** Interface Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config-if)# mac access-group 5 in`



MAC access list must have been created.

- Related Commands**
- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
  - **show access-lists** - Displays the access list statistics

## 65.2.17 permit

This command specifies the packets to be forwarded based on the MAC address and the associated parameters, that is, this command allows non-IP traffic to be forwarded if the conditions are matched.

```
permit { any | host <src-mac-address> } { any | host <dest-mac-address> } [ aarp
| amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042
| lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-
echo | vines-ip | xns-id | <protocol (0-65535)> ] [ encaps-type <value (1-
65535)> ] [ Vlan <vlan-id (1-4094)> ] [ priority <value (1-255)> ]
```

### For Metro

```
permit { any | host <src-mac-address> } { any | host <dest-mac-address> } [ {
aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |
etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios
| vines-echo | vines-ip | xns-id | <short (0-65535)> } ] [ encaps-type <integer
(1-65535)> ] [ vlan <vlan-id (1-4094)> ] [ priority <short (1-255)> ] [
outerEtherType < integer (1-65535)> ] [ svlan-id <vlan-id (1-4094)> ] [ cvlan-
priority <value (0-7)> ] [ svlan-priority <value (0-7)> ] [ { single-tag |
double-tag } ]
```

|                    |                             |                                                                                                      |
|--------------------|-----------------------------|------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>any   host &lt;src-</b>  | - Source MAC address to be matched with the packet                                                   |
| <b>Description</b> | <b>mac-address &gt;</b>     |                                                                                                      |
|                    | <b>any   host &lt;dest-</b> | - Destination MAC address to be matched with the packet                                              |
|                    | <b>mac-address &gt;</b>     |                                                                                                      |
|                    | <b>aarp</b>                 | - Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address |
|                    | <b>amber</b>                | - EtherType DEC-Amber                                                                                |
|                    | <b>dec-spanning</b>         | - EtherType Digital Equipment Corporation (DEC) spanning tree                                        |
|                    | <b>decnet-iv</b>            | - EtherType DECnet Phase IV protocol                                                                 |
|                    | <b>diagnostic</b>           | - EtherType DEC-Diagnostic                                                                           |
|                    | <b>dsm</b>                  | - EtherType DEC-DSM/DDP                                                                              |
|                    | <b>etype-6000</b>           | - EtherType 0x6000                                                                                   |

---

|                       |   |                                                                                                                                                                                                      |
|-----------------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>etype-8042</b>     | - | EtherType 0x8042                                                                                                                                                                                     |
| <b>lat</b>            | - | EtherType DEC-LAT                                                                                                                                                                                    |
| <b>lavc-sca</b>       | - | EtherType DEC-LAVC-SCA                                                                                                                                                                               |
| <b>mop-console</b>    | - | EtherType DEC-MOP Remote Console                                                                                                                                                                     |
| <b>mop-dump</b>       | - | EtherType DEC-MOP Dump                                                                                                                                                                               |
| <b>msdos</b>          | - | EtherType DEC-MSDOS                                                                                                                                                                                  |
| <b>mumps</b>          | - | EtherType DEC-MUMPS                                                                                                                                                                                  |
| <b>netbios</b>        | - | EtherType DEC- Network Basic Input/Output System (NETBIOS)                                                                                                                                           |
| <b>vines-echo</b>     | - | EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems                                                                                                                        |
| <b>vines-ip</b>       | - | EtherType VINES IP                                                                                                                                                                                   |
| <b>xns-id</b>         | - | EtherType Xerox Network Systems (XNS) protocol suite                                                                                                                                                 |
| <b>encaptype</b>      | - | Encapsulation Type                                                                                                                                                                                   |
| <b>vlan</b>           | - | VLAN ID to be filtered                                                                                                                                                                               |
| <b>priority</b>       | - | The priority of the L2 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority |
| <b>outerEtherType</b> | - | EtherType value to match on Service vlan tag                                                                                                                                                         |
| <b>svlan-id</b>       | - | Service VLAN value to match against incoming packets.                                                                                                                                                |

- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL MAC Configuration Mode

**Package** Workgroup, Enterprise and Metro

- Defaults**
- vlan-id - 0
  - priority - 1
  - outerEtherType - 0
  - svlan-id - 0
  - cvlan-priority - -1
  - svlan-priority - -1
  - single-tag | double-tag - Single tag

**Example** `iss(config-ext-macl)# permit host 00:11:22:33:44:55 any aarp priority 10`



- MAC access list must have been created.
- OuterEtherType, Service Vlan, Service Vlan Priority and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **deny** - Specifies the packets to be rejected based on the MAC address and the associated parameters
- **show access-lists** - Displays the access list statistics

## 65.2.18 deny

This command specifies the packets to be rejected based on the MAC address and the associated parameters.

```
deny { any | host <src-mac-address> } { any | host <dest-mac-address> } [ aarp |
amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 |
lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo
| vines-ip | xns-id | <protocol (0-65535)> ] [ encapsype <value (1-65535)> ] [
Vlan <vlan-id (1-4094)> ] [ priority <value (1-255)> ]
```

### For Metro

```
deny { any | host <src-mac-address> } { any | host <dest-mac-address> } [ {
aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |
etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios
| vines-echo | vines-ip | xns-id | <short (0-65535)> } ] [ encapsype <integer
(1-65535)> ] [ vlan <vlan-id (1-4094)> ] [ priority <short (1-255)> ] [
outerEtherType < integer (1-65535)> ] [ svlan-id <vlan-id (1-4094)> ] [ cvlan-
priority <priority (0-7)> ] [ svlan-priority <value (0-7)> ] [ { single-tag |
double-tag } ]
```

|                           |                                             |                                                                                                      |
|---------------------------|---------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>any   host &lt;src-mac-address &gt;</b>  | - Source MAC address to be matched with the packet                                                   |
|                           | <b>any   host &lt;dest-mac-address &gt;</b> | - Destination MAC address to be matched with the packet                                              |
|                           | <b>aarp</b>                                 | - EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address |
|                           | <b>amber</b>                                | - EtherType DEC-Amber                                                                                |
|                           | <b>dec-spanning</b>                         | - EtherType Digital Equipment Corporation (DEC) spanning tree                                        |
|                           | <b>decent-iv</b>                            | - EtherType DECnet Phase IV protocol                                                                 |
|                           | <b>diagnostic</b>                           | - EtherType DEC-Diagnostic                                                                           |
|                           | <b>dsm</b>                                  | - EtherType DEC-DSM/DDP                                                                              |

|                       |                                                                                                                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>etype-6000</b>     | - EtherType 0x6000                                                                                                                                                                                      |
| <b>etype-8042</b>     | - EtherType 0x8042                                                                                                                                                                                      |
| <b>lat</b>            | - EtherType DEC-LAT                                                                                                                                                                                     |
| <b>lavc-sca</b>       | - EtherType DEC-LAVC-SCA                                                                                                                                                                                |
| <b>mop-console</b>    | - EtherType DEC-MOP Remote Console                                                                                                                                                                      |
| <b>mop-dump</b>       | - EtherType DEC-MOP Dump                                                                                                                                                                                |
| <b>msdos</b>          | - EtherType DEC-MSDOS                                                                                                                                                                                   |
| <b>mumps</b>          | - EtherType DEC-MUMPS                                                                                                                                                                                   |
| <b>netbios</b>        | - EtherType DEC- Network Basic Input/Output System (NETBIOS)                                                                                                                                            |
| <b>vines-echo</b>     | - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems                                                                                                                         |
| <b>vines-ip</b>       | - EtherType VINES IP                                                                                                                                                                                    |
| <b>xns-id</b>         | - EtherType Xerox Network Systems (XNS) protocol suite                                                                                                                                                  |
| <b>encaptype</b>      | - Encapsulation Type                                                                                                                                                                                    |
| <b>vlan</b>           | - VLAN ID to be filtered                                                                                                                                                                                |
| <b>priority</b>       | - The priority of the L2 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. |
| <b>outerEtherType</b> | - EtherType value to match on Service vlan tag                                                                                                                                                          |
| <b>svlan-id</b>       | - Service VLAN value to match against incoming packets.                                                                                                                                                 |

- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL MAC Configuration Mode

**Package** Workgroup, Enterprise and Metro

- Defaults**
- vlan-id - 0
  - priority - 1
  - outerEtherType - 0
  - svlan-id - 0
  - cvlan-priority - -1
  - svlan-priority - -1
  - single-tag | double-tag - Single tag

**Example**

```
iss(config-ext-macl)# deny any host 00:11:22:33:44:55 priority 200
```



- MAC access list must have been created.
- OuterEtherType, Service Vlan, Service Vlan Priority and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **show access-lists** - Displays the access list statistics

## 65.2.19 show access-lists

This command displays the access lists configuration.

```
show access-lists [{"ip | mac}] <access-list-number (1-65535)> ]
```

|                    |            |                   |
|--------------------|------------|-------------------|
| <b>Syntax</b>      | <b>ip</b>  | - IP Access List  |
| <b>Description</b> | <b>mac</b> | - MAC Access List |

**Mode** Privileged/User EXEC Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show access-lists

```
EIP ACCESS LISTS
```

```
-----
```

```
Standard IP Access List 34
```

```
-----
```

```

IP address Type                : IPV4
Source IP address              : 172.30.3.134
Source IP address mask         : 255.255.255.255
Source IP Prefix Length        : 32
Destination IP address         : 0.0.0.0
Destination IP address mask    : 0.0.0.0
Destination IP Prefix Length   : 0
Flow Identifier                 : 0
In Port List                   : NIL
Out Port List                  : NIL
Filter Action                   : Deny
Status                          : InActive

```

```
Extended IP Access List 1002
```

```
-----
```

```
Filter Priority                 : 1
```

```

Filter Protocol Type           : ANY
IP address Type                : IPV4
Source IP address              : 0.0.0.0
Source IP address mask        : 0.0.0.0
Source IP Prefix Length       : 0
Destination IP address        : 0.0.0.0
Destination IP address mask   : 0.0.0.0
Destination IP Prefix Length  : 0
Flow Identifier                : 0
In Port List                   : NIL
Out Port List                  : NIL
Filter TOS                     : Invalid combination
Filter DSCP                    : NIL
Filter Action                  : Permit
Status                         : InActive

```

Extended IP Access List 10022

-----

```

Filter Priority                 : 1
Filter Protocol Type           : ANY
IP address Type                : IPV4
Source IP address              : 0.0.0.0
Source IP address mask        : 0.0.0.0
Source IP Prefix Length       : 0
Destination IP address        : 0.0.0.0
Destination IP address mask   : 0.0.0.0
Destination IP Prefix Length  : 0
Flow Identifier                : 0
In Port List                   : NIL
Out Port List                  : NIL
Filter TOS                     : Invalid combination
Filter DSCP                    : NIL
Filter Action                  : Permit
Status                         : InActive

```

## MAC ACCESS LISTS

-----

No MAC Access Lists have been configured



- OuterEtherType, Service Vlan, Service Vlan Priority, innerEtherType, Customer Vlan and Customer Vlan Priority options are applicable only with Metro Ethernet Feature and bridge mode is provider.

**Related  
Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters
- **deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched
- **permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- **deny - ip/ospf/pim/protocol type** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters
- **deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters
- **permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters
- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- **ip access-group** - Enables access control for the packets on the interface
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **deny** - specifies the packets to be rejected based on the MAC address and the associated parameters

---

## 65.3 CXE Specific Commands

This section describes the CLI commands executable only in CXE target for configuring ACL feature supported by ISS.

The list of CLI commands for the configuration of ACL is as follows:

- ip access-list
- mac access-list extended
- permit - standard mode
- deny - standard mode
- permit- ip/ospf/pim/protocol type
- deny - ip/ospf/pim/protocol type
- permit tcp
- deny tcp
- permit udp
- deny udp
- permit icmp
- deny icmp
- mac access-group
- permit
- deny
- show access-lists

## 65.3.1 ip access-list

This command creates IP ACLs and enters the IP Access-list configuration mode. Standard access lists create filters based on IP address and network mask only (L3 filters only). Extended access lists enables specification of filters based on the type of protocol, range of TCP/UDP ports as well as the IP address and network mask (Layer 4 filters).

Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode.

The no form of the command deletes the IP access-list.

```
ip access-list { standard <access-list-number (1-50)> | extended <access-list-number (51-90)>}
```

```
no ip access-list { standard <access-list-number (1-50)> | extended <access-list-number (51-90)>}
```

**Syntax Description**

**standard** - Standard access-list number

**extended** - Extended access-list number

**Mode** Global Configuration Mode

**Example** `iss(config)# ip access-list standard 1`



ACLs on the system perform both access control and Layer 3 field classification. To define Layer 3 fields' access-lists the **ip access-list** command must be used.

- Related Command**
- **permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters
  - **deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched
  - **permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
  - **deny - ip/ospf/pim/protocol type** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
  - **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters
  - **deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters
  - **permit udp** - Specifies the UDP packets to be forwarded based on the

---

associated parameters

- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- **show access-lists** - Displays the access list configuration

## 65.3.2 mac access-list extended

This command creates Layer 2 MAC ACLs, i.e. this command creates a MAC access-list and returns the MAC-Access list configuration mode to the user. The no form of the command deletes the MAC access-list.

```
mac access-list extended <access-list-number (1-50)>
```

```
no mac access-list extended <short (1-50)>
```

**Mode** Global Configuration Mode

**Example** `iss(config)# mac access-list extended 5`



ACLs on the system perform both access control and layer 2 field classification. To define Layer 2 access lists, the `mac access-list` command must be used.

**Related Command**

- **show access-lists** - Displays the access list configuration
- **permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **deny** - Specifies the packets to be rejected based on the MAC address and the associated parameters

### 65.3.3 permit - standard mode

This command specifies the packets to be forwarded depending upon the associated parameters. Standard IP access lists use source addresses for matching operations.

```
permit { any | host <src-ip-address> | <network-src-ip> <mask> } [{ any | host
<dest-ip-address> | <network-dest-ip> <mask> } ]
```

|                           |                                                                                 |                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <pre>any host &lt;src-ip-address&gt;  &lt;network-src-ip&gt; &lt;mask&gt;</pre> | <ul style="list-style-type: none"> <li>- Source IP address can be             <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is from and the network mask to use with the source IP address</li> </ul> </li> </ul> |
|---------------------------|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                   |                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>any host &lt;dest-ip-address&gt;  &lt;network-dest-ip&gt; &lt;mask&gt;</pre> | <ul style="list-style-type: none"> <li>- Destination IP address can be             <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is destined for and the network mask to use with the destination IP address</li> </ul> </li> </ul> |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Mode** IP ACL Configuration (standard)

**Example** `iss(config-std-nacl)# permit host 100.0.0.10 host 10.0.0.1`

- Related Command**
- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
  - **deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched
  - **show access-lists** - Displays the access list configuration

## 65.3.4 deny - standard mode

This command denies traffic if the conditions defined in the deny statement are matched.

```
deny{ any | host <src-ip-address> | <network-src-ip > <mask> } [ { any | host
<dest-ip-address> | <network-dest-ip> <mask> } ]
```

|                           |                                                                                 |                                                                                                                                                                                                                                                                                                                                     |
|---------------------------|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <pre>any host &lt;src-ip-address&gt;  &lt;network-src-ip&gt; &lt;mask&gt;</pre> | <ul style="list-style-type: none"> <li>- Source IP address can be <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is from and the network mask to use with the source IP address</li> </ul> </li> </ul> |
|---------------------------|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                   |                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>any host &lt;dest-ip-address&gt;  &lt;network-dest-ip&gt; &lt;mask&gt;</pre> | <ul style="list-style-type: none"> <li>- Destination IP address can be <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is destined for and the network mask to use with the destination IP address</li> </ul> </li> </ul> |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Mode** IP ACL Configuration (standard)

**Example** `iss(config-std-nacl)# deny host 100.0.0.10 any`

**Related Command**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit - standard mode` - Specifies the packets to be forwarded depending upon the associated parameters
- `show access-lists` - Displays the access list configuration

## 65.3.5 permit- ip/ospf/pim/protocol type

This command allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.

```
permit { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } [{tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>} ] [vlan <VlanID (1-4094)>]
```

|                           |                                                       |                                                                                                                                                                                                                                                                                                 |
|---------------------------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | ip  ospf pim  <protocol-type (1-255)>                 | - Type of protocol for the packet. It can also be a protocol number                                                                                                                                                                                                                             |
|                           | any  host <src-ip-address>   <src-ip-address> <mask>  | - Source IP address can be <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul>                   |
|                           | any host <dest-ip-address>   <dest-ip-address> <mask> | - Destination IP address can be <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> |
|                           | tos                                                   | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                                                              |
|                           | vlan                                                  | - VLAN to which the packet is classified at ingress                                                                                                                                                                                                                                             |
| <b>Mode</b>               | ACL Extended Access List Configuration Mode           |                                                                                                                                                                                                                                                                                                 |
| <b>Defaults</b>           | protocol-type                                         | - 255                                                                                                                                                                                                                                                                                           |
|                           | priority                                              | - 1                                                                                                                                                                                                                                                                                             |

**Example**      `iss(config-ext-nacl)# permit 200 host 100.0.0.10 any tos 6`



Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.

**Related Command**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access list configuration
- `deny - ip/ospf/pim/protocol type` - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched

## 65.3.6 deny - ip/ospf/pim/protocol type

This command denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.

```
deny { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-
address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-
ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay |
normal |<value (0-7)>} | dscp <value (0-63)>} ] [vlan <VlanID (1-4094)>]
```

|                           |                                                     |                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | ip  ospf pim  <protocol-type (1-255)>               | - Type of protocol for the packet. It can also be a protocol number                                                                                                                                                                                                                                                                                |
|                           | any  host <src-ip-address>  <src-ip-address> <mask> | <ul style="list-style-type: none"> <li>- Source IP address can be <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul> </li> </ul>                   |
|                           | any host <dest-ip-address> <dest-ip-address> <mask> | <ul style="list-style-type: none"> <li>- Destination IP address can be <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> </li> </ul> |
|                           | tos                                                 | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                                                                                                                 |
|                           | vlan                                                | - VLAN to which the packet is classified at ingress                                                                                                                                                                                                                                                                                                |
| <b>Mode</b>               | ACL Extended Access List Configuration Mode         |                                                                                                                                                                                                                                                                                                                                                    |
| <b>Defaults</b>           | protocol type                                       | - 255                                                                                                                                                                                                                                                                                                                                              |

priority - 1

**Example** `iss(config-ext-nacl)# deny ospf any host 10.0.0.1 tos max-throughput vlan 2`



Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.

**Related Command**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- **show access-lists** - Displays the access list configuration

## 65.3.7 permit tcp

This command specifies the TCP packets to be forwarded based on the associated parameters.

```
permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp <value (0-
63)>}] [vlan <VlanID (1-4094)>]
```

|                    |                                  |                                                                                                                              |
|--------------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>any   host</b>                | - Source IP address can be                                                                                                   |
| <b>Description</b> | <b>&lt;src-ip-address&gt;  </b>  | - 'any' or                                                                                                                   |
|                    | <b>&lt;src-ip-address&gt;</b>    | - the word 'host' and the dotted decimal address or                                                                          |
|                    | <b>&lt;src-mask&gt;</b>          | - number of the network or the host that the packet is from and the network mask to use with the source address              |
|                    | <b>port-number</b>               | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.     |
|                    |                                  | - eq=equal                                                                                                                   |
|                    |                                  | - lt=less than                                                                                                               |
|                    |                                  | - gt=greater than                                                                                                            |
|                    |                                  | - range=a range of ports; two different port numbers must be specified                                                       |
|                    | <b>any   host</b>                | - Destination IP address can be                                                                                              |
|                    | <b>&lt;dest-ip-address&gt;  </b> | - 'any' or                                                                                                                   |
|                    | <b>&lt;dest-ip-address&gt;</b>   | - the word 'host' and the dotted decimal address or                                                                          |
|                    | <b>&lt;dest-mask&gt;</b>         | - number of the network or the host that the packet is destined for and the network mask to use with the destination address |
|                    | <b>ack</b>                       | - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3).                       |
|                    | <b>rst</b>                       | - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3).                                    |

```

tos{
max-reliability |
max-throughput |
min-delay |
normal|

<value (0-7)> |
dscp<value (0-63)>

vlan

```

- Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.

- VLAN to which the packet is classified at ingress

**Mode** ACL Extended Access List Configuration Mode

**Defaults**

```

tos-value - 0

ack - 'any' (3) [indicates that TCP ACK bit will not be checked to decide the action]

rst - any' (3) [indicates that TCP RST bit will not be checked to decide the action]

```

**Example** `iss(config-ext-nacl)# permit tcp any 10.0.0.1 255.0.0.0`

**Related Command**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access list configuration
- `deny tcp` - Specifies the TCP packets to be rejected based on the associated parameters

## 65.3.8 deny tcp

This command specifies the TCP packets to be rejected based on the associated parameters.

```
deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value
(0-63)>}] [vlan <VlanID (1-4094)>]
```

|                    |                                 |                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>any  host</b>                | - Source IP address can be                                                                                                                                                                                                                              |
| <b>Description</b> | <b>&lt;src-ip-address&gt; </b>  | - 'any' or                                                                                                                                                                                                                                              |
|                    | <b>&lt;src-ip-address&gt;</b>   | - the word 'host' and the dotted decimal address or                                                                                                                                                                                                     |
|                    | <b>&lt;src-mask&gt;</b>         | - number of the network or the host that the packet is from and the network mask to use with the source address                                                                                                                                         |
|                    | <b>port-number</b>              | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.<br>- eq=equal<br>- lt=less than<br>- gt=greater than<br>- range=a range of ports; two different port numbers must be specified |
|                    | <b>any host</b>                 | - Destination IP address can be                                                                                                                                                                                                                         |
|                    | <b>&lt;dest-ip-address&gt; </b> | - 'any' or                                                                                                                                                                                                                                              |
|                    | <b>&lt;dest-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address or                                                                                                                                                                                                     |
|                    | <b>&lt;dest-mask&gt;</b>        | - number of the network or the host that the packet is destined for and the network mask to use with the destination address                                                                                                                            |
|                    | <b>ack</b>                      | - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3)                                                                                                                                                   |

|             |                                                                                                                                                                                                    |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>rst</b>  | - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3)                                                                                                           |
| <b>tos</b>  | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets. |
| <b>vlan</b> | VLAN to which the packet is classified at ingress                                                                                                                                                  |

**Mode** ACL Extended Access List Configuration Mode

|                 |                  |                                                                                   |
|-----------------|------------------|-----------------------------------------------------------------------------------|
| <b>Defaults</b> | <b>tos-value</b> | - 0                                                                               |
|                 | <b>ack</b>       | - 'any' (3) [indicates that TCP ACK bit will not be checked to decide the action] |
|                 | <b>rst</b>       | - 'any' (3) [indicates that TCP RST bit will not be checked to decide the action] |

**Example** `iss(config-ext-nacl)# deny tcp 100.0.0.10 255.0.0.0 eq 20 any`



- The TCP ACK bit to be checked against the packet can be establish (1), non-establish (2) or any (3). The default value is 'any' (3). It means that ACK bit will not be checked to decide the action.
- The TCP RST bit to be checked against the packet can be set (1), notset (2) or any (3). The default value is 'any' (3). It means that TCP RST bit will not be checked to decide the action.

- Related Command**
- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
  - **show access-lists** - Displays the access list configuration
  - **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters

## 65.3.9 permit udp

This command specifies the UDP packets to be forwarded based on the associated parameters.

```
permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask>} [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{ gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{tos{max-reliability|max-
throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [vlan
<VlanID (1-4094)>]
```

|                    |                                 |                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>any  host</b>                | - Source IP address can be                                                                                                                                                                                                                              |
| <b>Description</b> | <b>&lt;src-ip-address&gt; </b>  | - 'any' or                                                                                                                                                                                                                                              |
|                    | <b>&lt;src-ip-address&gt;</b>   | - the word 'host' and the dotted decimal address                                                                                                                                                                                                        |
|                    | <b>&lt;src-mask&gt;</b>         | or<br>- number of the network or the host that the packet is from and the network mask to use with the source address                                                                                                                                   |
|                    | <b>port-number</b>              | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.<br>- eq=equal<br>- lt=less than<br>- gt=greater than<br>- range=a range of ports; two different port numbers must be specified |
|                    | <b>any host</b>                 | - Destination IP address can be                                                                                                                                                                                                                         |
|                    | <b>&lt;dest-ip-address&gt; </b> | - 'any' or                                                                                                                                                                                                                                              |
|                    | <b>&lt;dest-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address                                                                                                                                                                                                        |
|                    | <b>&lt;dest-mask&gt;</b>        | or<br>- number of the network or the host that the packet is destined for and the network mask to use with the destination address.                                                                                                                     |
|                    | <b>tos {</b>                    | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                      |
|                    | <b>max-reliability  </b>        |                                                                                                                                                                                                                                                         |
|                    | <b>max-throughput  </b>         |                                                                                                                                                                                                                                                         |
|                    | <b>min-delay  normal </b>       |                                                                                                                                                                                                                                                         |

```
<value (0-7)>      |  
dscp<value (0-63)>
```

**vlan** - VLAN to which the packet is classified at ingress

**Mode** ACL Extended Access List Configuration Mode

**Example** `iss(config-ext-nacl)# permit udp any gt 65000 any dscp 1`

**Related Command**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters

## 65.3.10 deny udp

This command specifies the UDP packets to be rejected based on the associated parameters.

```
deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{ gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{tos{max-reliability|max-
throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [vlan
<VlanID (1-4094)>]
```

|                    |                                 |                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>any  host</b>                | - Source IP address can be                                                                                                                                                                                                                              |
| <b>Description</b> | <b>&lt;src-ip-address&gt; </b>  | - 'any' or                                                                                                                                                                                                                                              |
|                    | <b>&lt;src-ip-address&gt;</b>   | - the word 'host' and the dotted decimal address                                                                                                                                                                                                        |
|                    | <b>&lt;src-mask&gt;</b>         | or<br>- number of the network or the host that the packet is from and the network mask to use with the source address                                                                                                                                   |
|                    | <b>port-number</b>              | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.<br>- eq=equal<br>- lt=less than<br>- gt=greater than<br>- range=a range of ports; two different port numbers must be specified |
|                    | <b>any host</b>                 | - Destination IP address can be                                                                                                                                                                                                                         |
|                    | <b>&lt;dest-ip-address&gt; </b> | - 'any' or                                                                                                                                                                                                                                              |
|                    | <b>&lt;dest-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address                                                                                                                                                                                                        |
|                    | <b>&lt;dest-mask&gt;</b>        | or<br>- number of the network or the host that the packet is destined for and the network mask to use with the destination address                                                                                                                      |
|                    | <b>tos</b>                      | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                      |

**vlan** - VLAN to which the packet is classified at ingress

**Mode** ACL Extended Access List Configuration Mode

**Example** `iss(config-ext-nacl)# deny udp host 10.0.0.1 any eq 20`

**Related Command**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters

## 65.3.11 permit icmp

This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.

```
permit icmp {any | host <src-ip-address> | <src-ip-address> <mask>} {any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
[<message-code (0-255)>] [vlan <VlanID (1-4094)>]
```

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <p><b>any   host</b> - Source IP address can be</p> <p><b>&lt;src-ip-address&gt;  </b></p> <p><b>&lt;src-ip-address&gt;</b> - 'any' or</p> <p><b>&lt;mask&gt;</b> - the word 'host' and the dotted decimal address or</p> <p>- number of the network or the host that the packet is from and the network mask to use with the source address</p><br><p><b>any   host</b> - Destination IP address can be</p> <p><b>&lt;dest-ip-address&gt;  </b></p> <p><b>&lt;dest-ip-address&gt;</b> - 'any' or</p> <p><b>&lt;mask&gt;</b> - the word 'host' and the dotted decimal address or</p> <p>- number of the network or the host that the packet is destined for and the network mask to use with the destination address</p><br><p><b>message-type</b> - Message type</p><br><p><b>message-code</b> - Message code</p><br><p><b>vlan</b> - VLAN to which the packet is classified at ingress</p> |
| <b>Mode</b>               | ACL Extended Access List Configuration Mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Defaults</b>           | message-type/message code - 255                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Example</b>            | <pre>iss(config-ext-nacl)# permit icmp any any</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



- The ICMP message type can be one of the following:

| Value | ICMP type               |
|-------|-------------------------|
| 0     | Echo reply              |
| 3     | Destination unreachable |
| 4     | Source quench           |
| 5     | Redirect                |
| 8     | Echo request            |
| 11    | Time exceeded           |
| 12    | Parameter problem       |
| 13    | Timestamp request       |
| 14    | Timestamp reply         |
| 15    | Information request     |
| 16    | Information reply       |
| 17    | Address mask request    |
| 18    | Address mask reply      |
| 155   | No ICMP type            |

- The ICMP code can be any of the following:

| Value | ICMP code                                       |
|-------|-------------------------------------------------|
| 0     | Network unreachable                             |
| 1     | Host unreachable                                |
| 2     | Protocol unreachable                            |
| 3     | Port unreachable                                |
| 4     | Fragment need                                   |
| 5     | Source route fail                               |
| 6     | Destination network unknown                     |
| 7     | Destination host unknown                        |
| 8     | Source host isolated                            |
| 9     | Destination network administratively prohibited |
| 10    | Destination host administratively prohibited    |
| 11    | Network unreachable TOS                         |
| 12    | Host unreachable TOS                            |
| 255   | No ICMP code                                    |

#### Related Command

- **ip access-list** - Created IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration

- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters

## 65.3.12 deny icmp

This command specifies the ICMP packets to be rejected based on the IP address and associated parameters.

```
deny icmp {any | host <src-ip-address> | <src-ip-address> <mask>} {any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
[<message-code (0-255)>] [vlan <VlanID (1-4094)>]
```

|                    |                                                                               |                                                                                                                              |
|--------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>any   host</b>                                                             | - Source IP address can be                                                                                                   |
| <b>Description</b> | <b>&lt;src-ip-address&gt;  </b>                                               | - 'any' or                                                                                                                   |
|                    | <b>&lt;src-ip-address&gt;</b>                                                 | - the word 'host' and the dotted decimal address or                                                                          |
|                    | <b>&lt;mask&gt;</b>                                                           | - number of the network or the host that the packet is from and the network mask to use with the source address              |
|                    | <b>any   host</b>                                                             | - Destination IP address can be                                                                                              |
|                    | <b>&lt;dest-ip-address&gt;  </b>                                              | - 'any' or                                                                                                                   |
|                    | <b>&lt;dest-ip-address&gt;</b>                                                | - the word 'host' and the dotted decimal address or                                                                          |
|                    | <b>&lt;mask&gt;</b>                                                           | - number of the network or the host that the packet is destined for and the network mask to use with the destination address |
|                    | <b>message-type</b>                                                           | - Message type                                                                                                               |
|                    | <b>message-code</b>                                                           | - Message code                                                                                                               |
|                    | <b>vlan</b>                                                                   | - VLAN to which the packet is classified at ingress                                                                          |
| <b>Mode</b>        | ACL Extended Access List Configuration Mode                                   |                                                                                                                              |
| <b>Defaults</b>    | message-type/message code                                                     | - 255                                                                                                                        |
| <b>Example</b>     | <pre>iss(config-ext-nacl)# deny icmp host 100.0.0.10 10.0.0.1 255.0.0.0</pre> |                                                                                                                              |



- The ICMP message type can be one of the following:

| Value | ICMP type               |
|-------|-------------------------|
| 0     | Echo reply              |
| 3     | Destination unreachable |
| 4     | Source quench           |
| 5     | Redirect                |
| 8     | Echo request            |
| 11    | Time exceeded           |
| 12    | Parameter problem       |
| 13    | Timestamp request       |
| 14    | Timestamp reply         |
| 15    | Information request     |
| 16    | Information reply       |
| 17    | Address mask request    |
| 18    | Address mask reply      |
| 155   | No ICMP type            |

- The ICMP code can be any of the following:

| Value | ICMP code                                       |
|-------|-------------------------------------------------|
| 0     | Network unreachable                             |
| 1     | Host unreachable                                |
| 2     | Protocol unreachable                            |
| 3     | Port unreachable                                |
| 4     | Fragment need                                   |
| 5     | Source route fail                               |
| 6     | Destination network unknown                     |
| 7     | Destination host unknown                        |
| 8     | Source host isolated                            |
| 9     | Destination network administratively prohibited |
| 10    | Destination host administratively prohibited    |
| 11    | Network unreachable TOS                         |
| 12    | Host unreachable TOS                            |
| 255   | No ICMP code                                    |

**Related**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration

**Command**

mode

- **show access-lists** - Displays the access list configuration
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters

## 65.3.13 mac access-group

This command applies a MAC access control list (ACL) to a Layer 2 interface. The no form of this command can be used to remove the MAC ACLs from the interface.

```
mac access-group <access-list-number (1-50)> {in | out}
```

```
no mac access-group [<access-list-number (1-50)>] {in | out}
```

|                           |                                                |
|---------------------------|------------------------------------------------|
| <b>Syntax Description</b> | <b>access-list-number</b> - Access List Number |
|                           | <b>in</b> - Inbound packets                    |
|                           | <b>Out</b> - Outbound packets                  |

**Mode** Interface Configuration Mode

**Example** `iss(config-if)# mac access-group 5 in`



- MAC access list must have been created
- The MAC ACL must not have been applied to any Layer 2 interface in the same direction

- Related Command**
- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
  - **show access-lists** - Displays the access list statistics

## 65.3.14 permit

This command specifies the packets to be forwarded based on the MAC address and the associated parameters, i.e. this command allows non-IP traffic to be forwarded if the conditions are matched.

```
permit { any | host <mac-address> } { any | host <mac-address> } [ aarp | amber |
dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat |
lavr-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo |
vines-ip | xns-id | <protocol (0-65535)> ] [ encaps-type <value (1-4)> ] [ Vlan
<vlan-id (1-4094)> ]
```

|                    |                            |   |                                                                                                    |
|--------------------|----------------------------|---|----------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>any host</b>            | - | Source and Destination MAC address to be matched with the packet                                   |
| <b>Description</b> | <b>&lt;mac-address&gt;</b> |   |                                                                                                    |
|                    | <b>aarp</b>                | - | EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address |
|                    | <b>amber</b>               | - | EtherType DEC-Amber                                                                                |
|                    | <b>dec-spanning</b>        | - | EtherType Digital Equipment Corporation (DEC) spanning tree                                        |
|                    | <b>decnet-iv</b>           | - | EtherType DECnet Phase IV protocol                                                                 |
|                    | <b>diagnostic</b>          | - | EtherType DEC-Diagnostic                                                                           |
|                    | <b>dsm</b>                 | - | EtherType DEC-DSM                                                                                  |
|                    | <b>etype-6000</b>          | - | EtherType 0x6000                                                                                   |
|                    | <b>etype-8042</b>          | - | EtherType 0x8042                                                                                   |
|                    | <b>lat</b>                 | - | EtherType DEC-LAT                                                                                  |
|                    | <b>lavr-sca</b>            | - | EtherType DEC-LAVC-SCA                                                                             |
|                    | <b>mop-console</b>         | - | EtherType DEC-MOP Remote Console                                                                   |
|                    | <b>mop-dump</b>            | - | EtherType DEC-MOP Dump                                                                             |

|                   |   |                                                                               |
|-------------------|---|-------------------------------------------------------------------------------|
| <b>msdos</b>      | - | EtherType DEC-MSDOS                                                           |
| <b>mumps</b>      | - | EtherType DEC-MUMPS                                                           |
| <b>netbios</b>    | - | EtherType DEC- Network Basic Input/Output System (NETBIOS)                    |
| <b>vines-echo</b> | - | EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems |
| <b>vines-ip</b>   | - | EtherType VINES IP                                                            |
| <b>xns-id</b>     | - | EtherType Xerox Network Systems (XNS) protocol suite                          |
| <b>protocol</b>   | - | The non-IP protocol value to be filtered                                      |
| <b>encaptype</b>  | - | Encapsulation Type                                                            |
| <b>vlan</b>       | - | VLAN ID to be filtered                                                        |

**Mode** ACL MAC Configuration Mode

**Defaults**

|          |   |   |
|----------|---|---|
| protocol | - | 0 |
| vlan-id  | - | 0 |

**Example** `iss(config-ext-macl)# permit host 00:11:22:33:44:55 any aarp`



- MAC access list must have been created.
- If the protocol value is zero then this indicates that the filter is applicable for all the protocols.

**Related Command**

- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **deny** - Specifies the packets to be rejected based on the MAC address and the associated parameters

- **show access-lists** - Displays the access list statistics

## 65.3.15 deny

This command specifies the packets to be rejected based on the MAC address and the associated parameters.

```
deny { any | host <mac-address> } { any | host <mac-address> } [ aarp | amber |
dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat |
lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo |
vines-ip | xns-id | <protocol (0-65535)> ] [ encaps-type <value (1-4)> ] [ Vlan
<vlan-id (1-4094)> ]
```

|                    |                            |   |                                                                                                    |
|--------------------|----------------------------|---|----------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>any   host</b>          | - | Source MAC address to be matched with the packet                                                   |
| <b>Description</b> | <b>&lt;mac-address&gt;</b> |   |                                                                                                    |
|                    | <b>any   host</b>          | - | Destination MAC address to be matched with the packet                                              |
|                    | <b>&lt;mac-address&gt;</b> |   |                                                                                                    |
|                    | <b>aarp</b>                | - | EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address |
|                    | <b>amber</b>               | - | EtherType DEC-Amber                                                                                |
|                    | <b>dec-spanning</b>        | - | EtherType Digital Equipment Corporation (DEC) spanning tree                                        |
|                    | <b>decnet-iv</b>           | - | EtherType DECnet Phase IV protocol                                                                 |
|                    | <b>diagnostic</b>          | - | EtherType DEC-Diagnostic                                                                           |
|                    | <b>dsm</b>                 | - | EtherType DEC-DSM                                                                                  |
|                    | <b>etype-6000</b>          | - | EtherType 0x6000                                                                                   |
|                    | <b>etype-8042</b>          | - | EtherType 0x8042                                                                                   |
|                    | <b>lat</b>                 | - | EtherType DEC-LAT                                                                                  |
|                    | <b>lavc-sca</b>            | - | EtherType DEC-LAVC-SCA                                                                             |

|                    |                                                                                 |
|--------------------|---------------------------------------------------------------------------------|
| <b>mop-console</b> | - EtherType DEC-MOP Remote Console                                              |
| <b>mop-dump</b>    | - EtherType DEC-MOP Dump                                                        |
| <b>msdos</b>       | - EtherType DEC-MSDOS                                                           |
| <b>mumps</b>       | - EtherType DEC-MUMPS                                                           |
| <b>netbios</b>     | - EtherType DEC- Network Basic Input/Output System (NETBIOS)                    |
| <b>vines-echo</b>  | - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems |
| <b>vines-ip</b>    | - EtherType VINES IP                                                            |
| <b>xns-id</b>      | - EtherType Xerox Network Systems (XNS) protocol suite                          |
| <b>protocol</b>    | - The non-IP protocol value to be filtered                                      |
| <b>encaptype</b>   | - Encapsulation Type                                                            |
| <b>vlan</b>        | - VLAN ID to be filtered                                                        |

**Mode** ACL MAC Configuration Mode

**Defaults** protocol - 0

vlan-id - 0

**Example** `iss(config-ext-macl)# deny any host 00:11:22:33:44:55 any`



- MAC access list must have been created.
- If the protocol value is zero then this indicates that the filter is applicable for all the protocols.

**Related Command**

- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2

---

interface

- **permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **show access-lists** - Displays the access list statistics

## 65.3.16 show access-lists

This command displays the access lists configuration.

```
show access-lists [[{ip | mac}] <access-list-number (1-65535)> ]
```

|                           |            |                   |
|---------------------------|------------|-------------------|
| <b>Syntax Description</b> | <b>ip</b>  | - IP Access List  |
|                           | <b>mac</b> | - MAC Access List |

**Mode** Privileged/User EXEC Mode

**Example** iss# show access-lists

```
IP ACCESS LISTS
```

```
-----  
Standard IP Access List 1
```

```
-----  
Source IP address           : 0.0.0.0  
Source IP address mask     : 0.0.0.0  
Destination IP address     : 0.0.0.0  
Destination IP address mask : 0.0.0.0  
In Port List               : NIL  
Out Port List              : NIL  
Filter Action               : Permit  
Status                     : InActive
```

```
MAC ACCESS LISTS
```

```
-----  
Extended MAC Access List 1
```

```
-----  
Filter Priority             : 1  
Ether Type                 : 0  
Protocol Type              : 0  
Vlan Id                    : 0  
Destination MAC Address    : 00:00:00:00:00:00  
Source MAC Address         : 00:00:00:00:00:00  
In Port List               : NIL  
Filter Action               : Deny  
Status                     : InActive
```

```
iss# show access-lists ip 1
```

```
Standard IP Access List 1
```

```
Source IP address           : 0.0.0.0
Source IP address mask     : 0.0.0.0
Destination IP address     : 0.0.0.0
Destination IP address mask : 0.0.0.0
In Port List               : NIL
Out Port List              : NIL
Filter Action               : Permit
Status                     : InActive
```

```
iss# show access-lists mac 1
```

```
Extended MAC Access List 1
```

```
-----
Filter Priority             : 1
Ether Type                 : 0
Protocol Type              : 0
Vlan Id                    : 0
Destination MAC Address    : 00:00:00:00:00:00
Source MAC Address         : 00:00:00:00:00:00
In Port List               : NIL
Filter Action               : Deny
Status                     : InActive
```

**Related Command**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters
- **deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched
- **permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- **deny - ip/ospf/pim/protocol type** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters
- **deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters
- **permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters
- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface

- **permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **deny** - specifies the packets to be rejected based on the MAC address and the associated parameters

## 65.4 Marvell 6095 Specific Commands

This section describes the CLI commands executable only in Marvell 6095 target for configuring ACL feature supported by ISS.

The list of CLI commands for the configuration of ACL is as follows:

- ip access-list
- mac access-list extended
- permit - standard mode
- deny - standard mode
- permit host
- deny host
- permit- ip/ospf/pim/protocol type
- deny - ip/ospf/pim/protocol type
- permit tcp
- deny tcp
- permit udp
- deny udp
- permit icmp
- deny icmp
- ip access-group
- mac access-group
- permit
- deny
- show access-lists

## 65.4.1 ip access-list

This command creates IP ACLs and enters the IP Access-list configuration mode. Standard access lists create filters based on IP address and network mask only (L3 filters only). Extended access lists enables specification of filters based on the type of protocol, range of TCP/UDP ports as well as the IP address and network mask (Layer 4 filters).

Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode.

The no form of the command deletes the IP access-list.

```
ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> }
```

```
no ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> }
```

|                           |                 |                               |
|---------------------------|-----------------|-------------------------------|
| <b>Syntax Description</b> | <b>standard</b> | - Standard access-list number |
|                           | <b>extended</b> | - Extended access-list number |

**Mode** Global Configuration Mode

**Package** Metro

**Example** `iss(config)# ip access-list standard 1`



ACLs on the system perform both access control and Layer 3 field classification. To define Layer 3 fields' access-lists the `ip access-list` command must be used.

### Related Commands

- `permit - standard mode` - Specifies the packets to be forwarded depending upon the associated parameters
- `deny - standard mode` - Denies traffic if the conditions defined in the deny statement are matched
- `permit- ip/ospf/pim/protocol type` - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- `deny - ip/ospf/pim/protocol type` - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- `permit tcp` - Specifies the TCP packets to be forwarded based on the associated parameters
- `deny tcp` - Specifies the TCP packets to be rejected based on the associated parameters
- `permit udp` - Specifies the UDP packets to be forwarded based on the associated

---

parameters

- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- **ip access-group** - Enables access control for the packets on the interface
- **show access-lists** - Displays the access list configuration

## 65.4.2 mac access-list extended

This command creates Layer 2 MAC ACLs, that is, this command creates a MAC access-list and returns the MAC-Access list configuration mode to the user. The no form of the command deletes the MAC access-list.

```
mac access-list extended <access-list-number (1-65535)>
```

```
no mac access-list extended <short (1-65535)>
```

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss(config)# mac access-list extended 5



ACLs on the system perform both access control and layer 2 field classification. To define Layer 2 access lists, the mac access-list command must be used.

### Related Commands

- **show access-lists** - Displays the access list configuration
- **permit host dest-mac** - specifies packets to be forwarded Based on MAC address and associated parameters
- **deny host dest-mac** - .Specified the packets to be rejected based on MAC address and associated parameters.

### 65.4.3 permit - standard mode

This command specifies the packets to be forwarded depending upon the associated parameters. Standard IP access lists use source addresses for matching operations.

```
permit { any | host <src-ip-address> | <network-src-ip> <mask> } [ { any | host <dest-ip-address> | <network-dest-ip> <mask> } ]
```

|                           |                                                                                                           |                                                                                                                                                                                                                                                                  |
|---------------------------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>any host</b><br><b>&lt;src-ip-address&gt; </b><br><b>&lt;network-src-ip&gt;</b><br><b>&lt;mask&gt;</b> | <ul style="list-style-type: none"> <li>- Source IP address can be</li> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- the host that the packet is from and the network mask to use with the source IP address</li> </ul> |
|---------------------------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                              |                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>any host &lt;dest-ip-</b><br><b>address&gt; </b><br><b>&lt;network-dest-ip&gt;</b><br><b>&lt;mask&gt;</b> | <ul style="list-style-type: none"> <li>- Destination IP address can be</li> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- the host that the packet is destined for and the network mask to use with the destination IP address</li> </ul> |
|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Mode** ACL Standard Access List Configuration Mode

**Package** Metro

**Example** `iss(config-std-nacl)# permit host 100.0.0.10 host 10.0.0.1`

- Related Commands**
- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
  - **deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched
  - **show access-lists** - Displays the access list configuration

## 65.4.4 deny - standard mode

This command denies traffic if the conditions defined in the deny statement are matched.

```
deny{ any | host <src-ip-address> | <network-src-ip> <mask> } [ { any | host
<dest-ip-address> | <network-dest-ip> <mask> } ]
```

|                    |                                     |                                                                                                                    |
|--------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <code>any   host &lt;src-</code>    | - Source IP address can be                                                                                         |
| <b>Description</b> | <code>ip-address&gt;  </code>       | - 'any' or                                                                                                         |
|                    | <code>&lt;network-src-ip&gt;</code> | - the word 'host' and the dotted decimal address                                                                   |
|                    | <code>&lt;mask&gt;</code>           | or                                                                                                                 |
|                    |                                     | - number of the network or the host that the packet is from and the network mask to use with the source IP address |

|  |                                      |                                                                                                                                 |
|--|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
|  | <code>any   host &lt;dest-</code>    | - Destination IP address can be                                                                                                 |
|  | <code>ip-address&gt;  </code>        | - 'any' or                                                                                                                      |
|  | <code>&lt;network-dest-ip&gt;</code> | - the word 'host' and the dotted decimal address                                                                                |
|  | <code>&lt;mask&gt;</code>            | or                                                                                                                              |
|  |                                      | - number of the network or the host that the packet is destined for and the network mask to use with the destination IP address |

**Mode** ACL Standard Access List Configuration Mode

**Package** Metro

**Example** `iss(config-std-nacl)# deny host 100.0.0.10 any`

**Related Commands**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit - standard mode` - Specifies the packets to be forwarded depending upon the associated parameters
- `show access-lists` - Displays the access list configuration

## 65.4.5 permit host

This command specifies packets to forward, based on MAC address and associated parameters.

```
permit host {dest-mac <aa:aa:aa:aa:aa:aa> | src-mac <aa:aa:aa:aa:aa:aa>} vlan
<integer (1-4094)>
```

|                           |                                                                                                                                                                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <pre>&lt;aa:aa:aa:aa:aa:a a&gt;</pre> <p>- Forwards the packets containing the specified source / destination MAC address.</p>                                                                                                             |
|                           | <pre>vlan&lt;integer (1- 4094)&gt;</pre> <p>- Configures the MAC address for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created.<br/>This value ranges between 1 and 4094.</p>        |
| <b>Mode</b>               | ACL Extended Access List Configuration Mode                                                                                                                                                                                                |
| <b>Package</b>            | Workgroup                                                                                                                                                                                                                                  |
| <b>Example</b>            | <pre>iss(config-ext-macl)# permit host dest-mac 00:22:33:44:55:66 vlan 1</pre>                                                                                                                                                             |
| <b>Related Commands</b>   | <ul style="list-style-type: none"> <li>• <b>deny host</b> - .Specifies the packets to be rejected based on MAC address and associated parameters.</li> <li>• <b>show access-lists</b> - Displays the access list configuration.</li> </ul> |

## 65.4.6 deny host

This command specifies the packets to be rejected based on MAC Address and associated parameters.

```
deny host {dest-mac <aa:aa:aa:aa:aa:aa> | src-mac <aa:aa:aa:aa:aa:aa>} vlan
<integer (1-4094)>
```

**Syntax Description** <aa:aa:aa:aa:aa:aa> - Rejects the packets containing the specified source / destination MAC address.

vlan<integer (1-4094)> - Configures the MAC address for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created.  
This value ranges between 1 and 4094.

**Mode** ACL Extended Access List Configuration Mode.

**Package** Workgroup

**Example** `iss(config-ext-nacl)# deny host dest-mac 00:22:33:44:55:66`

**Related Commands**

- `permit host` - Specifies the packets to be forwarded, based on MAC address and associated parameters.
- `show access-lists`-Displays the access list configuration.

## 65.4.7 permit- ip/ospf/pim/protocol type

This command allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.

```
permit { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-
address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-
ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay |
normal |<value (0-7)>} | dscp <value (0-63)>} ] [ priority <value (1-255)>] [
svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-
id (1-4094)>] [ cvlan-priority <value (0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <pre>ip  ospf pim  &lt;protocol-type (1- 255)&gt; any  host &lt;src-ip-address&gt;  &lt;src-ip-address&gt; &lt;mask&gt;</pre> | <ul style="list-style-type: none"> <li>- Type of protocol for the packet. It can also be a protocol number.</li> <li>- Source IP address can be             <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is from and the network mask to use with the source address.</li> </ul> </li> </ul> |
|                           | <pre>any host &lt;dest-ip-address&gt;  &lt;dest-ip-address&gt; &lt;mask&gt;</pre>                                             | <ul style="list-style-type: none"> <li>- Destination IP address can be             <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> </li> </ul>                                                              |
| <b>tos</b>                |                                                                                                                               | <ul style="list-style-type: none"> <li>- Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.</li> </ul>                                                                                                                                                                        |
| <b>priority</b>           |                                                                                                                               | <ul style="list-style-type: none"> <li>- The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.</li> </ul>                                                                                                                                                                   |
| <b>svlan-id</b>           |                                                                                                                               | <ul style="list-style-type: none"> <li>- Service VLAN value to match against incoming packets.</li> </ul>                                                                                                                                                                                                                                                                                                                   |
| <b>svlan-priority</b>     |                                                                                                                               | <ul style="list-style-type: none"> <li>- Service VLAN priority value to match against incoming packets.</li> </ul>                                                                                                                                                                                                                                                                                                          |

|                       |   |                                                                 |
|-----------------------|---|-----------------------------------------------------------------|
| <b>cvlan-id</b>       | - | Customer VLAN value to match against incoming packets.          |
| <b>cvlan-priority</b> | - | Customer VLAN priority value to match against incoming packets. |
| <b>single-tag</b>     | - | Filter to be applied on Single VLAN tagged packets.             |
| <b>double-tag</b>     | - | Filter to be applied on double VLAN tagged packets.             |

**Mode** ACL Extended Access List Configuration Mode

**Package** Metro

|                 |                                |   |            |
|-----------------|--------------------------------|---|------------|
| <b>Defaults</b> | <b>protocol-type</b>           | - | 255        |
|                 | <b>priority</b>                | - | 1          |
|                 | <b>svlan-id</b>                | - | 0          |
|                 | <b>svlan-priority</b>          | - | -1         |
|                 | <b>cvlan-id</b>                | - | 0          |
|                 | <b>cvlan-priority</b>          | - | -1         |
|                 | <b>single-tag   double-tag</b> | - | Single tag |

**Example** `iss(config-ext-nacl)# permit 200 host 100.0.0.10 any tos 6`



- Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.
- Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **deny - ip/ospf/pim/protocol type** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched



|                       |   |                                                                 |
|-----------------------|---|-----------------------------------------------------------------|
| <b>cvlan-id</b>       | - | Customer VLAN value to match against incoming packets.          |
| <b>cvlan-priority</b> | - | Customer VLAN priority value to match against incoming packets. |
| <b>single-tag</b>     | - | Filter to be applied on Single VLAN tagged packets.             |
| <b>double-tag</b>     | - | Filter to be applied on double VLAN tagged packets.             |

**Mode** ACL Extended Access List Configuration Mode

**Package** Metro

|                 |                         |   |            |
|-----------------|-------------------------|---|------------|
| <b>Defaults</b> | protocol type           | - | 255        |
|                 | priority                | - | 1          |
|                 | svlan-id                | - | 0          |
|                 | svlan-priority          | - | -1         |
|                 | cvlan-id                | - | 0          |
|                 | cvlan-priority          | - | -1         |
|                 | single-tag   double-tag | - | Single tag |

**Example** `iss(config-ext-nacl)# deny ospf any host 10.0.0.1 tos max-throughput`



- Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.
- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit- ip/ospf/pim/protocol type` - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- `show access-lists` - Displays the access list configuration

## 65.4.9 permit tcp

This command specifies the TCP packets to be forwarded based on the associated parameters.

```
permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp <value (0-
63)>}] [ priority <short (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-
priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value
(0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                                                                                                    |                                                                                                                                                                                                                                                         |
|---------------------------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>tcp</b>                                                                                                         | - Transport Control Protocol                                                                                                                                                                                                                            |
|                           | <b>any  host</b><br><b>&lt;src-ip-address&gt; </b><br><b>&lt;src-ip-address&gt; &lt;</b><br><b>src-mask &gt;</b>   | - Source IP address can be<br>- 'any' or<br>- the word 'host' and the dotted decimal address or<br>- number of the network or the host that the packet is from and the network mask to use with the source address                                      |
|                           | <b>port-number</b>                                                                                                 | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.<br>- eq=equal<br>- lt=less than<br>- gt=greater than<br>- range=a range of ports; two different port numbers must be specified |
|                           | <b>any host</b><br><b>&lt;dest-ip-address&gt;</b><br><b> &lt;dest-ip-address&gt;</b><br><b>&lt; dest-mask &gt;</b> | - Destination IP address can be<br>- 'any' or<br>- the word 'host' and the dotted decimal address or<br>- number of the network or the host that the packet is destined for and the network mask to use with the destination address                    |
|                           | <b>ack</b>                                                                                                         | - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3).                                                                                                                                                  |

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |     |     |                                                                                       |     |                                                                                       |          |     |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----|-----|---------------------------------------------------------------------------------------|-----|---------------------------------------------------------------------------------------|----------|-----|
| <b>rst</b>            | - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3).                                                                                                                                                                                                                                                                                                                                                                                          |           |     |     |                                                                                       |     |                                                                                       |          |     |
| <b>tos</b>            | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                                                                                                                                                                                                                                                 |           |     |     |                                                                                       |     |                                                                                       |          |     |
| <b>priority</b>       | - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.                                                                                                                                                                                                                                                                               |           |     |     |                                                                                       |     |                                                                                       |          |     |
| <b>svlan-id</b>       | - Service VLAN value to match against incoming packets.                                                                                                                                                                                                                                                                                                                                                                                                                            |           |     |     |                                                                                       |     |                                                                                       |          |     |
| <b>svlan-priority</b> | - Service VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                                                                                                                                                                                                   |           |     |     |                                                                                       |     |                                                                                       |          |     |
| <b>cvlan-id</b>       | - Customer VLAN value to match against incoming packets.                                                                                                                                                                                                                                                                                                                                                                                                                           |           |     |     |                                                                                       |     |                                                                                       |          |     |
| <b>cvlan-priority</b> | - Customer VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                                                                                                                                                                                                  |           |     |     |                                                                                       |     |                                                                                       |          |     |
| <b>single-tag</b>     | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                                                                                                                                                                                                                                                                                                              |           |     |     |                                                                                       |     |                                                                                       |          |     |
| <b>double-tag</b>     | - Filter to be applied on double VLAN tagged packets.                                                                                                                                                                                                                                                                                                                                                                                                                              |           |     |     |                                                                                       |     |                                                                                       |          |     |
| <b>Mode</b>           | ACL Extended Access List Configuration Mode                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |     |     |                                                                                       |     |                                                                                       |          |     |
| <b>Package</b>        | Metro                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |           |     |     |                                                                                       |     |                                                                                       |          |     |
| <b>Defaults</b>       | <table border="0"> <tr> <td style="vertical-align: top;">tos-value</td> <td>- 0</td> </tr> <tr> <td style="vertical-align: top;">ack</td> <td>- 'any' (3) [indicates that the TCP ACK bit will not be checked to decide the action]</td> </tr> <tr> <td style="vertical-align: top;">rst</td> <td>- 'any' (3) [indicates that the TCP RST bit will not be checked to decide the action]</td> </tr> <tr> <td style="vertical-align: top;">svlan-id</td> <td>- 0</td> </tr> </table> | tos-value | - 0 | ack | - 'any' (3) [indicates that the TCP ACK bit will not be checked to decide the action] | rst | - 'any' (3) [indicates that the TCP RST bit will not be checked to decide the action] | svlan-id | - 0 |
| tos-value             | - 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |     |     |                                                                                       |     |                                                                                       |          |     |
| ack                   | - 'any' (3) [indicates that the TCP ACK bit will not be checked to decide the action]                                                                                                                                                                                                                                                                                                                                                                                              |           |     |     |                                                                                       |     |                                                                                       |          |     |
| rst                   | - 'any' (3) [indicates that the TCP RST bit will not be checked to decide the action]                                                                                                                                                                                                                                                                                                                                                                                              |           |     |     |                                                                                       |     |                                                                                       |          |     |
| svlan-id              | - 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |     |     |                                                                                       |     |                                                                                       |          |     |

|                         |   |            |
|-------------------------|---|------------|
| svlan-priority          | - | -1         |
| cvlan-id                | - | 0          |
| cvlan-priority          | - | -1         |
| single-tag   double-tag | - | Single tag |

**Example** `iss(config-ext-nacl)# permit tcp any 10.0.0.1 255.255.255.255`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters

## 65.4.10 deny tcp

This command specifies the TCP packets to be rejected based on the associated parameters.

```
deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}] | dscp <value
(0-63)>}] [ priority <short (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-
priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value
(0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                 |                                                                                                                                                                                                                                                                                                                          |
|---------------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>tcp</b>                      | - Transmission control protocol                                                                                                                                                                                                                                                                                          |
|                           | <b>any  host</b>                | - Source IP address can be                                                                                                                                                                                                                                                                                               |
|                           | <b>&lt;src-ip-address&gt; </b>  | - 'any' or                                                                                                                                                                                                                                                                                                               |
|                           | <b>&lt;src-ip-address&gt;</b>   | - the word 'host' and the dotted decimal address or                                                                                                                                                                                                                                                                      |
|                           | <b>&lt;src-mask&gt;</b>         | - number of the network or the host that the packet is from and the network mask to use with the source address                                                                                                                                                                                                          |
|                           | <b>port-number</b>              | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators. <ul style="list-style-type: none"> <li>- eq=equal</li> <li>- lt=less than</li> <li>- gt=greater than</li> <li>- range=a range of ports; two different port numbers must be specified</li> </ul> |
|                           | <b>any host</b>                 | - Destination IP address can be                                                                                                                                                                                                                                                                                          |
|                           | <b>&lt;dest-ip-address&gt; </b> | - 'any' or                                                                                                                                                                                                                                                                                                               |
|                           | <b>&lt;dest-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address or                                                                                                                                                                                                                                                                      |
|                           | <b>&lt;dest-mask&gt;</b>        | - number of the network or the host that the packet is destined for and the network mask to use with the destination address                                                                                                                                                                                             |

---

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |           |     |     |                                                                                   |     |                                                                                   |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----|-----|-----------------------------------------------------------------------------------|-----|-----------------------------------------------------------------------------------|
| <b>ack</b>            | - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3)                                                                                                                                                                                                                                                                                                                                                                                      |           |     |     |                                                                                   |     |                                                                                   |
| <b>rst</b>            | - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3)                                                                                                                                                                                                                                                                                                                                                                                                   |           |     |     |                                                                                   |     |                                                                                   |
| <b>tos</b>            | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                                                                                                                                                                                                                                                         |           |     |     |                                                                                   |     |                                                                                   |
| <b>priority</b>       | - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.                                                                                                                                                                                                                                                                                       |           |     |     |                                                                                   |     |                                                                                   |
| <b>svlan-id</b>       | - Service VLAN value to match against incoming packets.                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |     |     |                                                                                   |     |                                                                                   |
| <b>svlan-priority</b> | - Service VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                                                                                                                                                                                                           |           |     |     |                                                                                   |     |                                                                                   |
| <b>cvlan-id</b>       | - Customer VLAN value to match against incoming packets.                                                                                                                                                                                                                                                                                                                                                                                                                                   |           |     |     |                                                                                   |     |                                                                                   |
| <b>cvlan-priority</b> | - Customer VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                                                                                                                                                                                                          |           |     |     |                                                                                   |     |                                                                                   |
| <b>single-tag</b>     | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                                                                                                                                                                                                                                                                                                                      |           |     |     |                                                                                   |     |                                                                                   |
| <b>double-tag</b>     | - Filter to be applied on double VLAN tagged packets.                                                                                                                                                                                                                                                                                                                                                                                                                                      |           |     |     |                                                                                   |     |                                                                                   |
| <b>Mode</b>           | ACL Extended Access List Configuration Mode                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |     |     |                                                                                   |     |                                                                                   |
| <b>Package</b>        | Metro                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |           |     |     |                                                                                   |     |                                                                                   |
| <b>Defaults</b>       | <table border="0"> <tr> <td style="vertical-align: top;">tos-value</td> <td style="vertical-align: top;">- 0</td> </tr> <tr> <td style="vertical-align: top;">ack</td> <td style="vertical-align: top;">- 'any' (3) [indicates that TCP ACK bit will not be checked to decide the action]</td> </tr> <tr> <td style="vertical-align: top;">rst</td> <td style="vertical-align: top;">- 'any' (3) [indicates that TCP RST bit will not be checked to decide the action]</td> </tr> </table> | tos-value | - 0 | ack | - 'any' (3) [indicates that TCP ACK bit will not be checked to decide the action] | rst | - 'any' (3) [indicates that TCP RST bit will not be checked to decide the action] |
| tos-value             | - 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |     |     |                                                                                   |     |                                                                                   |
| ack                   | - 'any' (3) [indicates that TCP ACK bit will not be checked to decide the action]                                                                                                                                                                                                                                                                                                                                                                                                          |           |     |     |                                                                                   |     |                                                                                   |
| rst                   | - 'any' (3) [indicates that TCP RST bit will not be checked to decide the action]                                                                                                                                                                                                                                                                                                                                                                                                          |           |     |     |                                                                                   |     |                                                                                   |

|                         |   |            |
|-------------------------|---|------------|
| svlan-id                | - | 0          |
| svlan-priority          | - | -1         |
| cvlan-id                | - | 0          |
| cvlan-priority          | - | -1         |
| single-tag   double-tag | - | Single tag |

**Example** `iss(config-ext-nacl)# deny tcp 100.0.0.10 255.255.255.0 eq 20 any`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

**Related Commands**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access list configuration
- `permit tcp` - Specifies the TCP packets to be forwarded based on the associated parameters

## 65.4.11 permit udp

This command specifies the UDP packets to be forwarded based on the associated parameters.

```
permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{ gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{tos{max-reliability|max-
throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [
priority <short (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-priority
<value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value (0-7)>]
[ { single-tag | double-tag } ]
```

|                           |                                 |                                                                                                                                                                                                                                                         |
|---------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>udp</b>                      | - User Datagram Protocol                                                                                                                                                                                                                                |
|                           | <b>any  host</b>                | - Source IP address can be                                                                                                                                                                                                                              |
|                           | <b>&lt;src-ip-address&gt; </b>  | - 'any' or                                                                                                                                                                                                                                              |
|                           | <b>&lt;src-ip-address&gt;</b>   | - the word 'host' and the dotted decimal address                                                                                                                                                                                                        |
|                           | <b>&lt;src-mask&gt;</b>         | or<br>- number of the network or the host that the packet is from and the network mask to use with the source address                                                                                                                                   |
|                           | <b>port-number</b>              | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.<br>- eq=equal<br>- lt=less than<br>- gt=greater than<br>- range=a range of ports; two different port numbers must be specified |
|                           | <b>any host</b>                 | - Destination IP address can be                                                                                                                                                                                                                         |
|                           | <b>&lt;dest-ip-address&gt; </b> | - 'any' or                                                                                                                                                                                                                                              |
|                           | <b>&lt;dest-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address                                                                                                                                                                                                        |
|                           | <b>&lt;dest-mask&gt;</b>        | or<br>- number of the network or the host that the packet is destined for and the network mask to use with the destination address                                                                                                                      |

|                       |                                                                                                                        |                                                                                                                                                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>tos</b>            | <pre> {max-reliability   max-throughput   min-delay   normal   &lt;value (0-7)&gt;   dscp &lt;value (0-63)&gt;} </pre> | <ul style="list-style-type: none"> <li>- Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.</li> </ul>   |
| <b>priority</b>       |                                                                                                                        | <ul style="list-style-type: none"> <li>- The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.</li> </ul> |
| <b>svlan-id</b>       |                                                                                                                        | <ul style="list-style-type: none"> <li>- Service VLAN value to match against incoming packets.</li> </ul>                                                                                                                                              |
| <b>svlan-priority</b> |                                                                                                                        | <ul style="list-style-type: none"> <li>- Service VLAN priority value to match against incoming packets.</li> </ul>                                                                                                                                     |
| <b>cvlan-id</b>       |                                                                                                                        | <ul style="list-style-type: none"> <li>- Customer VLAN value to match against incoming packets.</li> </ul>                                                                                                                                             |
| <b>cvlan-priority</b> |                                                                                                                        | <ul style="list-style-type: none"> <li>- Customer VLAN priority value to match against incoming packets.</li> </ul>                                                                                                                                    |
| <b>single-tag</b>     |                                                                                                                        | <ul style="list-style-type: none"> <li>- Filter to be applied on Single VLAN tagged packets.</li> </ul>                                                                                                                                                |
| <b>double-tag</b>     |                                                                                                                        | <ul style="list-style-type: none"> <li>- Filter to be applied on double VLAN tagged packets.</li> </ul>                                                                                                                                                |
| <b>Mode</b>           | ACL Extended Access List Configuration Mode                                                                            |                                                                                                                                                                                                                                                        |
| <b>Package</b>        | Metro                                                                                                                  |                                                                                                                                                                                                                                                        |
| <b>Defaults</b>       | <b>svlan-id</b>                                                                                                        | - 0                                                                                                                                                                                                                                                    |
|                       | <b>svlan-priority</b>                                                                                                  | - -1                                                                                                                                                                                                                                                   |
|                       | <b>cvlan-id</b>                                                                                                        | - 0                                                                                                                                                                                                                                                    |
|                       | <b>cvlan-priority</b>                                                                                                  | - -1                                                                                                                                                                                                                                                   |
|                       | <b>single-tag   double-tag</b>                                                                                         | - Single tag                                                                                                                                                                                                                                           |

**Example**      `iss(config-ext-nacl)# permit udp any gt 65000 any dscp 1`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related  
Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters

## 65.4.12 deny udp

This command specifies the UDP packets to be rejected based on the associated parameters.

```
deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{ gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{tos{max-reliability|max-
throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [
priority <short (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-priority
<value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value (0-7)>]
[ { single-tag | double-tag } ]
```

|                                 |                                |                                                                                                                                                                                                                                                         |
|---------------------------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b>       | <b>udp</b>                     | - User Datagram Protocol                                                                                                                                                                                                                                |
| <b>any  host</b>                | <b>&lt;src-ip-address&gt; </b> | - Source IP address can be                                                                                                                                                                                                                              |
| <b>&lt;src-ip-address&gt;</b>   | <b>&lt;src-ip-address&gt;</b>  | - 'any' or                                                                                                                                                                                                                                              |
| <b>&lt;src-mask&gt;</b>         | <b>&lt;src-mask&gt;</b>        | - the word 'host' and the dotted decimal address or<br>- number of the network or the host that the packet is from and the network mask to use with the source address                                                                                  |
| <b>port-number</b>              | <b>port-number</b>             | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.<br>- eq=equal<br>- lt=less than<br>- gt=greater than<br>- range=a range of ports; two different port numbers must be specified |
| <b>any host</b>                 | <b>&lt;dest-ip-address&gt;</b> | - Destination IP address can be                                                                                                                                                                                                                         |
| <b> &lt;dest-ip-address&gt;</b> | <b>&lt;dest-ip-address&gt;</b> | - 'any' or                                                                                                                                                                                                                                              |
| <b>&lt;dest-mask&gt;</b>        | <b>&lt;dest-mask&gt;</b>       | - the word 'host' and the dotted decimal address or<br>- number of the network or the host that the packet is destined for and the network mask to use with the destination address                                                                     |
| <b>tos</b>                      | <b>tos</b>                     | - Type of service. Can be max-reliability, max throughput,                                                                                                                                                                                              |

---

|                                                                                     |                                                                                       |                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                     |                                                                                       | min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                           |
|                                                                                     | <b>priority</b>                                                                       | - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. |
|                                                                                     | <b>svlan-id</b>                                                                       | - Service VLAN value to match against incoming packets.                                                                                                                                           |
|                                                                                     | <b>svlan-priority</b>                                                                 | - Service VLAN priority value to match against incoming packets.                                                                                                                                  |
|                                                                                     | <b>cvlan-id</b>                                                                       | - Customer VLAN value to match against incoming packets.                                                                                                                                          |
|                                                                                     | <b>cvlan-priority</b>                                                                 | - Customer VLAN priority value to match against incoming packets.                                                                                                                                 |
|                                                                                     | <b>single-tag</b>                                                                     | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                             |
|                                                                                     | <b>double-tag</b>                                                                     | - Filter to be applied on double VLAN tagged packets.                                                                                                                                             |
| <b>Mode</b>                                                                         | ACL Extended Access List Configuration Mode                                           |                                                                                                                                                                                                   |
| <b>Defaults</b>                                                                     | <b>svlan-id</b>                                                                       | - 0                                                                                                                                                                                               |
|                                                                                     | <b>svlan-priority</b>                                                                 | - -1                                                                                                                                                                                              |
|                                                                                     | <b>cvlan-id</b>                                                                       | - 0                                                                                                                                                                                               |
|                                                                                     | <b>cvlan-priority</b>                                                                 | - -1                                                                                                                                                                                              |
|                                                                                     | <b>single-tag   double-tag</b>                                                        | - Single tag                                                                                                                                                                                      |
| <b>Package</b>                                                                      | Metro                                                                                 |                                                                                                                                                                                                   |
| <b>Example</b>                                                                      | <code>iss(config-ext-nacl)# deny udp host 10.0.0.1 any eq 20</code>                   |                                                                                                                                                                                                   |
|  | Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options |                                                                                                                                                                                                   |

are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related  
Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters

## 65.4.13 permit icmp

This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.

```
permit icmp {any | host <src-ip-address> | <src-ip-address> <mask>} {any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
[<message-code (0-255)>] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-
4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-
priority <value (0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                 |                                                                                                                                                                                                   |
|---------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>icmp</b>                     | - Internet Control Message Protocol                                                                                                                                                               |
|                           | <b>any  host</b>                | - Source IP address can be                                                                                                                                                                        |
|                           | <b>&lt;src-ip-address&gt;</b>   | - 'any' or                                                                                                                                                                                        |
|                           | <b> &lt;src-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address                                                                                                                                                  |
|                           | <b>&lt;mask&gt;</b>             | or<br>- number of the network or the host that the packet is from and the network mask to use with the source address                                                                             |
|                           | <b>any host</b>                 | - Destination IP address can be                                                                                                                                                                   |
|                           | <b>&lt;dest-ip-address&gt; </b> | - 'any' or                                                                                                                                                                                        |
|                           | <b>&lt;dest-ip-address&gt;</b>  | - the word 'host' and the dotted decimal address                                                                                                                                                  |
|                           | <b>&lt;mask&gt;</b>             | or<br>- number of the network or the host that the packet is destined for and the network mask to use with the destination address                                                                |
|                           | <b>message-type</b>             | - Message type                                                                                                                                                                                    |
|                           | <b>message-code</b>             | - ICMP Message code                                                                                                                                                                               |
|                           | <b>priority</b>                 | - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. |
|                           | <b>svlan-id</b>                 | - Service VLAN value to match against incoming packets.                                                                                                                                           |

- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL Extended Access List Configuration Mode

**Package** Metro

**Defaults**

|                           |   |            |
|---------------------------|---|------------|
| message-type/message code | - | 255        |
| svlan-id                  | - | 0          |
| svlan-priority            | - | -1         |
| cvlan-id                  | - | 0          |
| cvlan-priority            | - | -1         |
| single-tag   double-tag   | - | Single tag |

**Example** `iss(config-ext-nacl)# permit icmp any any`



- The ICMP message type can be one of the following:

| Value | ICMP type               |
|-------|-------------------------|
| 0     | Echo reply              |
| 3     | Destination unreachable |
| 4     | Source quench           |
| 5     | Redirect                |
| 8     | Echo request            |
| 11    | Time exceeded           |

|     |                      |
|-----|----------------------|
| 12  | Parameter problem    |
| 13  | Timestamp request    |
| 14  | Timestamp reply      |
| 15  | Information request  |
| 16  | Information reply    |
| 17  | Address mask request |
| 18  | Address mask reply   |
| 155 | No ICMP type         |

- The ICMP code can be any of the following:

| - Value | ICMP code                                       |
|---------|-------------------------------------------------|
| - 0     | Network unreachable                             |
| - 1     | Host unreachable                                |
| - 2     | Protocol unreachable                            |
| - 3     | Port unreachable                                |
| - 4     | Fragment need                                   |
| - 5     | Source route fail                               |
| - 6     | Destination network unknown                     |
| - 7     | Destination host unknown                        |
| - 8     | Source host isolated                            |
| - 9     | Destination network administratively prohibited |
| - 10    | Destination host administratively prohibited    |
| - 11    | Network unreachable TOS                         |
| - 12    | Host unreachable TOS                            |
| - 255   | No ICMP code                                    |

- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **ip access-list** - Created IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters

## 65.4.14 deny icmp

This command specifies the ICMP packets to be rejected based on the IP address and associated parameters.

```
deny icmp {any | host <src-ip-address> | <src-ip-address> <mask>} {any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
[<message-code (0-255)>] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-
4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-
priority <value (0-7)>] [ { single-tag | double-tag } ]
```

|                    |                                                                                                                                 |                                                                                                                                                                                                                                                                                                        |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>icmp</b>                                                                                                                     | - Internet Control Message Protocol                                                                                                                                                                                                                                                                    |
| <b>Description</b> | <p><b>any  host</b></p> <p><b>&lt;src-ip-address&gt;  </b></p> <p><b>&lt;src-ip-address&gt;</b></p> <p><b>&lt;mask&gt;</b></p>  | <p>- Source IP address can be</p> <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul>                   |
|                    | <p><b>any host</b></p> <p><b>&lt;dest-ip-address&gt;  </b></p> <p><b>&lt;dest-ip-address&gt;</b></p> <p><b>&lt;mask&gt;</b></p> | <p>- Destination IP address can be</p> <ul style="list-style-type: none"> <li>- 'any' or</li> <li>- the word 'host' and the dotted decimal address or</li> <li>- number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> |
|                    | <b>message-type</b>                                                                                                             | - Message type                                                                                                                                                                                                                                                                                         |
|                    | <b>message-code</b>                                                                                                             | - ICMP Message code                                                                                                                                                                                                                                                                                    |
|                    | <b>priority</b>                                                                                                                 | - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.                                                                                                      |
|                    | <b>svlan-id</b>                                                                                                                 | - Service VLAN value to match against incoming packets.                                                                                                                                                                                                                                                |
|                    | <b>svlan-priority</b>                                                                                                           | - Service VLAN priority value to match against incoming                                                                                                                                                                                                                                                |

packets.

- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL Extended Access List Configuration Mode

**Package** Metro

- Defaults**
- message-type/  
message code - 255
  - svlan-id - 0
  - svlan-priority - -1
  - cvlan-id - 0
  - cvlan-priority - -1
  - single-tag | double-tag - Single tag

**Example** `iss(config-ext-nacl)# deny icmp host 100.0.0.10 10.0.0.1  
255.255.255.255`



- The ICMP message type can be one of the following:

| Value | ICMP type               |
|-------|-------------------------|
| 0     | Echo reply              |
| 3     | Destination unreachable |
| 4     | Source quench           |
| 5     | Redirect                |
| 8     | Echo request            |
| 11    | Time exceeded           |

|     |                      |
|-----|----------------------|
| 12  | Parameter problem    |
| 13  | Timestamp request    |
| 14  | Timestamp reply      |
| 15  | Information request  |
| 16  | Information reply    |
| 17  | Address mask request |
| 18  | Address mask reply   |
| 155 | No ICMP type         |

- The ICMP code can be any of the following:

| Value | ICMP code                                       |
|-------|-------------------------------------------------|
| 0     | Network unreachable                             |
| 1     | Host unreachable                                |
| 2     | Protocol unreachable                            |
| 3     | Port unreachable                                |
| 4     | Fragment need                                   |
| 5     | Source route fail                               |
| 6     | Destination network unknown                     |
| 7     | Destination host unknown                        |
| 8     | Source host isolated                            |
| 9     | Destination network administratively prohibited |
| 10    | Destination host administratively prohibited    |
| 11    | Network unreachable TOS                         |
| 12    | Host unreachable TOS                            |
| 255   | No ICMP code                                    |

- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

#### Related Commands

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters

## 65.4.15 ip access-group

This command enables access control for the packets on the interface. It controls access to a Layer 2 or Layer 3 interface. The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out.

```
ip access-group <access-list-number (1-65535)> {in | out}
```

```
no ip access-group [<access-list-number (1-65535)>] {in | out}
```

**Syntax Description**      **access-list-number** - IP access control list number

**in** - Inbound packets

**out** - Outbound packets

**Mode**                    Interface Configuration Mode

**Package**                Metro

**Example**                iss(config-if)# ip access-group 1 in



- IP access list must have been created.
- Following are the limitations for this command to be applicable to Layer 2 interfaces.
  - The out keyword is not supported by Layer 2 interfaces.
  - An IP ACL applied to a Layer 2 interface filters only the IP packets. MAC access-group interface configuration command with MAC extended ACLs must be used to filter non-IP packets.

- Related Commands**
- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
  - **show access-lists** - Displays the access list configuration

## 65.4.16 mac access-group

This command applies a MAC access control list (ACL) to a Layer 2 interface. The no form of this command can be used to remove the MAC ACLs from the interface.

```
mac access-group <access-list-number (1-65535)> {in | out}
```

```
no mac access-group [<access-list-number (1-65535)>] {in | out}
```

**Syntax Description**      **access-list-number** - Access List Number

**in** - Inbound packets

**out** - Outbound packets

**Mode**      Interface Configuration Mode

**Package**      Metro

**Example**      `iss(config-if)# mac access-group 5 in`



MAC access list must have been created.

**Related Commands**

- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **show access-lists** - Displays the access list statistics

## 65.4.17 permit

This command specifies the packets to be forwarded based on the MAC address and the associated parameters, that is, this command allows non-IP traffic to be forwarded if the conditions are matched.

```
permit { any | host <src-mac-address> } { any | host <dest-mac-address> } [ {
aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |
etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios
| vines-echo | vines-ip | xns-id | <short (0-65535)> } ] [ encaps-type <integer
(1-65535)> ] [ vlan <vlan-id (1-4094)>] [ priority <short (1-255)>] [
outerEtherType < integer (1-65535)> ] [ svlan-id <vlan-id (1-4094)>] [ cvlan-
priority <value (0-7)>] [svlan-priority <value (0-7)>] [ { single-tag |
double-tag } ]
```

|                           |                                             |                                                                                                      |
|---------------------------|---------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>any   host &lt;src-mac-address &gt;</b>  | - Source MAC address to be matched with the packet                                                   |
|                           | <b>any   host &lt;dest-mac-address &gt;</b> | - Destination MAC address to be matched with the packet                                              |
|                           | <b>aarp</b>                                 | - EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address |
|                           | <b>amber</b>                                | - EtherType DEC-Amber                                                                                |
|                           | <b>dec-spanning</b>                         | - EtherType Digital Equipment Corporation (DEC) spanning tree                                        |
|                           | <b>decnet-iv</b>                            | - EtherType DECnet Phase IV protocol                                                                 |
|                           | <b>diagnostic</b>                           | - EtherType DEC-Diagnostic                                                                           |
|                           | <b>dsm</b>                                  | - EtherType DEC-DSM/DDP                                                                              |
|                           | <b>etype-6000</b>                           | - EtherType 0x6000                                                                                   |
|                           | <b>etype-8042</b>                           | - EtherType 0x8042                                                                                   |
|                           | <b>lat</b>                                  | - EtherType DEC-LAT                                                                                  |
|                           | <b>lavc-sca</b>                             | - EtherType DEC-LAVC-SCA                                                                             |

---

|                       |                                                                                                                                                                                                        |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mop-console</b>    | - EtherType DEC-MOP Remote Console                                                                                                                                                                     |
| <b>mop-dump</b>       | - EtherType DEC-MOP Dump                                                                                                                                                                               |
| <b>msdos</b>          | - EtherType DEC-MSDOS                                                                                                                                                                                  |
| <b>mumps</b>          | - EtherType DEC-MUMPS                                                                                                                                                                                  |
| <b>netbios</b>        | - EtherType DEC- Network Basic Input/Output System (NETBIOS)                                                                                                                                           |
| <b>vines-echo</b>     | - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems                                                                                                                        |
| <b>vines-ip</b>       | - EtherType VINES IP                                                                                                                                                                                   |
| <b>xns-id</b>         | - EtherType Xerox Network Systems (XNS) protocol suite                                                                                                                                                 |
| <b>encaptype</b>      | - Encapsulation Type                                                                                                                                                                                   |
| <b>vlan</b>           | - VLAN ID to be filtered                                                                                                                                                                               |
| <b>priority</b>       | - The priority of the L2 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority |
| <b>outerEtherType</b> | - EtherType value to match on Service vlan tag                                                                                                                                                         |
| <b>svlan-id</b>       | - Service VLAN value to match against incoming packets.                                                                                                                                                |
| <b>cvlan-priority</b> | - Customer VLAN priority value to match against incoming packets.                                                                                                                                      |
| <b>svlan-priority</b> | - Service VLAN priority value to match against incoming packets.                                                                                                                                       |
| <b>single-tag</b>     | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                                  |

**double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL MAC Configuration Mode

**Package** Metro

**Defaults**

|                         |   |            |
|-------------------------|---|------------|
| vlan-id                 | - | 0          |
| priority                | - | 1          |
| outerEtherType          | - | 0          |
| svlan-id                | - | 0          |
| cvlan-priority          | - | -1         |
| svlan-priority          | - | -1         |
| single-tag   double-tag | - | Single tag |

**Example** `iss(config-ext-macl)# permit host 00:11:22:33:44:55 any aarp priority 10`



- MAC access list must have been created.
- OuterEtherType, Service Vlan, Service Vlan Priority and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **deny** - Specifies the packets to be rejected based on the MAC address and the associated parameters
- **show access-lists** - Displays the access list statistics

## 65.4.18 deny

This command specifies the packets to be rejected based on the MAC address and the associated parameters.

```
deny { any | host <src-mac-address> } { any | host <dest-mac-address> } [ {
aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |
etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios
| vines-echo | vines-ip | xns-id | <short (0-65535)> } ] [ encaps-type <integer
(1-65535)> ] [ vlan <vlan-id (1-4094)>] [ priority <short (1-255)>] [
outerEtherType < integer (1-65535)> ] [ svlan-id <vlan-id (1-4094)>] [cvlan-
priority <priority (0-7)>] [ svlan-priority <value (0-7)>] [ { single-tag |
double-tag } ]
```

|                           |                                             |                                                                                                      |
|---------------------------|---------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>any   host &lt;src-mac-address &gt;</b>  | - Source MAC address to be matched with the packet                                                   |
|                           | <b>any   host &lt;dest-mac-address &gt;</b> | - Destination MAC address to be matched with the packet                                              |
|                           | <b>aarp</b>                                 | - EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address |
|                           | <b>amber</b>                                | - EtherType DEC-Amber                                                                                |
|                           | <b>dec-spanning</b>                         | - EtherType Digital Equipment Corporation (DEC) spanning tree                                        |
|                           | <b>decnet-iv</b>                            | - EtherType DECnet Phase IV protocol                                                                 |
|                           | <b>diagnostic</b>                           | - EtherType DEC-Diagnostic                                                                           |
|                           | <b>dsm</b>                                  | - EtherType DEC-DSM/DDP                                                                              |
|                           | <b>etype-6000</b>                           | - EtherType 0x6000                                                                                   |
|                           | <b>etype-8042</b>                           | - EtherType 0x8042                                                                                   |
|                           | <b>lat</b>                                  | - EtherType DEC-LAT                                                                                  |
|                           | <b>lavc-sca</b>                             | - EtherType DEC-LAVC-SCA                                                                             |

---

|                       |                                                                                                                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mop-console</b>    | - EtherType DEC-MOP Remote Console                                                                                                                                                                      |
| <b>mop-dump</b>       | - EtherType DEC-MOP Dump                                                                                                                                                                                |
| <b>msdos</b>          | - EtherType DEC-MSDOS                                                                                                                                                                                   |
| <b>mumps</b>          | - EtherType DEC-MUMPS                                                                                                                                                                                   |
| <b>netbios</b>        | - EtherType DEC- Network Basic Input/Output System (NETBIOS)                                                                                                                                            |
| <b>vines-echo</b>     | - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems                                                                                                                         |
| <b>vines-ip</b>       | - EtherType VINES IP                                                                                                                                                                                    |
| <b>xns-id</b>         | - EtherType Xerox Network Systems (XNS) protocol suite                                                                                                                                                  |
| <b>encaptype</b>      | - Encapsulation Type                                                                                                                                                                                    |
| <b>vlan</b>           | - VLAN ID to be filtered                                                                                                                                                                                |
| <b>priority</b>       | - The priority of the L2 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. |
| <b>outerEtherType</b> | - EtherType value to match on Service vlan tag                                                                                                                                                          |
| <b>svlan-id</b>       | - Service VLAN value to match against incoming packets.                                                                                                                                                 |
| <b>cvlan-priority</b> | - Customer VLAN priority value to match against incoming packets.                                                                                                                                       |
| <b>svlan-priority</b> | - Service VLAN priority value to match against incoming packets.                                                                                                                                        |
| <b>single-tag</b>     | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                                   |

**double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL MAC Configuration Mode

**Package** Metro

**Defaults** vlan-id - 0

priority - 1

outerEtherType - 0

svlan-id - 0

cvlan-priority - -1

svlan-priority - -1

single-tag | double-tag - Single tag

**Example**

```
iss(config-ext-macl)# deny any host 00:11:22:33:44:55 priority 200
```



- MAC access list must have been created.
- OuterEtherType, Service Vlan, Service Vlan Priority and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **show access-lists** - Displays the access list statistics

## 65.4.19 show access-lists

This command displays the access lists configuration.

```
show access-lists [ mac <access-list-number (1-65535)> ]
```

### For Metro

```
show access-lists [{ip | mac}] <access-list-number (1-65535)> ]
```

|                           |                                                 |                                                                   |
|---------------------------|-------------------------------------------------|-------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>mac &lt;access-list-number (1-65535)&gt;</b> | - Displays the access list. The number ranges between 1 and 65535 |
|                           | <b>ip</b>                                       | - IP Access List                                                  |
|                           | <b>mac</b>                                      | - MAC Access List                                                 |

**Mode** Privileged/User EXEC Mode

**Example**

```
iss# show access-lists
MAC ACCESS LISTS
-----

Extended MAC Access List 1
-----
Vlan Id                : 1
Destination MAC Address : 00:02:03:04:05:04
Source MAC Address     : 00:00:00:00:00:00
Filter Action          : Permit
Status                 : Active

iss# show access-lists mac 1
Extended MAC Access List 1
-----
Vlan Id                : 1
Destination MAC Address : 00:02:03:04:05:04
Source MAC Address     : 00:00:00:00:00:00
Filter Action          : Permit
```

---

Status : Active

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters
- **deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched
- **permit host dest-mac** - Specifies the packets to be forwarded depending upon the associated parameters
- **deny host dest-mac** - Denies traffic if the conditions defined in the deny statement
- **permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- **deny - ip/ospf/pim/protocol type** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters
- **deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters
- **permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters
- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- **ip access-group** - Enables access control for the packets on the interface
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **deny** - Specifies the packets to be rejected based on the MAC address and the associated parameters

## 65.5 xCAT Specific Commands

This section describes the CLI commands executable only in xCAT target for configuring ACL feature supported by ISS.

The list of CLI commands for the configuration of ACL is as follows:

- ip access-list
- mac access-list extended
- user-defined access-list
- userdefined-list
- permit usr-defined-packet-type
- deny usr-defined-packet-type
- permit - standard mode
- deny - standard mode
- permit- ip/ospf/pim/protocol type
- permit ipv6
- deny ipv6
- deny - ip/ospf/pim/protocol type
- permit tcp
- deny tcp
- permit udp
- deny udp
- permit icmp
- deny icmp
- ip access-group
- mac access-group
- user-defined access-group
- Permit
- deny
- show access-lists

## 65.5.1 ip access-list

This command creates IP ACLs and enters the IP Access-list configuration mode. Standard access lists create filters based on IP address and network mask only (L3 filters only). Extended access lists enables specification of filters based on the type of protocol, range of TCP/UDP ports as well as the IP address and network mask (Layer 4 filters).

Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode.

The no form of the command deletes the IP access-list.

```
ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> }
```

```
no ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> }
```

|                           |                 |                               |
|---------------------------|-----------------|-------------------------------|
| <b>Syntax Description</b> | <b>standard</b> | - Standard access-list number |
|                           | <b>extended</b> | - Extended access-list number |

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config)# ip access-list standard 1`



ACLs on the system perform both access control and Layer 3 field classification. To define Layer 3 fields' access-lists the `ip access-list` command must be used.

### Related Commands

- **permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters
- **deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched
- **permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- **deny - ip/ospf/pim/protocol type** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters
- **deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters
- **permit udp** - Specifies the UDP packets to be forwarded based on the associated

---

parameters

- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- **ip access-group** - Enables access control for the packets on the interface
- **show access-lists** - Displays the access list configuration

## 65.5.2 mac access-list extended

This command creates Layer 2 MAC ACLs, that is, this command creates a MAC access-list and returns the MAC-Access list configuration mode to the user. The no form of the command deletes the MAC access-list.

```
mac access-list extended <access-list-number (1-65535)>
```

```
no mac access-list extended <short (1-65535)>
```

|                    |                    |   |                    |
|--------------------|--------------------|---|--------------------|
| <b>Syntax</b>      | <b>access-</b>     | - | Access list number |
| <b>Description</b> | <b>list-number</b> |   |                    |

|             |                           |
|-------------|---------------------------|
| <b>Mode</b> | Global Configuration Mode |
|-------------|---------------------------|

|                |                                 |
|----------------|---------------------------------|
| <b>Package</b> | Workgroup, Enterprise and Metro |
|----------------|---------------------------------|

|                |                                         |
|----------------|-----------------------------------------|
| <b>Example</b> | iss(config)# mac access-list extended 5 |
|----------------|-----------------------------------------|



ACLs on the system perform both access control and layer 2 field classification. To define Layer 2 access lists, the mac access-list command must be used.

### Related Commands

- **show access-lists** - Displays the access list configuration
- **Permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **deny** - Specifies the packets to be rejected based on the MAC address and the associated parameters
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface.

## 65.5.3 user-defined access-list

This command creates a user defined access-list. The no form of the command deletes the user defined access-list. The value ranges between 1 to 65535.

```
user-defined access-list <access-list-number (1-65535)>
```

```
no user-defined access-list <short (1-65535)>
```

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config)# user-defined access-list 5`



ACLs on the system perform both access control and layer 2 field classification based on user defined bytes in the packets.

**Related Commands**

- **permit usr-defined-packet-type** - Permits Packet Based on User Defined Packet type
- **Permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **deny** - Specifies the packets to be rejected based on the MAC address and the associated parameters
- **show access-lists** - Displays the access list configuration
- **userdefined-list** - Creates a user defined access list by applying AND, OR, NOT operation ( regular expressions) on existing ACL rules or specifying match on user-defined packet offsets.
- **user-defined access-group** - Applies a user defined access list (ACL) to an interface.

## 65.5.4 userdefined-list

This command creates a user defined access list after application of regular expressions AND, OR, NOT on existing ACL rules

```
userdefined-list {{ ip-acl1-and-ip-acl2| ip-acl1-or-ip-acl2 | mac-acl1-and-
mac-acl2 | mac-acl1-and-ip-acl2 | mac-acl1-or-mac-acl2 | ip-acl1-or-mac-acl2
} <short (1-65535)> <short (1-65535)> | { not-ip-acl1 | not-mac-acl1 }
<short (1-65535)>} priority <short (1-255)>
```

|                    |                              |   |                                                                                                                                                                                                                                                              |
|--------------------|------------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>ip-acl1-and-ip-acl2</b>   | - | Performs AND operation on two Layer 3 ACL Rules ( acl1 , acl2). And create a new layer 3 ACL rule that is represented by this user defined access-list..The filter action corresponding to the new ACL rule is identical to the base rules.                  |
| <b>Description</b> | <b>ip-acl1-or-ip-acl2</b>    | - | Performs OR operation on two layer 3 ACL Rules. This operation results in applying the action of ACL Rule 1 on ACL Rule 2                                                                                                                                    |
| <b>n</b>           | <b>mac-acl1-and-mac-acl2</b> | - | Performs AND operation on two layer 2 ACL Rules and create a new layer 2 ACL rule that is represented by this user defined access-list. The filter action corresponding to the new ACL rule is identical to the base rules.                                  |
|                    | <b>mac-acl1-and-ip-acl2</b>  | - | Performs AND operation on two ACL rules - acl1 ( layer 2 ACL Rule) and acl2 ( Layer 3 ACL rule) and create an new ACL Rule represented by this user defined access-list. The filter action corresponding to the new ACL rule is identical to the base rules. |
|                    | <b>mac-acl1-or-mac-acl2</b>  | - | Performs OR operation on two Layer 2 ACL Rules and results in application of filter-action of ACL1 on ACL2                                                                                                                                                   |
|                    | <b>ip-acl1-or-mac-acl2</b>   | - | Performs OR operation on Layer 3 ACL Rule (ACL1) using Layer 2 ACL rule ( ACL2) and results in application of filter-action of ACL1 on ACL2.                                                                                                                 |
|                    | <b>not-ip-acl1</b>           | - | Performs NOT operation on ACL Rule 1 and derive new Rule. The filter action for the derived ACL Rule is “deny” if base Rule is configured for filter action “permit” and vice-versa. Other actions are not applicable for this operation                     |

**not-mac-acl1** - Performs NOT operation on ACL Rule 1 and derive new Rule. The filter action for the derived ACL Rule is “deny” if base Rule is configured for filter action “permit” and vice-versa. Other actions are not applicable for this operation

**Priority <short (1-255)>** - Decides the filter rule which is applicable, when the packet matches with more than one filter rules. Higher value of ‘filter priority’ implies a higher priority. This value ranges between 1 and 255.

**Mode** User defined Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example**

```
iss(config-userdef-acl)# userdefined-list ip-acl1-and-ip-acl2
15 123
```

**Related Commands**

- **show access-lists** - Displays the access list configuration
- **user-defined access-list** - Creates user defined access-list.

## 65.5.5 permit usr-defined-packet-type

This command permits packets matching a particular User Defined Byte and by specifying the packet type – namely user-defined, tcp-ipv4, udp, mpls, ipv4, ipv6, frag-ip.

```
permit usr-defined-packet-type { user-def | tcp-ipv4 | udp-ipv4 | mpls | ipv4
| ipv6 | frag-ip } offset-base {12 | 13 | 14 | ipv6-ext-hdr | ether-type |
<short(0-127)>} offset1 <short(0-127)> <short(0-255)>[offset2 <short(0-127)>
<short(0-255)>][offset3 <short(0-127)> <short(0-255)>][offset4 <short(0-127)>
<short(0-255)>][offset5 <short(0-127)> <short(0-255)>][offset6 <short(0-127)>
<short(0-255)>][redirect {interface <ifXtype> <ifnum> | <ifXtype><iface_list>
[<ifXtype><iface_list>]load-balance {src-ip | dst-ip | src-mac | dst-mac |
vlanid | src-tcport| dst-tcport | src-udpport | dst-udpport | udb <short(0-
127)>}}][sub-action {none | modify-vlan<short (1-4094)> | nested-vlan <short
(1 -4094)>}] priority <short (1-255)>
```

|                               |                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax<br/>Description</b> | <b>user-def</b>    | - Specifies the packet type as user defined.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                               | <b>tcp-ipv4</b>    | - Specifies the packet type as tcp in the ipV4 packet.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                               | <b>udp-ipv4</b>    | - Specifies the packet type as udp in the ipV4 packet.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                               | <b>mpls</b>        | - Specifies the packet type as mpls.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                               | <b>ipv4</b>        | - Specifies the packet type as ipv4.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                               | <b>ipv6</b>        | - Specifies the packet type as ipv6.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                               | <b>frag-ip</b>     | - Specifies the packet type as fragmented ip.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                               | <b>offset-base</b> | - Specifies the start of the packet from which the user defined byte should be considered. <ul style="list-style-type: none"> <li>• 12 – Start of the packet is considered as layer 2</li> <li>• 13 – Start of the packet is considered as layer 3</li> <li>• 14 – Start of the packet is considered as layer 4</li> <li>• ipv6-ext-hdr - Start of the packet is considered as ipv6 extended header.</li> <li>• ether-type – Start of the packet is considered as ether type.</li> </ul> |

- 
- |                     |                                                                                                                                                                                                                                                                              |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>offset1</b>      | - Specifies the offset position and offset value that needs to be considered as the match for offset1. The two input value ranges 0 to 127 and 0 to 255.                                                                                                                     |
| <b>offset2</b>      | - Specifies the offset position and offset value value that needs to be considered as the match for offset 2. The two input value ranges 0 to 127 and 0 to 255.                                                                                                              |
| <b>Offset3</b>      | - Specifies the offset position and offset value that needs to be considered as the match for offset 3. The two input value ranges 0 to 127 and 0 to 255.                                                                                                                    |
| <b>Offset4</b>      | - Specifies the offset position and offset value that needs to be considered as the match for offset 4. The two input value ranges 0 to 127 and 0 to 255.                                                                                                                    |
| <b>Offset5</b>      | - Specifies the offset position and offset value that needs to be considered as the match for offset 5. The two input value ranges 0 to 127 and 0 to 255.                                                                                                                    |
| <b>Offset6</b>      | - Specifies the offset position and value that needs to be considered as the match for offset 6. The two input value ranges 0 to 127 and 0 to 255.                                                                                                                           |
| <b>Redirect</b>     | - Redirects the packet to the destination interface or set of interfaces. <ul style="list-style-type: none"><li>• ifXtype – Specifies the interfae type</li><li>• ifnum – Specifies the interface number</li><li>• iface_list – Specifies the list of interfaces</li></ul>   |
| <b>load-balance</b> | - Specifies the parameters based on which the traffic distribution needs to be done. Options are: <ul style="list-style-type: none"><li>• src-ip</li><li>• dst-ip</li><li>• src-mac</li><li>• dst-mac</li><li>• vlanid</li><li>• src-tcpport</li><li>• dst-tcpport</li></ul> |

- src-udpport
- dst-udpport
- udb

Options in the Layer 3 header are classified as IPv4 or IPv6 based on packet type

**sub-action**

- Specifies the VLAN specific sub action to be performed on the packet -
  - none – Actions relating to the VLAN ID will not be considered.
  - modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
  - nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.

**Priority** <short (1-255)>

- Decides the filter rule which is applicable, when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. This value ranges between 1 and 255.

**Mode** User defined Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config-userdef-acl)# permit usr-defined-packet-type user-def offset-base 12 offset1 5 10 load-balance src-ip`

- Related Commands**
- **show access-lists** - Displays the access list configuration
  - **user-defined access-list** - Creates the user defined access-list.

## 65.5.6 deny usr-defined-packet-type

This command denies packets matching a particular User Defined Byte and by specifying the packet type – namely user-defined, tcp-ipv4, udp, mpls, ipv4, ipv6, frag-ip.

```
deny  usr-defined-packet-type { user-def | tcp-ipv4 | udp-ipv4 | mpls | ipv4
|ipv6 | frag-ip }offset-base {12 | 13 | 14 | ipv6-ext-hdr | ether-type |
<short(0-127)>} offset1 <short(0-127)> <short(0-255)> [offset2 <short(0-127)>
<short(0-255)>][offset3 <short(0-127)> <short(0-255)>] [offset4 <short(0-127)>
<short(0-255)>][offset5 <short(0-127)> <short(0-255)>] [offset6 <short(0-127)>
<short(0-255)>] priority <short(1-255)>
```

### Syntax Description

- |                                |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>usr-defined-packet-type</b> | - | <ul style="list-style-type: none"> <li>• user-def – Specifies the packet type as user defined</li> <li>• tcp-ipv4 – Specifies the packet type as tcp in the ipV4 packet.</li> <li>• udp-ipv4 - Specifies the packet type as udp in the ipV4 packet.</li> <li>• mpls - Specifies the packet type as mpls.</li> <li>• ipv4 - Specifies the packet type as ipv4.</li> <li>• ipv6 - Specifies the packet type as ipv6.</li> <li>• frag-ip - Specifies the packet type as fragmented ip.</li> </ul>                                             |
| <b>offset-base</b>             | - | <ul style="list-style-type: none"> <li>• Specifies the start of the packet from which the user defined byte should be considered <ul style="list-style-type: none"> <li>• 12 – Start of the packet is considered as layer 2</li> <li>• 13 – Start of the packet is considered as layer 3</li> <li>• 14 – Start of the packet is considered as layer 4</li> <li>• ipv6-ext-hdr – Start of the packet is considered as ipv6 extended header.</li> <li>• ether-type – Start of the packet is considered as ether type.</li> </ul> </li> </ul> |
| <b>offset1</b>                 | - | <ul style="list-style-type: none"> <li>• Specifies the offset position and offset value that needs to be considered as the match for offset1. The two input value ranges 0 to 127 and 0 to 255.</li> </ul>                                                                                                                                                                                                                                                                                                                                 |
| <b>offset2</b>                 | - | <ul style="list-style-type: none"> <li>• Specifies the offset position and offset value that needs to be considered as the match for offset2.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                   |

---

|                         |                                                                                                                       |                                                                                                                                                                                                           |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         |                                                                                                                       | The two input value ranges 0 to 127 and 0 to 255                                                                                                                                                          |
| <b>Offset3</b>          | -                                                                                                                     | Specifies the offset position and offset value that needs to be considered as the match for offset3. The two input value ranges 0 to 127 and 0 to 255                                                     |
| <b>Offset4</b>          | -                                                                                                                     | Specifies the offset position and offset value that needs to be considered as the match for offset4. The two input value ranges 0 to 127 and 0 to 255.                                                    |
| <b>Offset5</b>          | -                                                                                                                     | Specifies the offset position and offset value that needs to be considered as the match for offset5. The two input value ranges 0 to 127 and 0 to 255                                                     |
| <b>Offset6</b>          | -                                                                                                                     | Specifies the offset position and offset value that needs to be considered as the match for offset6. The two input value ranges 0 to 127 and 0 to 255                                                     |
| <b>Priority</b>         | <b>&lt;short (1-255)&gt;</b>                                                                                          | - Decides the filter rule which is applicable, when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. This value ranges between 1 and 255. |
| <b>Mode</b>             | User defined Configuration Mode                                                                                       |                                                                                                                                                                                                           |
| <b>Package</b>          | Workgroup, Enterprise and Metro                                                                                       |                                                                                                                                                                                                           |
| <b>Example</b>          | <pre>iss(config-userdef-acl)# deny usr-defined-packet-type user-def offset-base 12 offset1 112 25</pre>               |                                                                                                                                                                                                           |
| <b>Related Commands</b> | <ul style="list-style-type: none"> <li>• <b>show access-lists</b> - Displays the access list configuration</li> </ul> |                                                                                                                                                                                                           |

## 65.5.7 permit - standard mode

This command specifies the packets to be forwarded depending upon the associated parameters. Standard IP access lists use source addresses for matching operations.

```
permit { any | host <src-ip-address> | <network-src-ip> <mask> } [{ any | host
<dest-ip-address> | <network-dest-ip> <mask>}] redirect {interface <ifXtype>
<ifnum> | <ifXtype><iface_list> [<ifXtype><iface_list>] load-balance {src-ip |
dst-ip | src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport | src-udpport
| dst-udpport}}] [sub-action {none | modify-vlan<short (1-4094)> | nested-vlan
<short (1 -4094)>}] priority <short (1-255)>
```

|                    |                                                                |   |                                                                                                                                                                                                                                                                                               |
|--------------------|----------------------------------------------------------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | any host                                                       | - | Source IP address can be                                                                                                                                                                                                                                                                      |
| <b>Description</b> | <b>n</b><br><src-ip-address> <br><network-src-ip-<br>><mask>   |   | <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the dotted decimal address</li> <li>• the IP address of the host that the packet is from and the network mask to use with the source IP address</li> </ul>                                                                       |
|                    | any host<br><dest-ip-address> <br>< network-dest-ip><br><mask> |   | <ul style="list-style-type: none"> <li>- Destination IP address can be</li> <li>• 'any' or</li> <li>• the dotted decimal address or</li> <li>• the IP address of the host that the packet is destined for and the network mask to use with the destination IP address</li> </ul>              |
|                    | <b>redirect</b>                                                |   | <ul style="list-style-type: none"> <li>- Redirects the action to the destination interface or set of interfaces.</li> <li>• ifXtype – Specifies the interface type</li> <li>• ifnum – Specifies the interface number</li> <li>• iface_list – Specifies the list of interfaces</li> </ul>      |
|                    | <b>load-balance</b>                                            |   | <ul style="list-style-type: none"> <li>- Specifies the parameters based on which the traffic distribution needs to be done. Options are:</li> <li>• src-ip</li> <li>• src-mac</li> <li>• dst-ip</li> <li>• dst-mac</li> <li>• vlanid</li> <li>• src-tcpport</li> <li>• dst-tcpport</li> </ul> |

- src-udpport
- dst-udpport

Options in the Layer 3 header are classified as IPv4 or IPv6 based on packet type

- sub-action**
- Specifies the VLAN specific sub action to be performed on the packet -
    - none – Actions relating to the VLAN ID will not be considered.
    - modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
    - nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.
- Priority**      **<short**      -      Decides the filter rule which is applicable, when the  
(1–255) >

**Mode**            IP ACL Configuration (standard)

**Package**        Workgroup, Enterprise and Metro

**Example**        `iss(config-std-nacl)# permit host 100.0.0.10`

- Related Command s**
- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
  - **deny – standard mode** - Denies traffic if the conditions defined in the deny statement are matched
  - **show access-lists** - Displays the access list configuration

## 65.5.8 deny - standard mode

This command denies traffic if the conditions defined in the deny statement are matched.

```
deny{ any | host <src-ip-address> | <network-src-ip> <mask> } [ { any | host
<dest-ip-address> | <network-dest-ip> <mask> } ] priority <short (1-255)>
```

|                    |                                                                                                  |                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <code>any host</code>                                                                            | - Source IP address can be                                                                                                                                                                                                                                         |
| <b>Description</b> | <code>src-ip-address </code><br><code>&lt;network-src-ip&gt;</code><br><code>&lt;mask&gt;</code> | <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is from and the network mask to use with the source IP address</li> </ul>              |
|                    | <code>any host</code>                                                                            | - Destination IP address can be                                                                                                                                                                                                                                    |
|                    | <code>dest-ip-address </code><br><code>&lt;network-dest-ip&gt;</code><br><code>mask&gt;</code>   | <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is destined for and the network mask to use with the destination IP address</li> </ul> |
|                    | <b>Priority</b> <code>&lt;short (1-255)&gt;</code>                                               | - Decides the filter rule which is applicable, when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. This value ranges between 1 and 255.                                                          |

**Mode** IP ACL Configuration (standard)

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config-std-nacl)# deny host 100.0.0.10 any`

- Related Commands**
- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
  - `permit - standard mode` - Specifies the packets to be forwarded depending upon the associated parameters
  - `show access-lists` - Displays the access list configuration

## 65.5.9 permit- ip/ospf/pim/protocol type

This command allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.

```
permit { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-
address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-
ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay |
normal |<value (0-7)>} | dscp <value (0-63)>} ] [priority <value (1-
255)>] [redirect {interface <ifXtype> <ifnum> | <ifXtype><iface_list>
[<ifXtype><iface_list>] load-balance {src-ip | dst-ip | src-mac | dst-mac |
vlanid | src-tcpport | dst-tcpport | src-udpport | dst-udpport}}] [sub-action
{none | modify-vlan<short (1-4094)> | nested-vlan <short (1 -4094)>}]
```

### For Metro

```
permit { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-
address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-
ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay |
normal |<value (0-7)>} | dscp <value (0-63)>} ] [ priority <value (1-255)>] [
svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-
id (1-4094)>] [ cvlan-priority <value (0-7)>] [ { single-tag | double-tag } ]
[redirect {interface <ifXtype> <ifnum> | <ifXtype><iface_list>
[<ifXtype><iface_list>] load-balance {src-ip | dst-ip | src-mac | dst-mac |
vlanid | src-tcpport | dst-tcpport | src-udpport | dst-udpport}}] [sub-action
{none | modify-vlan<short (1-4094)> | nested-vlan <short (1 -4094)>}]
```

|                           |                                                                                                                   |                                                                                                                                                                                                                                                                                     |
|---------------------------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | ip  ospf pim <br>< protocol-type<br>(1-255)><br><br>any  host<br><src-ip-address> <br><src-ip-address> <<br>mask> | - Type of protocol for the packet. It can also be a protocol number.                                                                                                                                                                                                                |
|                           | <br>any host<br><dest-ip-address> <br><dest-ip-address><br><mask>                                                 | - Source IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the dotted decimal address or</li> <li>• the IP Address of the network or the host that the packet is from and the network mask to use with the source address.</li> </ul>                  |
|                           |                                                                                                                   | - Destination IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the dotted decimal address or</li> <li>• the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> |

---

|                       |                                                                                                                                                                                                                                                                                                    |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>tos</b>            | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                                                                 |
| <b>priority</b>       | - The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.                                                                                            |
| <b>svlan-id</b>       | - Service VLAN value to match against incoming packets.                                                                                                                                                                                                                                            |
| <b>svlan-priority</b> | - Service VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                   |
| <b>cvlan-id</b>       | - Customer VLAN value to match against incoming packets.                                                                                                                                                                                                                                           |
| <b>cvlan-priority</b> | - Customer VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                  |
| <b>single-tag</b>     | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                                                                                                                              |
| <b>double-tag</b>     | - Filter to be applied on double VLAN tagged packets.                                                                                                                                                                                                                                              |
| <b>redirect</b>       | - Redirects the action to the destination interface or set of interfaces. <ul style="list-style-type: none"><li>• ifXtype – Specifies the interface type</li><li>• ifnum – Specifies the interface number</li><li>• iface_list – Specifies the list of interfaces</li></ul>                        |
| <b>load-balance</b>   | - Specifies the parameters based on which the traffic distribution needs to be done. Options are: <ul style="list-style-type: none"><li>• src-ip</li><li>• dst-ip</li><li>• src-mac</li><li>• dst-mac</li><li>• vlanid</li><li>• src-tcpport</li><li>• dst-tcpport</li><li>• src-udpport</li></ul> |

- dst-udpport
- Specifies the VLAN specific sub action to be performed on the packet -
  - none – Actions relating to the VLAN ID will not be considered.
  - modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
  - nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults**

|                         |   |            |
|-------------------------|---|------------|
| protocol-type           | - | 255        |
| priority                | - | 1          |
| svlan-id                | - | 0          |
| svlan-priority          | - | -1         |
| cvlan-id                | - | 0          |
| cvlan-priority          | - | -1         |
| single-tag   double-tag | - | Single tag |

**Example** `iss(config-ext-nacl)# permit 200 host 100.0.0.10 any tos 6 load balance src-ip`



- Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.
- Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

**Related Commands**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access list configuration
- `deny - ip/ospf/pim/protocol type` - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched

## 65.5.10 permit ipv6

This command specifies IP packets to be forwarded based on protocol and associated parameters.

```
permit ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr>
<integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> }} [redirect
{interface <ifXtype> <ifnum> | <ifXtype><iface_list>
[<ifXtype><iface_list>]load-balance {src-ip | dst-ip | src-mac | dst-mac |
vlanid | src-tcpport| dst-tcpport | src-udpport | dst-udpport}}][sub-action
{none | modify-vlan<short (1-4094)> | nested-vlan <short (1 -4094)>}]priority
<short (1-255)>]
```

|                           |                                                           |   |                                                                                                                                                                                                                                                                                                                                     |
|---------------------------|-----------------------------------------------------------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>flow-label</b>                                         | - | Flow identifier in IPv6 header.                                                                                                                                                                                                                                                                                                     |
|                           | <b>any   host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</b> | - | Source address of the host / any host.                                                                                                                                                                                                                                                                                              |
|                           | <b>any   host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</b> | - | Destination address of the host / any host.                                                                                                                                                                                                                                                                                         |
|                           | <b>redirect</b>                                           |   | Redirects the action to the destination interface or set of interfaces. <ul style="list-style-type: none"> <li>• ifXtype – Specifies the interface type</li> <li>• ifnum – Specifies the interface number</li> <li>• iface_list – Specifies the list of interfaces</li> </ul>                                                       |
|                           | <b>load-balance</b>                                       |   | Specifies the parameters based on which the traffic distribution needs to be done. Options are: <ul style="list-style-type: none"> <li>• src-ip</li> <li>• dst-ip</li> <li>• src-mac</li> <li>• dst-mac</li> <li>• vlanid</li> <li>• src-tcpport</li> <li>• dst-tcpport</li> <li>• src-udpport</li> <li>• dst-udpport</li> </ul>    |
|                           | <b>sub-action</b>                                         |   | Specifies the VLAN specific sub action to be performed on the packet - <ul style="list-style-type: none"> <li>• none – Actions relating to the VLAN ID will not be considered.</li> <li>• modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</li> </ul> |

|                                                                                   |                                                                                        |                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                   |                                                                                        | <ul style="list-style-type: none"> <li>nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.</li> </ul>                                                                      |
| <b>Priority</b>                                                                   | <b>&lt;short (1–255)&gt;</b>                                                           | - Decides the filter rule which is applicable, when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. This value ranges between 1 and 255. |
| <b>Mode</b>                                                                       | ACL Extended Access List Configuration Mode                                            |                                                                                                                                                                                                           |
| <b>Package</b>                                                                    | Workgroup, Enterprise and Metro                                                        |                                                                                                                                                                                                           |
| <b>Example</b>                                                                    | <pre>iss(config-ext-nacl)# permit ipv6 host c004::04 28 any load- balance src-ip</pre> |                                                                                                                                                                                                           |
|  | Flow label cannot be configured along with either source/destination IP address.       |                                                                                                                                                                                                           |
| <b>Related Commands</b>                                                           | <b>show access-lists</b> - Displays the access lists configuration.                    |                                                                                                                                                                                                           |

## 65.5.11 deny ipv6

This command specifies IPv6 packets to be rejected based on protocol and associated parameters.

```
deny ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr> <integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> }} priority <short (1-255)>
```

|                           |                                                           |   |                                                                                                                                                                                                         |
|---------------------------|-----------------------------------------------------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>flow-label</b>                                         | - | Flow identifier in IPv6 header.                                                                                                                                                                         |
|                           | <b>any   host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</b> | - | Source address of the host / any host.                                                                                                                                                                  |
|                           | <b>any   host &lt;ip6_addr&gt; &lt;integer(0-128)&gt;</b> | - | Destination address of the host / any host.                                                                                                                                                             |
|                           | <b>Priority &lt;short (1-255)&gt;</b>                     | - | Decides the filter rule which is applicable, when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. This value ranges between 1 and 255. |

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example**

```
iss(config-ext-nacl)# deny ipv6 host c004::04 28 any
iss(config-ext-nacl)# deny ipv6 flow-label 40
```



Flow label cannot be configured along with either source/destination IP address.

**Related Commands** `show access-lists` - Displays the access lists configuration.

## 65.5.12 deny - ip/ospf/pim/protocol type

This command denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.

```
deny { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>} ] [ priority <value (1-255)>]
```

### For Metro

```
deny { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } [ {tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>} ] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-4094)>] [ svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value (0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | ip  ospf pim <br><protocol-type<br>(1-255)><br><br>any  host<br><src-ip-address> <br><src-ip-address><br><mask><br><br>any host<br><dest-ip-address> <br><dest-ip-address><br><mask><br><br>tos<br><br>priority | <ul style="list-style-type: none"> <li>- Type of protocol for the packet. It can also be a protocol number.</li> <li>- Source IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul> </li> <li>- Destination IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> </li> <li>- Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.</li> <li>- The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.</li> </ul> |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- svlan-id** - Service VLAN value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

- Defaults**
- protocol type - 255
  - priority - 1
  - svlan-id - 0
  - svlan-priority - -1
  - cvlan-id - 0
  - cvlan-priority - -1
  - single-tag | double-tag - Single tag

**Example** `iss(config-ext-nacl)# deny ospf any host 10.0.0.1 tos max-throughput`



- Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.
- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands** • `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode

- **permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- **show access-lists** - Displays the access list configuration

## 65.5.13 permit tcp

This command specifies the TCP packets to be forwarded based on the associated parameters.

```
permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp <value (0-
63)>}] [ priority <short(1-255)>] [redirect {interface <ifXtype> <ifnum> |
<ifXtype><iface_list> [<ifXtype><iface_list>] load-balance {src-ip | dst-ip |
src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport | src-udpport | dst-
udpport}}] [sub-action {none | modify-vlan<short (1-4094)> | nested-vlan
<short (1 -4094)>}]
```

### For Metro

```
permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp <value (0-
63)>}] [ priority <short (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-
priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value
(0-7)>] [ { single-tag | double-tag } ] [redirect {interface <ifXtype>
<ifnum> | <ifXtype><iface_list> [<ifXtype><iface_list>] load-balance {src-ip |
dst-ip | src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport | src-udpport
| dst-udpport}}] [sub-action {none | modify-vlan<short (1-4094)> | nested-
vlan <short (1 -4094)>}]
```

|                           |                                                                             |   |                                                                                                                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | tcp                                                                         | - | Transport Control Protocol                                                                                                                                                                                                                                      |
|                           | any  host<br><br><src-ip-address>  <br><br><src-ip-address> <<br>src-mask > | - | Source IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the dotted decimal address OR</li> <li>• the IP address of the network or the host that the packet is from and the network mask to use with the source address</li> </ul> |
|                           | port-number                                                                 | - | Port Number. The input for the source and the destination port-number is prefixed with one of the following operators. <ul style="list-style-type: none"> <li>• eq=equal</li> </ul>                                                                             |

|                                  |                                                                                                                                                                                                                                                     |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                  | <ul style="list-style-type: none"> <li>• lt=less than</li> <li>• gt=greater than</li> <li>• range=a range of ports; two different port numbers must be specified</li> </ul>                                                                         |
| <b>any   host</b>                | - Destination IP address can be                                                                                                                                                                                                                     |
| <b>&lt;dest-ip-address&gt;</b>   | <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the dotted decimal address or</li> <li>• the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> |
| <b>  &lt;dest-ip-address&gt;</b> |                                                                                                                                                                                                                                                     |
| <b>&lt; dest-mask &gt;</b>       |                                                                                                                                                                                                                                                     |
| <b>ack</b>                       | - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3).                                                                                                                                              |
| <b>rst</b>                       | - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3).                                                                                                                                                           |
| <b>tos</b>                       | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                  |
| <b>priority</b>                  | - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.                                                |
| <b>svlan-id</b>                  | - Service VLAN value to match against incoming packets.                                                                                                                                                                                             |
| <b>svlan-priority</b>            | - Service VLAN priority value to match against incoming packets.                                                                                                                                                                                    |
| <b>cvlan-id</b>                  | - Customer VLAN value to match against incoming packets.                                                                                                                                                                                            |
| <b>cvlan-priority</b>            | - Customer VLAN priority value to match against incoming packets.                                                                                                                                                                                   |
| <b>single-tag</b>                | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                                                                               |
| <b>double-tag</b>                | - Filter to be applied on double VLAN tagged packets.                                                                                                                                                                                               |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                          |           |     |     |                                                                                       |     |                                                                                       |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----|-----|---------------------------------------------------------------------------------------|-----|---------------------------------------------------------------------------------------|
| <b>redirect</b>     | <p>Redirects the action to the destination interface or set of interfaces.</p> <ul style="list-style-type: none"> <li>• ifXtype – Specifies the interface type</li> <li>• ifnum – Specifies the interface number</li> <li>• iface_list – Specifies the list of interfaces</li> </ul>                                                                                                                                                     |           |     |     |                                                                                       |     |                                                                                       |
| <b>Load-balance</b> | <p>Specifies the parameters based on which the traffic distribution needs to be done. Options are:</p> <ul style="list-style-type: none"> <li>• src-ip</li> <li>• dst-ip</li> <li>• src-mac</li> <li>• dst-mac</li> <li>• vlanid</li> <li>• src-tcpport</li> <li>• dst-tcpport</li> <li>• src-udpport</li> <li>• dst-udpport</li> </ul>                                                                                                  |           |     |     |                                                                                       |     |                                                                                       |
| <b>sub-action</b>   | <p>Specifies the VLAN specific sub action to be performed on the packet -</p> <ul style="list-style-type: none"> <li>• none – Actions relating to the VLAN ID will not be considered.</li> <li>• modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</li> <li>• nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.</li> </ul> |           |     |     |                                                                                       |     |                                                                                       |
| <b>Mode</b>         | ACL Extended Access List Configuration Mode                                                                                                                                                                                                                                                                                                                                                                                              |           |     |     |                                                                                       |     |                                                                                       |
| <b>Package</b>      | Workgroup, Enterprise and Metro                                                                                                                                                                                                                                                                                                                                                                                                          |           |     |     |                                                                                       |     |                                                                                       |
| <b>Defaults</b>     | <table border="0"> <tr> <td style="padding-right: 20px;">tos-value</td> <td>- 0</td> </tr> <tr> <td style="padding-right: 20px;">ack</td> <td>- 'any' (3) [indicates that the TCP ACK bit will not be checked to decide the action]</td> </tr> <tr> <td style="padding-right: 20px;">rst</td> <td>- 'any' (3) [indicates that the TCP RST bit will not be checked to decide the action]</td> </tr> </table>                              | tos-value | - 0 | ack | - 'any' (3) [indicates that the TCP ACK bit will not be checked to decide the action] | rst | - 'any' (3) [indicates that the TCP RST bit will not be checked to decide the action] |
| tos-value           | - 0                                                                                                                                                                                                                                                                                                                                                                                                                                      |           |     |     |                                                                                       |     |                                                                                       |
| ack                 | - 'any' (3) [indicates that the TCP ACK bit will not be checked to decide the action]                                                                                                                                                                                                                                                                                                                                                    |           |     |     |                                                                                       |     |                                                                                       |
| rst                 | - 'any' (3) [indicates that the TCP RST bit will not be checked to decide the action]                                                                                                                                                                                                                                                                                                                                                    |           |     |     |                                                                                       |     |                                                                                       |

---

|                         |   |            |
|-------------------------|---|------------|
| svlan-id                | - | 0          |
| svlan-priority          | - | -1         |
| cvlan-id                | - | 0          |
| cvlan-priority          | - | -1         |
| single-tag   double-tag | - | Single tag |

**Example** `iss(config-ext-nacl)# permit tcp any 10.0.0.1 load-balance scr-ip`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related  
Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters

## 65.5.14 deny tcp

This command specifies the TCP packets to be rejected based on the associated parameters.

```
deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}} | dscp <value
(0-63)>}] [ priority <short (1-255)>]
```

### For Metro

```
deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt
<port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-
reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}} | dscp <value
(0-63)>}] [ priority <short (1-255)>] [ svlan-id <vlan-id (1-4094)>] [svlan-
priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-priority <value
(0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                |                                                                                                                          |
|---------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>tcp</b>                     | - Transmission control protocol                                                                                          |
|                           | <b>any  host</b>               | - Source IP address can be                                                                                               |
|                           | <b>&lt;src-ip-address&gt; </b> | • 'any' or                                                                                                               |
|                           | <b>&lt;src-ip-address&gt;</b>  | • the word 'host' and the dotted decimal address or                                                                      |
|                           | <b>&lt;src-mask&gt;</b>        | • number of the network or the host that the packet is from and the network mask to use with the source address          |
|                           | <b>port-number</b>             | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators. |
|                           |                                | • eq=equal                                                                                                               |
|                           |                                | • lt=less than                                                                                                           |
|                           |                                | • gt=greater than                                                                                                        |
|                           |                                | • range=a range of ports; two different port numbers must be specified                                                   |

- any|host** - Destination IP address can be
- <dest-ip-address>|**
- <dest-ip-address>**
- <dest-mask>**
- 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is destined for and the network mask to use with the destination address
- ack** - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3)
- rst** - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3)
- tos** - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.
- priority** - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
- svlan-id** - Service VLAN value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- cvlan-id** - Customer VLAN value to match against incoming packets.
- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL Extended Access List Configuration Mode

|                 |                                 |                                                                                   |
|-----------------|---------------------------------|-----------------------------------------------------------------------------------|
| <b>Package</b>  | Workgroup, Enterprise and Metro |                                                                                   |
| <b>Defaults</b> | tos-value                       | - 0                                                                               |
|                 | ack                             | - 'any' (3) [indicates that TCP ACK bit will not be checked to decide the action] |
|                 | rst                             | - any' (3) [indicates that TCP RST bit will not be checked to decide the action]  |
|                 | svlan-id                        | - 0                                                                               |
|                 | svlan-priority                  | - -1                                                                              |
|                 | cvlan-id                        | - 0                                                                               |
|                 | cvlan-priority                  | - -1                                                                              |
|                 | single-tag   double-tag         | - Single tag                                                                      |

**Example**      `iss(config-ext-nacl)# deny tcp 100.0.0.10 255.255.255.0 eq 20 any`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters

## 65.5.15 permit udp

This command specifies the UDP packets to be forwarded based on the associated parameters.

```
permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [ { gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)> } ] [ { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } ] [ { gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-
number (1-65535)> <port-number (1-65535)> } ] [ { tos { max-reliability | max-
throughput | min-delay | normal | <tos-value (0-7)> } | dscp <value (0-63)> } ] [
priority <(1-255)> ] [ redirect { interface <ifXtype> <ifnum> |
<ifXtype> <iface_list> [ <ifXtype> <iface_list> ] load-balance { src-ip | dst-ip |
src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport | src-udpport | dst-
udpport } } ] [ sub-action { none | modify-vlan <short (1-4094)> | nested-vlan
<short (1 -4094)> } ]
```

### For Metro

```
permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [ { gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)> } ] [ { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } ] [ { gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)> } ] [ { tos { max-reliability | max-
throughput | min-delay | normal | <tos-value (0-7)> } | dscp <value (0-63)> } ] [
priority <short (1-255)> ] [ svlan-id <vlan-id (1-4094)> ] [ svlan-priority
<value (0-7)> ] [ cvlan-id <vlan-id (1-4094)> ] [ cvlan-priority <value (0-7)> ]
[ { single-tag | double-tag } ] [ redirect { interface <ifXtype> <ifnum> |
<ifXtype> <iface_list> [ <ifXtype> <iface_list> ] load-balance { src-ip | dst-ip |
src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport | src-udpport | dst-
udpport } } ] [ sub-action { none | modify-vlan <short (1-4094)> | nested-vlan
<short (1 -4094)> } ]
```

|                    |                                                                  |                                                                                                                                                                                                                                                                               |
|--------------------|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | udp                                                              | - User Datagram Protocol                                                                                                                                                                                                                                                      |
| <b>Description</b> | any  host<br><src-ip-address> <br><src-ip-address><br><src-mask> | - Source IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul> |
|                    | port-number                                                      | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.                                                                                                                                                      |

|                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                               | <ul style="list-style-type: none"> <li>• eq=equal</li> <li>• lt=less than</li> <li>• gt=greater than</li> <li>• range=a range of ports; two different port numbers must be specified</li> </ul>                                                                                                 |
| <b>any host</b><br><<br><b>dest-ip-address</b> >  <br>< <b>dest-ip-address</b> ><br>< <b>dest-mask</b> >                                                                      | - Destination IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> |
| <b>tos</b><br>{ <b>max-reliability</b>  <br><b>max-throughput</b>  <br><b>min-delay</b>   <b>normal</b><br>  < <b>value (0-7)</b> >  <br><b>dscp</b> < <b>value (0-63)</b> >} | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values between 0 and 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.                                                                                          |
| <b>priority</b>                                                                                                                                                               | - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.                                                                                            |
| <b>svlan-id</b>                                                                                                                                                               | - Service VLAN value to match against incoming packets.                                                                                                                                                                                                                                         |
| <b>svlan-priority</b>                                                                                                                                                         | - Service VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                |
| <b>cvlan-id</b>                                                                                                                                                               | - Customer VLAN value to match against incoming packets.                                                                                                                                                                                                                                        |
| <b>cvlan-priority</b>                                                                                                                                                         | - Customer VLAN priority value to match against incoming packets.                                                                                                                                                                                                                               |
| <b>single-tag</b>                                                                                                                                                             | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                                                                                                                           |
| <b>double-tag</b>                                                                                                                                                             | - Filter to be applied on double VLAN tagged packets.                                                                                                                                                                                                                                           |
| <b>redirect</b>                                                                                                                                                               | Redirects the action to the destination interface or set of                                                                                                                                                                                                                                     |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                          |          |   |   |                |   |    |          |   |   |                |   |    |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---|---|----------------|---|----|----------|---|---|----------------|---|----|
|                     | interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                              |          |   |   |                |   |    |          |   |   |                |   |    |
|                     | <ul style="list-style-type: none"> <li>• ifXtype – Specifies the interface type</li> <li>• ifnum – Specifies the interface number</li> <li>• iface_list – Specifies the list of interfaces</li> </ul>                                                                                                                                                                                                                                    |          |   |   |                |   |    |          |   |   |                |   |    |
| <b>load-balance</b> | <p>Specifies the parameters based on which the traffic distribution needs to be done. Options are:</p> <ul style="list-style-type: none"> <li>• src-ip</li> <li>• dst-ip</li> <li>• src-mac</li> <li>• dst-mac</li> <li>• vlanid</li> <li>• src-tcpport</li> <li>• dst-tcpport</li> <li>• src-udpport</li> <li>• dst-udpport</li> </ul>                                                                                                  |          |   |   |                |   |    |          |   |   |                |   |    |
| <b>sub-action</b>   | <p>Specifies the VLAN specific sub action to be performed on the packet -</p> <ul style="list-style-type: none"> <li>• none – Actions relating to the VLAN ID will not be considered.</li> <li>• modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</li> <li>• nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.</li> </ul> |          |   |   |                |   |    |          |   |   |                |   |    |
| <b>Mode</b>         | ACL Extended Access List Configuration Mode                                                                                                                                                                                                                                                                                                                                                                                              |          |   |   |                |   |    |          |   |   |                |   |    |
| <b>Package</b>      | Workgroup, Enterprise and Metro                                                                                                                                                                                                                                                                                                                                                                                                          |          |   |   |                |   |    |          |   |   |                |   |    |
| <b>Defaults</b>     | <table border="0"> <tr> <td>svlan-id</td> <td>-</td> <td>0</td> </tr> <tr> <td>svlan-priority</td> <td>-</td> <td>-1</td> </tr> <tr> <td>cvlan-id</td> <td>-</td> <td>0</td> </tr> <tr> <td>cvlan-priority</td> <td>-</td> <td>-1</td> </tr> </table>                                                                                                                                                                                    | svlan-id | - | 0 | svlan-priority | - | -1 | cvlan-id | - | 0 | cvlan-priority | - | -1 |
| svlan-id            | -                                                                                                                                                                                                                                                                                                                                                                                                                                        | 0        |   |   |                |   |    |          |   |   |                |   |    |
| svlan-priority      | -                                                                                                                                                                                                                                                                                                                                                                                                                                        | -1       |   |   |                |   |    |          |   |   |                |   |    |
| cvlan-id            | -                                                                                                                                                                                                                                                                                                                                                                                                                                        | 0        |   |   |                |   |    |          |   |   |                |   |    |
| cvlan-priority      | -                                                                                                                                                                                                                                                                                                                                                                                                                                        | -1       |   |   |                |   |    |          |   |   |                |   |    |

single-tag | double-tag - Single tag

**Example** `iss(config-ext-nacl)# permit udp any 100.0.0.10 load-balance src-ip`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters

## 65.5.16 deny udp

This command specifies the UDP packets to be rejected based on the associated parameters.

```
deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [ { gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)> } ] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [ { gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-
number (1-65535)> <port-number (1-65535)> } ] [ { tos { max-reliability | max-
throughput | min-delay | normal | <tos-value (0-7)> } | dscp <value (0-63)> } ] [
priority <(1-255)> ]
```

### For Metro

```
deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask> } [ { gt
<port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-
65535)> | range <port-number (1-65535)> <port-number (1-65535)> } ] { any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [ { gt <port-number (1-
65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)> } ] [ { tos { max-reliability | max-
throughput | min-delay | normal | <tos-value (0-7)> } | dscp <value (0-63)> } ] [
priority <short (1-255)> ] [ svlan-id <vlan-id (1-4094)> ] [ svlan-priority
<value (0-7)> ] [ cvlan-id <vlan-id (1-4094)> ] [ cvlan-priority <value (0-7)> ]
[ { single-tag | double-tag } ]
```

|                           |                                                                         |                                                                                                                                                                                                                                                                                                                          |
|---------------------------|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>udp</b>                                                              | - User Datagram Protocol                                                                                                                                                                                                                                                                                                 |
| <b>any   host</b>         | <b>&lt;src-ip-address&gt;   &lt;src-ip-address&gt; &lt;src-mask&gt;</b> | - Source IP address can be <ul style="list-style-type: none"> <li>• 'any' or</li> <li>• the word 'host' and the dotted decimal address or</li> <li>• number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul>                                            |
| <b>port-number</b>        |                                                                         | - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators. <ul style="list-style-type: none"> <li>• eq=equal</li> <li>• lt=less than</li> <li>• gt=greater than</li> <li>• range=a range of ports; two different port numbers must be specified</li> </ul> |
| <b>any   host</b>         |                                                                         | - Destination IP address can be                                                                                                                                                                                                                                                                                          |

|                                  |                                                                                                                                                                                                    |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;dest-ip-address&gt;</b>   | • 'any' or                                                                                                                                                                                         |
| <b>  &lt;dest-ip-address&gt;</b> | • the word 'host' and the dotted decimal address or                                                                                                                                                |
| <b>&lt;dest-mask&gt;</b>         | • number of the network or the host that the packet is destined for and the network mask to use with the destination address                                                                       |
|                                  |                                                                                                                                                                                                    |
| <b>tos</b>                       | - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets. |
|                                  |                                                                                                                                                                                                    |
| <b>priority</b>                  | - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.  |
|                                  |                                                                                                                                                                                                    |
| <b>svlan-id</b>                  | - Service VLAN value to match against incoming packets.                                                                                                                                            |
|                                  |                                                                                                                                                                                                    |
| <b>svlan-priority</b>            | - Service VLAN priority value to match against incoming packets.                                                                                                                                   |
|                                  |                                                                                                                                                                                                    |
| <b>cvlan-id</b>                  | - Customer VLAN value to match against incoming packets.                                                                                                                                           |
|                                  |                                                                                                                                                                                                    |
| <b>cvlan-priority</b>            | - Customer VLAN priority value to match against incoming packets.                                                                                                                                  |
|                                  |                                                                                                                                                                                                    |
| <b>single-tag</b>                | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                              |
|                                  |                                                                                                                                                                                                    |
| <b>double-tag</b>                | - Filter to be applied on double VLAN tagged packets.                                                                                                                                              |
|                                  |                                                                                                                                                                                                    |
| <b>Mode</b>                      | ACL Extended Access List Configuration Mode                                                                                                                                                        |
|                                  |                                                                                                                                                                                                    |
| <b>Package</b>                   | Workgroup, Enterprise and Metro                                                                                                                                                                    |
|                                  |                                                                                                                                                                                                    |
| <b>Defaults</b>                  | svlan-id - 0                                                                                                                                                                                       |
|                                  | svlan-priority - -1                                                                                                                                                                                |
|                                  | cvlan-id - 0                                                                                                                                                                                       |

`cvlan-priority` - -1

`single-tag | double-tag` - Single tag

**Example** `iss(config-ext-nacl)# deny udp host 10.0.0.1 any eq 20`



Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related  
Commands**

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access list configuration
- `permit udp` - Specifies the UDP packets to be forwarded based on the associated parameters

## 65.5.17 permit icmp

This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.

```
permit icmp {any | host <src-ip-address>|<src-ip-address> <mask>}{any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
[<message-code (0-255)>] [ priority <(1-255)>] [redirect {interface <ifXtype>
<ifnum> | <ifXtype><iface_list>[<ifXtype><iface_list>] load-balance {src-ip |
dst-ip | src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport | src-udpport
| dst-udpport}}] [sub-action {none | modify-vlan<short (1-4094)> | nested-
vlan <short (1 -4094)>}]
```

### For Metro

```
permit icmp {any | host <src-ip-address>|<src-ip-address> <mask>} {any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
[<message-code (0-255)>] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-
4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-
priority <value (0-7)>] [ { single-tag | double-tag } ] [redirect {interface
<ifXtype> <ifnum> | <ifXtype><iface_list> [<ifXtype><iface_list>] load-
balance {src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport | dst-
tcpport | src-udpport | dst-udpport}}] [sub-action {none | modify-vlan<short
(1-4094)> | nested-vlan <short (1 -4094)>}]
```

|                           |                                 |                                                                                                                                                                                |
|---------------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>icmp</b>                     | - Internet Control Message Protocol                                                                                                                                            |
|                           | <b>any  host</b>                | - Source IP address can be                                                                                                                                                     |
|                           | <b>&lt;src-ip-address&gt;</b>   | <ul style="list-style-type: none"> <li>• 'any' or</li> </ul>                                                                                                                   |
|                           | <b> &lt;src-ip-address&gt;</b>  | <ul style="list-style-type: none"> <li>• the word 'host' and the dotted decimal address or</li> </ul>                                                                          |
|                           | <b>&lt;mask&gt;</b>             | <ul style="list-style-type: none"> <li>• number of the network or the host that the packet is from and the network mask to use with the source address</li> </ul>              |
|                           | <b>any host</b>                 | - Destination IP address can be                                                                                                                                                |
|                           | <b>&lt;dest-ip-address&gt; </b> | <ul style="list-style-type: none"> <li>• 'any' or</li> </ul>                                                                                                                   |
|                           | <b>&lt;dest-ip-address&gt;</b>  | <ul style="list-style-type: none"> <li>• the word 'host' and the dotted decimal address or</li> </ul>                                                                          |
|                           | <b>&lt;mask&gt;</b>             | <ul style="list-style-type: none"> <li>• number of the network or the host that the packet is destined for and the network mask to use with the destination address</li> </ul> |
|                           | <b>message-type</b>             | - Message type                                                                                                                                                                 |

---

|                       |                                                                                                                                                                                                                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>message-code</b>   | - ICMP Message code                                                                                                                                                                                                                                                                                                      |
| <b>priority</b>       | - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.                                                                                                                        |
| <b>svlan-id</b>       | - Service VLAN value to match against incoming packets.                                                                                                                                                                                                                                                                  |
| <b>svlan-priority</b> | - Service VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                                         |
| <b>cvlan-id</b>       | - Customer VLAN value to match against incoming packets.                                                                                                                                                                                                                                                                 |
| <b>cvlan-priority</b> | - Customer VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                                        |
| <b>single-tag</b>     | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                                                                                                                                                    |
| <b>double-tag</b>     | - Filter to be applied on double VLAN tagged packets.                                                                                                                                                                                                                                                                    |
| <b>Redirect</b>       | - Redirects the action to the destination interface or set of interfaces. <ul style="list-style-type: none"><li>• ifXtype – Specifies the interface type</li><li>• ifnum – Specifies the interface number</li><li>• iface_list – Specifies the list of interfaces</li></ul>                                              |
| <b>load-balance</b>   | - Specifies the parameters based on which the traffic distribution needs to be done. Options are: <ul style="list-style-type: none"><li>• src-ip</li><li>• dst-ip</li><li>• src-mac</li><li>• dst-mac</li><li>• vlanid</li><li>• src-tcpport</li><li>• dst-tcpport</li><li>• src-udpport</li><li>• dst-udpport</li></ul> |

- sub-action**
- Specifies the VLAN specific sub action to be performed on the packet -
    - none – Actions relating to the VLAN ID will not be considered.
    - modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.
    - nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults**

|                           |   |            |
|---------------------------|---|------------|
| message-type/message code | - | 255        |
| svlan-id                  | - | 0          |
| svlan-priority            | - | -1         |
| cvlan-id                  | - | 0          |
| cvlan-priority            | - | -1         |
| single-tag   double-tag   | - | Single tag |

**Example** `iss(config-ext-nacl)# permit icmp any 10.0.0.1 load balance src-ip`



- The ICMP message type can be one of the following:

| Value | ICMP type               |
|-------|-------------------------|
| 0     | Echo reply              |
| 3     | Destination unreachable |
| 4     | Source quench           |
| 5     | Redirect                |
| 8     | Echo request            |
| 11    | Time exceeded           |
| 12    | Parameter problem       |
| 13    | Timestamp request       |

---

|     |                      |
|-----|----------------------|
| 14  | Timestamp reply      |
| 15  | Information request  |
| 16  | Information reply    |
| 17  | Address mask request |
| 18  | Address mask reply   |
| 155 | No ICMP type         |

- The ICMP code can be any of the following:

| - Value | ICMP code                                       |
|---------|-------------------------------------------------|
| - 0     | Network unreachable                             |
| - 1     | Host unreachable                                |
| - 2     | Protocol unreachable                            |
| - 3     | Port unreachable                                |
| - 4     | Fragment need                                   |
| - 5     | Source route fail                               |
| - 6     | Destination network unknown                     |
| - 7     | Destination host unknown                        |
| - 8     | Source host isolated                            |
| - 9     | Destination network administratively prohibited |
| - 10    | Destination host administratively prohibited    |
| - 11    | Network unreachable TOS                         |
| - 12    | Host unreachable TOS                            |
| - 255   | No ICMP code                                    |

- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related  
Commands**

- **ip access-list** - Created IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters

## 65.5.18 deny icmp

This command specifies the ICMP packets to be rejected based on the IP address and associated parameters.

```
deny icmp {any | host <src-ip-address>|<src-ip-address> <mask>}{any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
 [<message-code (0-255)>] [ priority <(1-255)>]
```

### For Metro

```
deny icmp {any | host <src-ip-address>|<src-ip-address> <mask>} {any | host
<dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>]
 [<message-code (0-255)>] [ priority <value (1-255)>] [ svlan-id <vlan-id (1-
4094)>] [svlan-priority <value (0-7)>] [ cvlan-id <vlan-id (1-4094)>] [ cvlan-
priority <value (0-7)>] [ { single-tag | double-tag } ]
```

|                           |                                 |                                                                                                                                                                                                   |
|---------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>icmp</b>                     | - Internet Control Message Protocol                                                                                                                                                               |
|                           | <b>any  host</b>                | - Source IP address can be                                                                                                                                                                        |
|                           | <b>&lt;src-ip-address&gt; </b>  | • 'any' or                                                                                                                                                                                        |
|                           | <b>&lt;src-ip-address&gt;</b>   | • the word 'host' and the dotted decimal address or                                                                                                                                               |
|                           | <b>&lt;mask&gt;</b>             | • number of the network or the host that the packet is from and the network mask to use with the source address                                                                                   |
|                           | <b>any host</b>                 | - Destination IP address can be                                                                                                                                                                   |
|                           | <b>&lt;dest-ip-address&gt; </b> | • 'any' or                                                                                                                                                                                        |
|                           | <b>&lt;dest-ip-address&gt;</b>  | • the word 'host' and the dotted decimal address or                                                                                                                                               |
|                           | <b>&lt;mask&gt;</b>             | • number of the network or the host that the packet is destined for and the network mask to use with the destination address                                                                      |
|                           | <b>message-type</b>             | - Message type                                                                                                                                                                                    |
|                           | <b>message-code</b>             | - ICMP Message code                                                                                                                                                                               |
|                           | <b>priority</b>                 | - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. |

|                       |   |                                                                 |
|-----------------------|---|-----------------------------------------------------------------|
| <b>svlan-id</b>       | - | Service VLAN value to match against incoming packets.           |
| <b>svlan-priority</b> | - | Service VLAN priority value to match against incoming packets.  |
| <b>cvlan-id</b>       | - | Customer VLAN value to match against incoming packets.          |
| <b>cvlan-priority</b> | - | Customer VLAN priority value to match against incoming packets. |
| <b>single-tag</b>     | - | Filter to be applied on Single VLAN tagged packets.             |
| <b>double-tag</b>     | - | Filter to be applied on double VLAN tagged packets.             |

**Mode** ACL Extended Access List Configuration Mode

**Package** Workgroup, Enterprise and Metro

|                 |                               |   |            |
|-----------------|-------------------------------|---|------------|
| <b>Defaults</b> | message-type/<br>message code | - | 255        |
|                 | svlan-id                      | - | 0          |
|                 | svlan-priority                | - | -1         |
|                 | cvlan-id                      | - | 0          |
|                 | cvlan-priority                | - | -1         |
|                 | single-tag   double-tag       | - | Single tag |

**Example**

```
iss(config-ext-nacl)# deny icmp host 100.0.0.10 10.0.0.1
255.255.255.255
```



- The ICMP message type can be one of the following:

| Value | ICMP type               |
|-------|-------------------------|
| 0     | Echo reply              |
| 3     | Destination unreachable |
| 4     | Source quench           |

|     |                      |
|-----|----------------------|
| 5   | Redirect             |
| 8   | Echo request         |
| 11  | Time exceeded        |
| 12  | Parameter problem    |
| 13  | Timestamp request    |
| 14  | Timestamp reply      |
| 15  | Information request  |
| 16  | Information reply    |
| 17  | Address mask request |
| 18  | Address mask reply   |
| 155 | No ICMP type         |

- The ICMP code can be any of the following:

| Value | ICMP code                                       |
|-------|-------------------------------------------------|
| 0     | Network unreachable                             |
| 1     | Host unreachable                                |
| 2     | Protocol unreachable                            |
| 3     | Port unreachable                                |
| 4     | Fragment need                                   |
| 5     | Source route fail                               |
| 6     | Destination network unknown                     |
| 7     | Destination host unknown                        |
| 8     | Source host isolated                            |
| 9     | Destination network administratively prohibited |
| 10    | Destination host administratively prohibited    |
| 11    | Network unreachable TOS                         |
| 12    | Host unreachable TOS                            |
| 255   | No ICMP code                                    |

- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters

## 65.5.19 ip access-group

This command enables access control for the packets on the interface. It controls access to a Layer 2 or Layer 3 interface. The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out.

```
ip access-group <access-list-number (1-65535)> {in | out}
```

```
no ip access-group [<access-list-number (1-65535)>] {in | out}
```

**Syntax Description**      **access-list-number** - IP access control list number

**in** - Inbound packets

**out** - Outbound packets

**Mode**                    Interface Configuration Mode

**Package**                Workgroup, Enterprise and Metro

**Example**                iss(config-if)# ip access-group 1 in



- IP access list must have been created.
- Following are the limitations for this command to be applicable to Layer 2 interfaces.
  1. The out keyword is not supported by Layer 2 interfaces.
  2. An IP ACL applied to a Layer 2 interface filters only the IP packets. MAC access-group interface configuration command with MAC extended ACLs must be used to filter non-IP packets.

**Related Commands**

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **show access-lists** - Displays the access list configuration

## 65.5.20 mac access-group

This command applies a MAC access control list (ACL) to a Layer 2 interface. The no form of this command can be used to remove the MAC ACLs from the interface.

```
mac access-group <access-list-number (1-65535)> in
```

```
no mac access-group [<access-list-number (1-65535)>] in
```

### For Metro

```
mac access-group <access-list-number (1-65535)> {in | out}
```

```
no mac access-group [<access-list-number (1-65535)>] {in | out}
```

|                           |                                                |
|---------------------------|------------------------------------------------|
| <b>Syntax Description</b> | <b>access-list-number</b> - Access List Number |
|                           | <b>in</b> - Inbound packets                    |
|                           | <b>out</b> - Outbound packets                  |

**Mode** Interface Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config-if)# mac access-group 5 in`



MAC access list must have been created.

- Related Commands**
- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
  - **show access-lists** - Displays the access list statistics
  - **Permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
  - **deny** - Specifies the packets to be rejected based on the MAC address and the associated parameters.

## 65.5.21 user-defined access-group

This command applies a user defined access list (ACL) to an interface. The no form of this command removes the User defined ACLs from the interface.

```
user-defined access-group <access-list-number (1-65535)> in
```

```
no user-defined access-group [<access-list-number (1-65535)>] in
```

|                           |                           |   |                               |
|---------------------------|---------------------------|---|-------------------------------|
| <b>Syntax Description</b> | <b>access-list-number</b> | - | IP access control list number |
|                           | <b>in</b>                 | - | Inbound packets               |

**Mode** Interface Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config-if)# user-defined access-group 5 in`



User defined access list should be created already, before executing this command.

- Related Commands**
- `show access-lists` - Displays the access list statistics
  - `user-defined access-list` - Creates the user defined access-list.

## 65.5.22 Permit

This command specifies the packets to be forwarded based on the MAC address and the associated parameters, that is, this command allows non-IP traffic to be forwarded if the conditions are matched.

```
permit { any | host <src-mac-address> } { any | host <dest-mac-address> } [ aarp |
amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 |
lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo
| vines-ip | xns-id | <protocol (0-65535)> ] [ encaps-type <value (1-65535)> ] [
Vlan <vlan-id (1-4094)> ] [ priority <value (1-255)> ] [ redirect { interface
<ifXtype> <ifnum> | <ifXtype><iface_list> [<ifXtype><iface_list>] load-
balance { src-ip | dst-ip | src-mac | dst-mac | vlanid | src-tcpport | dst-
tcpport | src-udpport | dst-udpport } } ] [ sub-action { none | modify-vlan <short
(1-4094)> | nested-vlan <short (1 -4094)> | strip-ether-hdr } } ] [ next-filter-
type { 12 | 13 | user-defined } next-filter-id <short (1-65535)> ]
```

### For Metro

```
permit { any | host <src-mac-address> } { any | host <dest-mac-address> } [
{ aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |
etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios
| vines-echo | vines-ip | xns-id | <short (0-65535)> } ] [ encaps-type <integer
(1-65535)> ] [ vlan <vlan-id (1-4094)> ] [ priority <short (1-255)> ] [
outerEtherType < integer (1-65535)> ] [ svlan-id <vlan-id (1-4094)> ] [ cvlan-
priority <value (0-7)> ] [ svlan-priority <value (0-7)> ] [ { single-tag |
double-tag } ] [ redirect { interface <ifXtype> <ifnum> |
<ifXtype><iface_list> [<ifXtype><iface_list>] load-balance { src-ip | dst-ip |
src-mac | dst-mac | vlanid | src-tcpport | dst-tcpport | src-udpport | dst-
udpport } } ] [ sub-action { none | modify-vlan <short (1-4094)> | nested-vlan
<short (1 -4094)> | strip-ether-hdr } } ] [ next-filter-type { 12 | 13 | user-
defined } next-filter-id <short (1-65535)> ]
```

|                           |                                |                                                                                                      |
|---------------------------|--------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | any   host <src-mac-address >  | - Source MAC address to be matched with the packet                                                   |
|                           | any   host <dest-mac-address > | - Destination MAC address to be matched with the packet                                              |
|                           | aarp                           | - EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address |
|                           | amber                          | - EtherType DEC-Amber                                                                                |
|                           | dec-spanning                   | - EtherType Digital Equipment Corporation (DEC) spanning tree                                        |
|                           | decnet-iv                      | - EtherType DECnet Phase IV protocol                                                                 |

|                       |                                                                                 |
|-----------------------|---------------------------------------------------------------------------------|
| <b>diagnostic</b>     | - EtherType DEC-Diagnostic                                                      |
| <b>dsm</b>            | - EtherType DEC-DSM/DDP                                                         |
| <b>etype-6000</b>     | - EtherType 0x6000                                                              |
| <b>etype-8042</b>     | - EtherType 0x8042                                                              |
| <b>lat</b>            | - EtherType DEC-LAT                                                             |
| <b>lavc-sca</b>       | - EtherType DEC-LAVC-SCA                                                        |
| <b>mop-console</b>    | - EtherType DEC-MOP Remote Console                                              |
| <b>mop-dump</b>       | - EtherType DEC-MOP Dump                                                        |
| <b>msdos</b>          | - EtherType DEC-MSDOS                                                           |
| <b>mumps</b>          | - EtherType DEC-MUMPS                                                           |
| <b>netbios</b>        | - EtherType DEC- Network Basic Input/Output System (NETBIOS)                    |
| <b>vines-echo</b>     | - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems |
| <b>vines-ip</b>       | - EtherType VINES IP                                                            |
| <b>xns-id</b>         | - EtherType Xerox Network Systems (XNS) protocol suite                          |
| <b>encaptype</b>      | - Encapsulation Type                                                            |
| <b>outerEtherType</b> | - EtherType value to match on Service vlan tag                                  |
| <b>svlan-id</b>       | - Service VLAN value to match against incoming packets.                         |

- 
- |                        |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>cvlan-priority</b>  | - Customer VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                                                                                                                                               |
| <b>svlan-priority</b>  | - Service VLAN priority value to match against incoming packets.                                                                                                                                                                                                                                                                                                                                                                |
| <b>single-tag</b>      | - Filter to be applied on Single VLAN tagged packets.                                                                                                                                                                                                                                                                                                                                                                           |
| <b>double-tag</b>      | - Filter to be applied on double VLAN tagged packets.                                                                                                                                                                                                                                                                                                                                                                           |
| <b>redirect</b>        | - Redirects the action to the destination interface or set of interfaces. <ul style="list-style-type: none"><li>• ifXtype – Specifies the interface type</li><li>• ifnum – Specifies the interface number</li><li>• iface_list – Specifies the list of interfaces</li></ul>                                                                                                                                                     |
| <b>load-balance</b>    | - Specifies the parameters based on which the traffic distribution needs to be done. Options are: <ul style="list-style-type: none"><li>• src-ip</li><li>• dst-ip</li><li>• src-mac</li><li>• dst-mac</li><li>• vlanid</li><li>• src-tcpport</li><li>• dst-tcpport</li><li>• src-udpport dst-udpport</li></ul>                                                                                                                  |
| <b>sub-action</b>      | - Specifies the VLAN specific sub action to be performed on the packet - <ul style="list-style-type: none"><li>• none – Actions relating to the VLAN ID will not be considered.</li><li>• modify-vlan – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</li><li>• nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured.</li></ul> |
| <b>strip-ether-hdr</b> | - Strips the outer ethernet header for MPLS packet.                                                                                                                                                                                                                                                                                                                                                                             |

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                     | <b>next-filter-type</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Specifies the type of the next ACL. The types can be                                                                                                                                                                                                          |
|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• <b>12</b> – Configures L2 filter rules in the system.</li> <li>• <b>13</b> – Configures L3 filter rules in the system</li> <li>• <b>user-defined</b> – Configures user defined filter rules in the system</li> </ul> |
|                                                                                     | <b>next-filter-id</b><br><short (1–65535) >]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Specifies the next filter identifier. The value ranges between 1 and 65535.                                                                                                                                                                                   |
| <b>Mode</b>                                                                         | ACL MAC Configuration Mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                               |
| <b>Package</b>                                                                      | Workgroup, Enterprise and Metro                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                               |
| <b>Defaults</b>                                                                     | vlan-id                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | - 0                                                                                                                                                                                                                                                           |
|                                                                                     | priority                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | - 1                                                                                                                                                                                                                                                           |
|                                                                                     | outerEtherType                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | - 0                                                                                                                                                                                                                                                           |
|                                                                                     | svlan-id                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | - 0                                                                                                                                                                                                                                                           |
|                                                                                     | cvlan-priority                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | - -1                                                                                                                                                                                                                                                          |
|                                                                                     | svlan-priority                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | - -1                                                                                                                                                                                                                                                          |
|                                                                                     | single-tag   double-tag                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | - Single tag                                                                                                                                                                                                                                                  |
| <b>Example</b>                                                                      | <pre>iss(config-ext-macl)# permit host 00:11:22:33:44:55 any load- balance src-ip sub-action modify lan 526</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                               |
|  | <ul style="list-style-type: none"> <li>• MAC access list must have been created.</li> <li>• OuterEtherType, Service Vlan, Service Vlan Priority and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.</li> </ul>                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                               |
| <b>Related Commands</b>                                                             | <ul style="list-style-type: none"> <li>• <b>mac access-list extended</b> - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user</li> <li>• <b>mac access-group</b> - Applies a MAC access control list (ACL) to a Layer 2 interface</li> <li>• <b>deny</b> - Specifies the packets to be rejected based on the MAC address and the associated parameters</li> <li>• <b>show access-lists</b> - Displays the access list statistics</li> <li>• <b>user-defined access-list</b> - Creates user defined access-list</li> </ul> |                                                                                                                                                                                                                                                               |

## 65.5.23 deny

This command specifies the packets to be rejected based on the MAC address and the associated parameters.

```
deny { any | host <src-mac-address> } { any | host <dest-mac-address> } [ aarp |
amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 |
lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo
| vines-ip | xns-id | <protocol (0-65535)> ] [ encapsype <value (1-65535)> ] [
Vlan <vlan-id (1-4094)> ] [ priority <value (1-255)> ]
```

### For Metro

```
deny { any | host <src-mac-address> } { any | host <dest-mac-address> } [ {
aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |
etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios
| vines-echo | vines-ip | xns-id | <short (0-65535)> } ] [ encapsype <integer
(1-65535)> ] [ vlan <vlan-id (1-4094)> ] [ priority <short (1-255)> ] [
outerEtherType < integer (1-65535)> ] [ svlan-id <vlan-id (1-4094)> ] [ cvlan-
priority <priority (0-7)> ] [ svlan-priority <value (0-7)> ] [ { single-tag |
double-tag } ]
```

|                           |                                             |                                                                                                      |
|---------------------------|---------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>any   host &lt;src-mac-address &gt;</b>  | - Source MAC address to be matched with the packet                                                   |
|                           | <b>any   host &lt;dest-mac-address &gt;</b> | - Destination MAC address to be matched with the packet                                              |
|                           | <b>aarp</b>                                 | - EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address |
|                           | <b>amber</b>                                | - EtherType DEC-Amber                                                                                |
|                           | <b>dec-spanning</b>                         | - EtherType Digital Equipment Corporation (DEC) spanning tree                                        |
|                           | <b>decent-iv</b>                            | - EtherType DECnet Phase IV protocol                                                                 |
|                           | <b>diagnostic</b>                           | - EtherType DEC-Diagnostic                                                                           |
|                           | <b>dsm</b>                                  | - EtherType DEC-DSM/DDP                                                                              |

|                       |                                                                                                                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>etype-6000</b>     | - EtherType 0x6000                                                                                                                                                                                      |
| <b>etype-8042</b>     | - EtherType 0x8042                                                                                                                                                                                      |
| <b>lat</b>            | - EtherType DEC-LAT                                                                                                                                                                                     |
| <b>lavc-sca</b>       | - EtherType DEC-LAVC-SCA                                                                                                                                                                                |
| <b>mop-console</b>    | - EtherType DEC-MOP Remote Console                                                                                                                                                                      |
| <b>mop-dump</b>       | - EtherType DEC-MOP Dump                                                                                                                                                                                |
| <b>msdos</b>          | - EtherType DEC-MSDOS                                                                                                                                                                                   |
| <b>mumps</b>          | - EtherType DEC-MUMPS                                                                                                                                                                                   |
| <b>netbios</b>        | - EtherType DEC- Network Basic Input/Output System (NETBIOS)                                                                                                                                            |
| <b>vines-echo</b>     | - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems                                                                                                                         |
| <b>vines-ip</b>       | - EtherType VINES IP                                                                                                                                                                                    |
| <b>xns-id</b>         | - EtherType Xerox Network Systems (XNS) protocol suite                                                                                                                                                  |
| <b>encaptype</b>      | - Encapsulation Type                                                                                                                                                                                    |
| <b>vlan</b>           | - VLAN ID to be filtered                                                                                                                                                                                |
| <b>priority</b>       | - The priority of the L2 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority. |
| <b>outerEtherType</b> | - EtherType value to match on Service vlan tag                                                                                                                                                          |
| <b>svlan-id</b>       | - Service VLAN value to match against incoming packets.                                                                                                                                                 |

- cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- svlan-priority** - Service VLAN priority value to match against incoming packets.
- single-tag** - Filter to be applied on Single VLAN tagged packets.
- double-tag** - Filter to be applied on double VLAN tagged packets.

**Mode** ACL MAC Configuration Mode

**Package** Workgroup, Enterprise and Metro

- Defaults**
- vlan-id - 0
  - priority - 1
  - outerEtherType - 0
  - svlan-id - 0
  - cvlan-priority - -1
  - svlan-priority - -1
  - single-tag | double-tag - Single tag

**Example** `iss(config-ext-macl)# deny any host 00:11:22:33:44:55 priority 200`



- MAC access list must have been created.
- OuterEtherType, Service Vlan, Service Vlan Priority and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

**Related Commands**

- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **Permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **show access-lists** - Displays the access list statistics
- **user-defined access-list** - Creates user defined access-list.

## 65.5.24 show access-lists

This command displays the access lists configuration.

```
show access-lists [{ip | mac | user-defined }] < access-list-number (1-65535)> ]
```

|                           |                     |                            |
|---------------------------|---------------------|----------------------------|
| <b>Syntax Description</b> | <b>ip</b>           | - IP Access List           |
|                           | <b>mac</b>          | - MAC Access List          |
|                           | <b>user-defined</b> | - user defined access list |

**Mode** Privileged/User EXEC Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show access-lists

```
IP ACCESS LISTS
```

```
-----
```

```
Standard IP Access List 1
```

```
-----
```

```
Filter Priority           : 1
IP address Type          : IPV4
Source IP address        : 0.0.0.0
Source IP address mask   : 0.0.0.0
Source IP Prefix Length  : 0
Destination IP address   : 0.0.0.0
Destination IP address mask : 0.0.0.0
Destination IP Prefix Length : 0
Flow Identifier          : 0
In Port List             : NIL
Out Port List            : NIL
Filter Action            : Permit
Redirect Port List       : NIL
TrafficDistField         : Unknown
Sub Action               : NONE
Sub Action Id            : 0
```

---

```
Status                               : InActive

Extended IP Access List 1001
-----

Filter Priority                       : 1
Filter Protocol Type                 : ANY
IP address Type                      : IPV4
Source IP address                    : 0.0.0.0
Source IP address mask               : 0.0.0.0
Source IP Prefix Length              : 0
Destination IP address               : 0.0.0.0
Destination IP address mask          : 0.0.0.0
Destination IP Prefix Length         : 0
Flow Identifier                      : 0
In Port List                         : NIL
Out Port List                        : NIL
Filter TOS                           : Invalid combination
Filter DSCP                          : NIL
Filter Action                        : Permit
Redirect Port List                   : NIL
TrafficDistField                     : Unknown
Sub Action                           : NONE
Sub Action Id                        : 0
Status                               : InActive
```

#### MAC ACCESS LISTS

```
-----

Extended MAC Access List 1
-----

Filter Priority                       : 1
Ether Type                           : 0
Protocol Type                        : 0
Vlan Id                              : 0
Destination MAC Address               : 00:00:00:00:00:00
```

```

Source MAC Address           : 00:00:00:00:00:00
In Port List                 : NIL
Filter Action                : Permit
Redirect Port List          : NIL
TrafficDistField            : Unknown
Sub Action                   : NONE
Sub Action Id                : 0
Status                       : InActive

```

#### USER DEFINED LISTS

##### -----

##### User Defined Access List 1

##### -----

```

Priority                     : 1
Packet Type                  : User-Defined
Offset Base                  : L2
OffSet Position              :
OffSet Value                  :
Filter Action                 : Permit
In Port List                 : NIL
Filter One Type               : None
Filter Id                    : 0
Filter Two Type               : None
Filter Id                    : 0
Redirect Port List           : NIL
TrafficDistField             : Unknown
Sub Action                   : NONE
Sub Action Id                : 0
Status                       : InActive

```



- OuterEtherType, Service Vlan, Service Vlan Priority, innerEtherType, Customer Vlan and Customer Vlan Priority options are applicable only with Metro Ethernet Feature and bridge mode is provider.

#### Related Commands

- **ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode
- **mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- **permit usr-defined-packet-type** - Permits Packet Based on User Defined

### Packet Byte

- **deny usr-defined-packet-type** - This command denies packet based on user defined byte.
- **permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters
- **deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched
- **permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- **deny - ip/ospf/pim/protocol type** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- **permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters
- **deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters
- **permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters
- **deny udp** - Specifies the UDP packets to be rejected based on the associated parameters
- **permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- **deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- **ip access-group** - Enables access control for the packets on the interface
- **mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface
- **Permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- **deny** - specifies the packets to be rejected based on the MAC address and the associated parameters
- **user-defined access-list** - Creates user defined access-list.
- **userdefined-list** - Creates a user defined access list by applying AND, OR, NOT operation on existing ACL rules
- **permit ipv6** - Specifies IP packets to be forwarded based on protocol and associated parameters.
- **deny ipv6** - Specifies IPv6 packets to be rejected based on protocol and associated parameters.
- **user-defined access-group** - Applies a user defined access list (ACL) to an interface

# Chapter

# 66

## DiffServ

---

DiffServ (Differentiated Services) is an architecture for providing different types or levels of service for network traffic. One key characteristic of Diffserv is that flows are aggregated in the network, so that core routers only need to distinguish a comparably small number of aggregated flows, even if those flows contain thousands or millions of individual flows.

Differentiated services are intended to provide a framework and building blocks to enable deployment of scalable service discrimination in the Internet. The differentiated services approach aims to speed deployment by separating the architecture into two major components, one of which is fairly well-understood and the other of which is just beginning to be understood. In this, we are guided by the original design of the Internet where the decision was made to separate the forwarding and routing components. Packet forwarding is the relatively simple task that needs to be performed on a per-packet basis as quickly as possible. Forwarding uses the packet header to find an entry in a routing table that determines the packet's output interface. Routing sets the entries in that table and may need to reflect a range of transit and other policies as well as to keep track of route failures. Routing tables are maintained as a background process to the forwarding task.

## 66.1 BCM Specific Commands

This section describes the CLI commands executable only in BCM target for configuring DiffServ feature supported by ISS.

The list of CLI commands for the configuration of DiffServ is as follows:

- set qos
- class-map
- policy-map
- match
- class
- set cos
- police
- shutdown qos
- cosq scheduling algorithm
- traffic class
- show policy-map
- show class-map
- show cosq algorithm
- show cosq weights-bw

## 66.1.1 set qos

This command enables differentiated services on the device. The disable option is used to disable the QoS feature on the device.

```
set qos { enable | disable }
```

**Syntax Description**

|               |                                   |
|---------------|-----------------------------------|
| <b>enable</b> | - Enables differentiated services |
|---------------|-----------------------------------|

|                |                                    |
|----------------|------------------------------------|
| <b>disable</b> | - Disables differentiated services |
|----------------|------------------------------------|

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** disable

**Example** iss(config)# set qos enable



- QoS must be globally enabled prior to the execution of the class-map and policy-map mode commands.
- When set as 'enabled', DiffServ Module programs the hardware and starts Protocol Operation.
- When set as 'disabled', it stops protocol operation by deleting the hardware configuration.

**Related Commands**

- **show policy-map** - Displays the quality of service (QoS) policy maps
- **show class-map** - Displays quality of service (QoS) class maps

## 66.1.2 class-map

This command creates a class map that is meant to be used for matching the packets to the class whose index is specified. This command is also used to enter the class-map configuration mode. The no form of this command is used to delete an existing class map and to return to global configuration mode.

```
class-map <class-map-number (1-65535) >
```

```
no class-map <class-map-number (1-65535) >
```

**Syntax Description**      **class-map-number**      -      QoS class map number

**Mode**                      Global Configuration Mode

**Package**                  Workgroup, Enterprise and Metro

**Example**                  `iss(config)# class-map 5`



- Differentiated services must have been enabled in the device.
- The class-map command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-interface basis.
- The **match** command is available from the class-map configuration mode.

**Related Command**      **show class-map** - Displays quality of service (QoS) class maps

## 66.1.3 policy-map

This command is used to enter the policy-map configuration mode. In the policy-map configuration mode the user can create or modify a policy map. The no form of this command deletes an existing policy map and returns to the global configuration mode.

```
policy-map <policy-map-number (1-65535)>
```

```
no policy-map <policy-map-number (1-65535)>
```

**Syntax**            **policy-map-number** - QoS Policy map number  
**Description**

**Mode**             Global Configuration Mode

**Package**          Workgroup, Enterprise and Metro

**Example**          iss(config)# policy-map 6



- Differentiated services must have been enabled in the device.
- The following two commands are available from the policy-map configuration mode:
  - **class**
  - **exit** - Exits from the policy map configuration mode and returns to the global configuration mode.

**Related Command**    **show policy-map** - Displays quality of service (QoS) policy maps

## 66.1.4 match

This command specifies the fields in the incoming packets that are to be examined for the classification of the packets. The IP access group / MAC access group can be used as match criteria.

```
match access-group { mac-access-list | ip-access-list } <acl-index-num (1-65535) >
```

|                           |                        |                                                                                                                                                                                                 |
|---------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>mac-access-list</b> | - Access list created based on MAC addresses for non-IP traffic                                                                                                                                 |
|                           | <b>ip-access-list</b>  | - Access list created based on IP addresses. The IP-access list can either be defined as a standard IP-access list or an extended IP-access list.                                               |
|                           | <b>acl-index-num</b>   | - Specifies the ACL index range. The ACL index range for an IP standard ACL is 1 to 1000 and IP extended ACL is 1001 to 65535.<br><br>The ACL index range for a MAC extended ACL is 1 to 65535. |

**Mode** Class Map Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss (config-cmap)# match access-group mac-access-list 5`



- Differentiated services must have been enabled in the device.
- MAC access list and IP access list must have been configured.

**Related Commands**

- **class-map** - Creates a class map to be used for matching the packets with the class whose name/index is specified
- **show class-map** - Displays QoS Class maps

## 66.1.5 class

This command defines a traffic classification for the policy to act. The class-map-number that is specified in the policy map ties the characteristics for that class to the class map and its match criteria, as configured by using the class-map global configuration command. On execution of the class command, the switch enters the policy-map class configuration mode.

The no form of this command un-maps the class-map from the current policy-map configuration.

```
class <class-map-number (1-65535)>
```

```
no class <class-map-number (1-65535)>
```

|                           |                                            |
|---------------------------|--------------------------------------------|
| <b>Syntax Description</b> | <b>class-map-number</b> - Class Map Number |
|---------------------------|--------------------------------------------|

|             |                               |
|-------------|-------------------------------|
| <b>Mode</b> | Policy-Map Configuration Mode |
|-------------|-------------------------------|

|                |                                 |
|----------------|---------------------------------|
| <b>Package</b> | Workgroup, Enterprise and Metro |
|----------------|---------------------------------|

|                |                            |
|----------------|----------------------------|
| <b>Example</b> | iss (config-pmap)# class 5 |
|----------------|----------------------------|



- Differentiated services must have been enabled in the device.
- The policy-map global configuration command must be executed prior to using the class command. After a policy map is specified, the user can either configure a policy for new classes or modify a policy for any existing classes in that policy map.
- The following configuration commands are available from the policy map class configuration mode:
  - **set cos**
  - **police**

|                         |                                                                                                                                                                                   |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Related Commands</b> | <ul style="list-style-type: none"> <li>• <b>policy-map</b> - Enters the policy map configuration mode</li> <li>• <b>show policy-map</b> - Displays the QoS policy maps</li> </ul> |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 66.1.6 set cos

This command defines the in-profile action by setting a class of service (CoS), Differentiated Services Code Point (DSCP), or IP-precedence value in the packet.

The no form of the command deletes the configured values.

```
set {cos <new-cos(0-7)> | ip dscp <new-dscp(0-63)> | ip precedence <new-
precedence(0-7)>}
```

```
no set {cos <new-cos(0-7)> | ip { dscp <new-dscp(0-63)> | precedence <new-
precedence(0-7)>}}
```

|                           |                      |                                                              |
|---------------------------|----------------------|--------------------------------------------------------------|
| <b>Syntax Description</b> | <b>cos</b>           | - New COS value assigned to the classified traffic           |
|                           | <b>ip dscp</b>       | - New DSCP value assigned to the classified traffic          |
|                           | <b>ip precedence</b> | - New IP-precedence value assigned to the classified traffic |

**Mode** Policy-Map Class Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss (config-pmap-c)# set cos 5`



To attach policy maps that contain the following elements to an ingress interface

- set policy-map class configuration commands must be used. Moreover, the police policy-map class configuration command can be used to mark down (reduce) the DSCP value at the ingress interface.
- Access control list (ACL) classification.
- Per-port per-VLAN classification.

- Related Commands**
- **class** - Defines a traffic classification for the policy set
  - **policy-map** - Used to enter the policy map configuration mode
  - **class-map** - Creates a class map
  - **show policy-map** - Displays the QoS policy map configuration

## 66.1.7 police

This command defines a policer for the classified traffic. This command also specifies the action to be taken if the specified rate is exceeded or if there is no match for the policy configured.

```
police <rate-Mbps(1-1023)> exceed-action {drop | policed-dscp-transmit <new-dscp(0-63)>}
```

|                           |                              |                                                                                                                                                                                                                                                                                       |
|---------------------------|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>rate-Mbps<sup>2</sup></b> | - Average traffic rate in mega bits per second (Mbps)                                                                                                                                                                                                                                 |
|                           | <b>exceed-action</b>         | - Indicates the action of the switch when the specified rate is exceeded.<br><b>drop</b> - drops the packet<br><b>policed-dscp-transmit</b> - changes the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then sends the packet |

**Mode** Policy-Map Class Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss (config-pmap-c)# police 128 exceed-action drop`



Although the command-line help string displays a large range of values, the rate Mbps option cannot exceed the configured port speed. If a larger value is entered, then the switch rejects the policy map when attached to an interface.

- Related Commands**
- **class** - Defines a traffic classification for the policy to act
  - **policy-map** - Used to enter the policy map configuration mode
  - **class-map** - Creates a class map used for matching packets
  - **show policy-map** - Displays the QoS policy maps

<sup>2</sup> The range of values for the average traffic rate (defined in Mbps units) specified in this command is specific for Broadcom 5690 target.

For a Chassis board target and other Broadcom targets, such as, BCM 5695 and Firebolt, the average traffic rate ranges between 64 and 1048572 and is defined in Kbps.

## 66.1.8 shutdown qos

This command shuts down the Quality-of-Service operation. The no form of the command starts and enables the Quality-of-Service operation.

**shutdown qos**

**no shutdown qos**

|                 |                                        |
|-----------------|----------------------------------------|
| <b>Mode</b>     | Global Configuration Mode              |
| <b>Package</b>  | Workgroup, Enterprise and Metro        |
| <b>Defaults</b> | QoS is started and enabled by default  |
| <b>Example</b>  | <code>iss(config)# shutdown qos</code> |



- When shutdown, all the pools used by DiffServ module will be released to the system.
- When started, the resources required by DiffServ module are allocated and the module starts running.

|                         |                                                                                                                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Related Commands</b> | <ul style="list-style-type: none"> <li>• <b>show policy-map</b> - Displays the quality of service (QoS) policy maps</li> <li>• <b>show class-map</b> - Displays quality of service (QoS) class maps</li> </ul> |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 66.1.9 cosq scheduling algorithm

This command sets cosq scheduling algorithm.

```
cosq scheduling algorithm { strict | rr | wrr | wfq | strict-rr | strict-wrr |
strict-wfq | deficit }
```

|                           |                   |                                 |
|---------------------------|-------------------|---------------------------------|
| <b>Syntax Description</b> | <b>strict</b>     | - strict                        |
|                           | <b>rr</b>         | - round robin                   |
|                           | <b>wrr</b>        | - weighted round robin          |
|                           | <b>wfq</b>        | - weighted fair queing          |
|                           | <b>strict-rr</b>  | - strict - round robin          |
|                           | <b>strict-wrr</b> | - strict - weighted round robin |
|                           | <b>strict-wfq</b> | - strict - weighted fair queing |
|                           | <b>deficit</b>    | - deficit                       |

**Mode** Interface Configuration mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config-if)# cosq scheduling algorithm strict`

- Related Commands**
- `show cosq algorithm` - Displays the CoSq algorithm used for the interface.
  - `show cosq weights-bw` - Ddisplays the CoSq weights and the bandwidth for the interface.

## 66.1.10 traffic class

This command sets weight and bandwidth for traffic classes.

```
traffic-class <integer(0-7)> weight <integer(0-15)> [ minbandwidth <integer(1-262143)>]
```

|                           |                      |   |                              |
|---------------------------|----------------------|---|------------------------------|
| <b>Syntax Description</b> | <b>traffic-class</b> | - | Configures cosq numbers      |
|                           | <b>weight</b>        | - | Configures cosq weights      |
|                           | <b>minbandwidth</b>  | - | Configures minimum bandwidth |

**Mode** Interface Configuration mode

**Package** Workgroup, Enterprise and Metro

**Defaults** weight - 1

**Example** iss(config-if)# traffic-class 1 weight 7 minbandwidth 1234

**Related Commands**

- **show cosq algorithm** - Displays the CoSq algorithm used for the interface.
- **show cosq weights-bw** - Displays the CoSq weights and the bandwidth for the interface.

## 66.1.11 show policy-map

This command displays the quality of service (QoS) policy maps, which defines the classification criteria for the incoming traffic. Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

```
show policy-map [<policy-map-num(1-65535)> [class <class-map-num(1-65535)>]]
```

**Syntax Description**

**policy-map-num** - Policy map number

**class** - Class map number

**Mode** Privileged/User EXEC Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show policy-map 24

```
DiffServ Configurations:
```

```
-----
```

```
Quality of Service has been enabled
```

```
Policy Map 24 is not active
```

```
Class Map: 20
```

```
-----
```

```
Protocol                               : 255
```

```
In Profile Entry
```

```
-----
```

```
In profile action                       : policed-precedence 5
```

```
Out Profile Entry
```

```
-----
```

```
Metering on
```

```
burst bytes/token size                 : 6
```

```
Refresh count                           : 1000
```

```
Out profile action                       : drop
```

```
No Match Entry
```

```
-----
```

```
No match action                         : policed-precedence 5
```

**Related Commands**

- **policy-map** - Used to enter the policy map configuration mode

- **class** - Defines a traffic classification for the policy to act
- **set cos** - Defines the in-profile action by setting a CoS, DSCP or IP-precedence value in the packet
- **police** - Defines a policer for the classified traffic



## 66.1.13 show cosq algorithm

This command displays the CoSq algorithm used for the interface.

```
show cosq algorithm [ interface <interface-type> <interface-id> ]
```

**Syntax Description**     **interface-type**     -   Interface Type

**interface-id**         -   Interface ID

**Mode**                     Global Configuration Mode

**Package**                 Workgroup, Enterprise and Metro

**Example**                 iss(config)# show cosq algorithm interface gigabitethernet  
0/1

```
CoSq Algorithm
```

```
-----
Interface            Algorithm
-----
Gi0/1                StrictPriority
.....
-----
```

## 66.1.14 show cosq weights-bw

This command displays the CoSq weights and the bandwidth for the interface.

```
show cosq weights-bw [ interface <interface-type> <interface-id> ]
```

**Syntax Description** **interface-type** - Interface Type

**interface-id** - Interface ID

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss(config)# show cosq weights-bw interface gigabitethernet 0/1

CoSq Weights and Bandwidths

```
-----
Interface  CoSqId  CoSqWeight  MinBw  MaxBw  Flag
-----  -
Gi0/1      0        1           0      0      2
Gi0/1      1        1           0      0      2
Gi0/1      2        1           0      0      2
Gi0/1      3        1           0      0      2
Gi0/1      4        1           0      0      2
Gi0/1      5        1           0      0      2
Gi0/1      6        1           0      0      2
Gi0/1      7        1           0      0      2
.....    ...      ..          ...    ...    ...
-----
```

## 66.2 CXE Specific Commands

This section describes the CLI commands executable only in CXE target for configuring DiffServ feature supported by ISS.

The list of CLI commands for the configuration of DiffServ is as follows:

- set qos
- class-map
- policy-map
- qos traffic-class
- qos random-detect
- qos map dscp-queue
- qos queue-precedence switched
- qos queue-precedence routed
- match
- class
- set cos
- set qos traffic-class
- bandwidth
- min-reserved-bandwidth
- queue-threshold
- set random-detect
- fair-queue
- weight
- qos bandwidth
- qos queue threshold
- qos set random-detect
- shutdown qos
- show policy-map
- show class-map
- show qos maps dscp-queue
- show qos maps trafficclass-fairqueue map
- show qos queue precedence
- show qos traffic-class
- show qos random-detect
- show qos interface

- show qos statistics

## 66.2.1 set qos

This command enables differentiated services on the device. The disable option is used to disable the QoS feature on the device.

```
set qos { enable | disable }
```

**Syntax Description**

|               |                                   |
|---------------|-----------------------------------|
| <b>enable</b> | - Enables differentiated services |
|---------------|-----------------------------------|

|                |                                    |
|----------------|------------------------------------|
| <b>disable</b> | - Disables differentiated services |
|----------------|------------------------------------|

**Mode** Global Configuration Mode

**Defaults** disable

**Example** iss(config)# set qos enable



- QoS must be globally enabled prior to the execution of all the commands in this section.
- When set as 'enabled', DiffServ Module programs the hardware and starts Protocol Operation.
- When set as 'disabled', it stops protocol operation by deleting the hardware configuration.

**Related Command**

- **show policy-map** - Displays the quality of service (QoS) policy maps
- **show class-map** - Displays quality of service (QoS) class maps

## 66.2.2 class-map

This command creates a class map that is meant to be used for matching the packets to the class whose index is specified. This command is also used to enter the class-map configuration mode. The no form of this command is used to delete an existing class map and to return to global configuration mode.

```
class-map <class-map-number (1-65535) >
```

```
no class-map <class-map-number (1-65535) >
```

**Mode** Global Configuration Mode

**Example** `iss(config)# class-map 5`



- Differentiated services must have been enabled in the device.
- The class-map command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-interface basis.
- The **match** command is available from the class-map configuration mode.

**Related Command** `show class-map` - Displays quality of service (QoS) class maps

## 66.2.3 policy-map

This command is used to enter the policy-map configuration mode. In the policy-map configuration mode the user can create or modify a policy map . The no form of this command deletes an existing policy map and returns to the global configuration mode.

```
policy-map <policy-map-number (1-65535) >
```

```
no policy-map <policy-map-number (1-65535) >
```

**Mode** Global Configuration Mode

**Example** `iss(config)# policy-map 6`



- Differentiated services must have been enabled in the device.
- The following two commands are available from the policy-map configuration mode:
  1. class
  2. exit - Exits from the policy map configuration mode and returns to the global configuration mode.

**Related Command** `show policy-map` - Displays quality of service (QoS) policy maps

## 66.2.4 qos traffic-class

This command creates a traffic class and selects its output port. The no form of the command deletes the traffic class and as a result all configurations are lost.

```
qos traffic-class <traffic-class-id(1-1023)> [map <output-port-type> <output-port-number>]
```

```
no qos traffic-class <traffic-class-id(1-1023)>
```

|                           |            |                                                                         |
|---------------------------|------------|-------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>map</b> | - Selects output port type and output port number for the traffic class |
|---------------------------|------------|-------------------------------------------------------------------------|

|             |                           |
|-------------|---------------------------|
| <b>Mode</b> | Global Configuration Mode |
|-------------|---------------------------|

|                |                                                           |
|----------------|-----------------------------------------------------------|
| <b>Example</b> | iss(config)# qos traffic-class 10 map gigabitethernet 0/1 |
|----------------|-----------------------------------------------------------|



- If the traffic class has already been created, then this command is used to enter in to the traffic-class configuration mode.
- The map option cannot be specified for an existing traffic class.

|                        |                                                                        |
|------------------------|------------------------------------------------------------------------|
| <b>Related Command</b> | <b>show qos traffic-class</b> - Displays the traffic class information |
|------------------------|------------------------------------------------------------------------|

## 66.2.5 qos random-detect

This command configures the RED (Random Early Detection) parameters. The no form of the command deletes the RED curve wherein all configurations are lost.

```
qos random-detect <RED Curve ID(1-126)> start <curve-start 16KB-units(0-16383)> stop <curve-stop 16KB-units(0-16383)> qrange <nearest-difference-between-start-and-stop log2-units(14-28)> stop-probability <drop-probability-at-Start+Qrange(0-200)>
```

```
no qos random-detect curve-id <RED Curve ID(1-126)>
```

|                           |                         |                                                                                                       |
|---------------------------|-------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>start</b>            | - Specifies the RED curve start                                                                       |
|                           | <b>stop</b>             | - Specifies the RED curve stop                                                                        |
|                           | <b>qrange</b>           | - Difference between start and stop rounded up to the nearest power of 2 (represented in log 2 units) |
|                           | <b>stop-probability</b> | - Specifies the sum of the drop probability at the start and qrange                                   |

**Mode** Global Configuration Mode

**Example**

```
iss(config)# qos random-detect 10 start 19 stop 36 qrange 19 stop-probability 200
```

**Related Command** `show qos random-detect` – Displays RED curve information

## 66.2.6 qos map dscp-queue

This command maps the given DSCP value to an egress queue.

```
qos map dscp-queue <DSCP (0-63)> to <queue (0-7)>
```

**Syntax Description**      `to`                              - Maps the DSCP value to the Egress Queue value

**Mode**                      Global Configuration Mode

**Defaults**                The following are the Default Queue values for the DSCP ranges.

| DSCP range | Queue Value |
|------------|-------------|
| -----      | -----       |
| 0 - 7      | Queue 0     |
| 8 - 15     | Queue 1     |
| 16 – 23    | Queue 2     |
| 24 – 31    | Queue 3     |
| 32 – 39    | Queue 4     |
| 40-47      | Queue 5     |
| 48-55      | Queue 6     |
| 56 –63     | Queue 7     |

**Example**                `iss(config)# qos map dscp-queue 20 to 7`

**Related Command**      `show qos maps dscp-queue` – Displays the DSCP to queue mapping information

## 66.2.7 qos queue-precedence switched

This command sets the queue precedence of DSCP, L2 COS for switched packets.

```
qos queue-precedence switched {[dscp <short (0-6)>] [cos <short (0-6)>]}
```

|                           |                                                                                                    |   |                                                     |
|---------------------------|----------------------------------------------------------------------------------------------------|---|-----------------------------------------------------|
| <b>Syntax Description</b> | <b>dscp</b>                                                                                        | - | DSCP value for which the precedence needs to be set |
|                           | <b>cos</b>                                                                                         | - | CoS value for which the precedence needs to be set  |
| <b>Mode</b>               | Global Configuration Mode                                                                          |   |                                                     |
| <b>Default</b>            | DSCP                                                                                               | 5 |                                                     |
|                           | COS                                                                                                | 6 |                                                     |
| <b>Example</b>            | iss(config)# qos queue-precedence switched dscp 2 cos 5                                            |   |                                                     |
| <b>Related Command</b>    | <b>show qos queue precedence</b> – Displays the queue precedence of the DSCP and the L2 COS values |   |                                                     |

## 66.2.8 qos queue-precedence routed

This command sets the queue precedence of DSCP, L2 COS for routed packets.

```
qos queue-precedence routed {[dscp <short (0-6)>] [cos <short (0-6)>]}
```

|                           |                           |                                                       |
|---------------------------|---------------------------|-------------------------------------------------------|
| <b>Syntax Description</b> | <b>dscp</b>               | - DSCP value for which the precedence needs to be set |
|                           | <b>cos</b>                | - CoS value for which the precedence needs to be set  |
| <b>Mode</b>               | Global Configuration Mode |                                                       |
| <b>Default</b>            | DSCP                      | 6                                                     |
|                           | CoS                       | 5                                                     |

**Example**      `iss(config)# qos queue-precedence routed dscp 1 cos 3`



Higher precedence for DSCP indicates that the egress queue will be selected based on the actual DSCP value.

**Related Command**      `show qos queue precedence` – Displays the queue precedence of the DSCP and the L2 COS values

## 66.2.9 match

This command specifies the fields in the incoming packets that are to be examined for the classification of the packets. The IP access group / MAC access group can be used as match-criteria.

```
match access-group { mac-access-list | ip-access-list } <acl-index-num (1-65535) >
```

|                           |                        |                                                                                                                                                                                                 |
|---------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>mac-access-list</b> | - Access list created based on MAC addresses for non-IP traffic                                                                                                                                 |
|                           | <b>ip-access-list</b>  | - Access list created based on IP addresses. The IP-access list can either be defined as a standard IP-access list or an extended IP-access list.                                               |
|                           | <b>acl-index-num</b>   | - Specifies the ACL index range. The ACL index range for an IP standard ACL is 1 to 1000 and IP extended ACL is 1001 to 65535.<br><br>The ACL index range for a MAC extended ACL is 1 to 65535. |

**Mode** Class Map Configuration Mode

**Example** `iss (config-cmap)# match access-group mac-access-list 5`



- Differentiated services must have been enabled in the device.
- MAC access list and IP access list must have been configured.

- Related Command**
- **class-map** - Creates a class map to be used for matching the packets with the class whose name/index is specified
  - **show class-map** - Displays QoS Class maps

## 66.2.10 class

This command defines a traffic classification for the policy to act. The class-map-num that is specified in the policy map ties the characteristics for that class to the class map and its match criteria as configured by using the class-map global configuration command. On execution of the class command, the switch enters the policy-map class configuration mode.

The no form of this command un-maps the class-map from the current policy-map configuration.

```
class <class-map-number (1-65535) >
```

```
no class <class-map-number (1-65535) >
```

**Mode** Policy-Map Configuration Mode

**Example** `iss (config-pmap)# class 5`



- Differentiated services must have been enabled in the device.
- The policy-map global configuration command must be executed prior to using the class command. After a policy map is specified, the user can either configure a policy for new classes or modify a policy for any of the existing classes in that policy map.
- The following configuration commands are available from the policy map class configuration mode:

```
set cos
```

- Related Command**
- `policy-map` - Enters the policy map configuration mode
  - `show policy-map` - Displays the QoS policy maps

## 66.2.11 set cos

This command defines the in-profile action by setting a class of service (CoS), Differentiated Services Code Point (DSCP), or IP-precedence value in the packet.

The no form of the command deletes the configured values.

```
set {cos <new-cos(0-7)> | ip dscp <new-dscp(0-63)> | ip precedence <new-
precedence(0-7)>}
```

```
no set {cos <new-cos(0-7)> | ip { dscp <new-dscp(0-63)> | precedence <new-
precedence(0-7)>}}
```

|                           |                      |   |                                                            |
|---------------------------|----------------------|---|------------------------------------------------------------|
| <b>Syntax Description</b> | <b>cos</b>           | - | New COS value assigned to the classified traffic           |
|                           | <b>ip dscp</b>       | - | New DSCP value assigned to the classified traffic          |
|                           | <b>ip precedence</b> | - | New IP-precedence value assigned to the classified traffic |

**Mode** Policy-Map Class Configuration Mode

**Example** `iss (config-pmap-c)# set cos 5`



To attach policy maps that contain the following elements to an ingress interface, set policy-map class configuration commands must be used.

- Access control list (ACL) classification
- Per-port per-VLAN classification

**Related Command**

- **class** - Defines a traffic classification for the policy set
- **policy-map** - Used to enter the policy map configuration mode
- **class-map** - Creates a class map
- **show policy-map** - Displays the QoS policy map configuration

## 66.2.12 set qos traffic-class

This command maps a traffic class for the policy and the no form of the command unmaps the traffic class from the policy.

```
set qos traffic-class <traffic-class-id(1-1023)>
```

```
no set qos traffic-class
```

**Mode** Policy-Map Class Configuration Mode

**Defaults** 0

**Example** `iss(config-pmap-c)# set qos traffic-class 10`



Traffic class must have been created prior to the execution of this command.

**Related Command** `qos traffic-class` – Creates a traffic class and selects its output port

## 66.2.13 bandwidth

This command configures the maximum bandwidth for this traffic class in multiples of 64000 bps. If the drop option is set the queue thresholds are set to zero, so that packets above this rate are immediately dropped.

The no form of the command sets the default value for the maximum bandwidth and applies the previously configured drop threshold values. If the drop option is specified then the drop threshold values alone are applied and the maximum bandwidth configuration is not reset.

```
bandwidth <rate 64kbps-units(1-250000)> [exceed-action-drop]
```

```
no bandwidth [exceed-action-drop]
```

**Mode** Traffic Class Configuration Mode

**Defaults** 15625

**Example** `iss(config-tc)# bandwidth 1000 exceed-action-drop`



To specify the 'exceed action drop', the traffic class must have been mapped to an output port.

- Related Command**
- `qos traffic-class` – Creates a traffic class and selects its output port
  - `show qos traffic-class` – Displays the traffic class information

## 66.2.14 min-reserved-bandwidth

This command configures the guaranteed bandwidth for the given policy in multiples of 64000 bps and the no form of the command sets the default value for the guaranteed bandwidth.

```
min-reserved-bandwidth <rate 64kbps-units(1-250000)>
```

```
no min-reserved-bandwidth
```

**Mode** Traffic Class Configuration Mode

**Defaults** 0

**Example** `iss(config-tc)# min-reserved-bandwidth 100`



- Traffic class must have been mapped to an output port.
- Sum of the Guaranteed bandwidths of traffic classes mapped to the same output port must be less than the maximum bandwidth on that port.

**Related Command**

- `qos traffic-class` – Creates a traffic class and selects its output port
- `show qos traffic-class` – Displays the traffic class information

## 66.2.15 queue-threshold

This command configure the three queue drop thresholds for the traffic class in log2 units of the actual bytes. The no form of the command sets the default values for all three drop levels,

```
queue-threshold { [<level1 log2-units (14-27)>] [<level2 log2-units (17-24)>]
 [<level3 log2-units (17-24)>] }
```

```
no queue-threshold
```

|                           |               |                           |
|---------------------------|---------------|---------------------------|
| <b>Syntax Description</b> | <b>level1</b> | - Preferred Output Queue  |
|                           | <b>level2</b> | - Discard Preferred Limit |
|                           | <b>level3</b> | - Discard Wanted Limit    |

**Mode** Traffic Class Configuration Mode

|                 |        |      |
|-----------------|--------|------|
| <b>Defaults</b> | level1 | - 14 |
|                 | level2 | - 17 |
|                 | level3 | - 17 |

**Example** `iss(config-tc)# queue-threshold 20 18 24`



- Traffic class must have been mapped to an output port.
- The queue drop levels cannot be set if exceed-action-drop is set.

**Related Command**

- `qos traffic-class` – Creates a traffic class and selects its output port
- `bandwidth` – Configures the maximum bandwidth for this traffic class in multiples of 64000 bps
- `show qos traffic-class` – Displays the traffic class information

## 66.2.16 set random-detect

This command associates the RED curve with the traffic class and the no form of the command unmaps the existing RED Curve from the traffic class.

```
set random-detect <REDCurve ID (1-63)>
```

```
no set random-detect
```

**Mode** Traffic Class Configuration Mode

**Defaults** 0

**Example** iss(config-tc)# set random-detect 35



- Traffic class must have been mapped to an output port.
- RED curve must have been created.

**Related Command**

- `qos traffic-class` – Creates a traffic class and selects its output port
- `qos random-detect` – Configures the RED (Random Early Detection) parameters
- `show qos traffic-class` – Displays the traffic class information

## 66.2.17 fair-queue

This command enables flowgroups and sets the number of flowgroups for the traffic-class. The no form of the command disables flowgroups for the traffic class.

```
fair-queue {1 | 2 | 8 | 32 | 64 | 128 | 256 | 512}
```

```
no fair-queue
```

**Mode** Traffic Class Configuration Mode

**Defaults** 0

**Example** `iss(config-tc)# fair-queue 8`



- Traffic class must have been mapped to an output port.
- The maximum number of flowgroups available is 2048. This is shared among the active traffic-classes.

**Related Command**

- `qos traffic-class` – Creates a traffic class and selects its output port
- `show qos traffic-class` – Displays the traffic class information
- `show qos maps trafficclass-fairqueue map` – Displays the range of fair queues mapped to each active traffic class

## 66.2.18 weight

This command sets the traffic class weight factor or the weight shift and the no form of the command sets the default weight factor or weight shift for the traffic class.

```
weight {factor <short (0-7)>|shift <short (0-7)>}
```

```
no weight {factor|shift}
```

|                           |               |                 |
|---------------------------|---------------|-----------------|
| <b>Syntax Description</b> | <b>factor</b> | - Weight Factor |
|---------------------------|---------------|-----------------|

|  |              |                |
|--|--------------|----------------|
|  | <b>shift</b> | - Shift Factor |
|--|--------------|----------------|

|                 |        |   |
|-----------------|--------|---|
| <b>Defaults</b> | factor | 4 |
|-----------------|--------|---|

|  |       |   |
|--|-------|---|
|  | shift | 4 |
|--|-------|---|

|             |                                  |  |
|-------------|----------------------------------|--|
| <b>Mode</b> | Traffic Class Configuration Mode |  |
|-------------|----------------------------------|--|

|                |                                 |  |
|----------------|---------------------------------|--|
| <b>Example</b> | iss(config-tc)# weight factor 6 |  |
|----------------|---------------------------------|--|



Traffic class must have been mapped to an output port.

|                        |                                                                                                                                                                                                                   |  |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <b>Related Command</b> | <ul style="list-style-type: none"><li>• <b>qos traffic-class</b> – Creates a traffic class and selects its output port</li><li>• <b>show qos traffic-class</b> – Displays the traffic class information</li></ul> |  |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

## 66.2.19 qos bandwidth

This command configures the maximum bandwidth for this port in multiples of 64000 bps. If the drop option is set, the queue thresholds are set to zero so that packets above this rate are immediately dropped.

The no form of the command sets the default value for the maximum bandwidth and applies the previously configured drop level values. If the drop option is specified then the drop threshold values alone are applied and the maximum bandwidth configuration is not reset.

```
qos bandwidth <rate-64kbps(1-250000)> [exceed-action-drop]
```

```
no qos bandwidth [exceed-action-drop]
```

|                           |                                                                        |               |
|---------------------------|------------------------------------------------------------------------|---------------|
| <b>Syntax Description</b> | <b>exceed-action-drop</b>                                              | - Drop option |
| <b>Mode</b>               | Interface Configuration Mode                                           |               |
| <b>Default values</b>     | 15625                                                                  |               |
| <b>Example</b>            | iss(config-if)# qos bandwidth 2000                                     |               |
| <b>Related Command</b>    | <b>show qos interface</b> – Displays interface related QoS information |               |

## 66.2.20 qos queue threshold

This command configures the three queue drop levels for this port in log2 units of the actual bytes. The no form of the command sets the default values for all three drop levels.

```
qos queue-threshold [<level1 log2-units(14-27)>] [<level2 log2-units(17-24)>]
[<level3 log2-units (17-24)>]}
```

```
no qos queue-threshold
```

**Syntax Description**

|               |                          |
|---------------|--------------------------|
| <b>level1</b> | - Preferred Output Queue |
|---------------|--------------------------|

|                |                           |
|----------------|---------------------------|
| <b>Level12</b> | - Discard Preferred Limit |
|----------------|---------------------------|

|                |                        |
|----------------|------------------------|
| <b>Level13</b> | - Discard Wanted Limit |
|----------------|------------------------|

**Mode** Interface Configuration Mode

**Defaults**

|        |      |
|--------|------|
| level1 | - 14 |
|--------|------|

|        |      |
|--------|------|
| level2 | - 17 |
|--------|------|

|        |      |
|--------|------|
| level3 | - 17 |
|--------|------|

**Example** iss(config-if)# qos queue-threshold 20 18 24



The queue drop levels cannot be set if exceed-action-drop is set.

**Related Command**

- **qos bandwidth** – Configures the maximum bandwidth for this port in multiples of 64000 bps
- **show qos interface** – Displays interface related QoS information

## 66.2.21 qos set random-detect

This command associates the RED curve with the port and the no form of the command unmaps the existing RED Curve from this port.

```
qos set random-detect <REDCurve ID (64-126)>
```

```
no qos set random-detect
```

**Mode** Interface Configuration Mode

**Default** 127

### Example

```
iss(config-if)# qos set random-detect 50
```



RED curve must have been created.

### Related Command

- **qos random-detect** – Configures the RED (Random Early Detection) parameters
- **show qos interface** – Displays interface related QoS information

## 66.2.22 shutdown qos

This command shuts down the Quality-of-Service operation. The no form of the command starts and enables the Quality-of-Service operation.

**shutdown qos**

**no shutdown qos**

**Mode** Global Configuration Mode

**Defaults** QoS is started and enabled by default

**Example** `iss(config)# shutdown qos`



- When shutdown, all the pools used by DiffServ module will be released to the system.
- When started, the resources required by DiffServ module are allocated and the module starts running.

**Related Command**

- **show policy-map** - Displays the quality of service (QoS) policy maps
- **show class-map** - Displays quality of service (QoS) class maps

## 66.2.23 show policy-map

This command displays the quality of service (QoS) policy maps, which defines the classification criteria for the incoming traffic. Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

```
show policy-map [<policy-map-num(1-65535)> [class <class-map-num(1-65535)>]]
```

**Syntax Description**

**policy-map-num** - Policy map number

**class** - Class map number

**Mode** Privileged/User EXEC Mode

**Example** iss# show policy-map 24

```
DiffServ Configurations:
```

```
-----
```

```
Quality of Service has been enabled
Policy Map 24 is not active
Class Map: 20
```

```
-----
```

```
Protocol                               : 255
In Profile Entry
```

```
-----
```

```
In profile action                       : policed-precedence 5
Out Profile Entry
```

```
-----
```

```
Metering on
burst bytes/token size                 : 6
Refresh count                          : 1000
Out profile action                     : drop
```

```
No Match Entry
```

```
-----
```

```
No match action                       : policed-precedence 5
```

**Related Command**

- **policy-map** - Used to enter the policy map configuration mode
- **class** - Defines a traffic classification for the policy to act
- **set cos** - Defines the in-profile action by setting a CoS, DSCP or IP-precedence value in the packet



## 66.2.25 show qos maps dscp-queue

This command displays the DSCP to queue mapping information. The d1 column specifies the most-significant digit of the original DSCP, the d2 row specifies the least-significant digit of the original DSCP. The intersection of d1 and d2 gives the mapped queue number.

**show qos maps dscp-queue map**

**Mode** Privileged/User EXEC Mode

**Example** iss# show qos maps dscp-queue map

DiffServ DSCP-Queue map

```
-----
d1 : d2  0  1  2  3  4  5  6  7  8  9
0 :    00 00 00 00 00 00 00 00 01 01
1 :    01 01 01 01 01 01 02 02 02 02
2 :    07 02 02 02 03 03 03 03 03 03
3 :    03 03 04 04 04 04 04 04 04 04
4 :    05 05 05 05 05 05 05 05 06 06
5 :    06 06 06 06 06 06 07 07 07 07
6 :    07 07 07 07
```

**Related Command** **qos map dscp-queue** – Maps the given DSCP value to an egress queue

## 66.2.26 show qos maps trafficclass-fairqueue map

This command displays the range of fair queues mapped to each active traffic class.

**show qos maps trafficclass-fairqueue map**

**Mode** Privileged/User EXEC Mode

**Example** iss# show qos maps trafficclass-fairqueue map

```
DiffServ TrafficClass-FairQueue mapping:
```

```
-----  
Traffic-class 77: 1-2
```

**Related Command** **fair-queue** – Enables flowgroups and sets the number of flowgroups for this traffic-class

## 66.2.27 show qos queue precedence

This command displays the queue precedence of the DSCP and the L2 COS values for switched and routed traffic.

### show qos queue precedence

**Mode** Privileged/User EXEC Mode

**Example**

```
iss# show qos queue precedence
Queue Precedence
-----
Switched:
COS Precedence : 5
DSCP Precedence : 2

Routed:
COS Precedence : 3
DSCP Precedence : 1
```

- Related Command**
- **qos queue-precedence switched** – Sets the queue precedence of DSCP, L2 COS for switched packets
  - **qos queue-precedence routed** – Sets the queue precedence of DSCP, L2 COS for routed packets

## 66.2.28 show qos traffic-class

This command displays the traffic class information.

```
show qos traffic-class [<traffic-class-id(1-1023)>]
```

**Mode** Privileged/User EXEC Mode

**Example** iss# show qos traffic-class

```
DiffServ Traffic class Configurations:
```

```
-----  
Quality of Service has been enabled
```

```
Traffic class 2 is active
```

```
Output port           : 2  
Maximum bandwidth    : 2 (in multiples of 64000 bps)  
Guaranteed bandwidth : 0 (in multiples of 64000 bps)  
Drop Threshold1      : 0 (in log2 units of actual bytes)  
Drop Threshold2      : 0 (in log2 units of actual bytes)  
Drop Threshold3      : 0 (in log2 units of actual bytes)  
Weight factor        : 4  
Weight shift         : 4  
First fair-queue assigned : 0  
Number of fair-queues used : 0  
RED Curve ID         : 0  
Number of bytes accepted : 0  
Number of bytes discarded : 0
```

```
Traffic class 7 is active
```

```
Output port           : 5  
Maximum bandwidth    : 1000 (in multiples of 64000 bps)  
Guaranteed bandwidth : 100 (in multiples of 64000 bps)  
Drop Threshold1      : 0 (in log2 units of actual bytes)  
Drop Threshold2      : 0 (in log2 units of actual bytes)  
Drop Threshold3      : 0 (in log2 units of actual bytes)  
Weight factor        : 4  
Weight shift         : 4  
First fair-queue assigned : 0  
Number of fair-queues used : 0  
RED Curve ID         : 0  
Number of bytes accepted : 0  
Number of bytes discarded : 0
```

```
Traffic class 10 is active
```

```
Output port           : 1  
Maximum bandwidth    : 15625 (in multiples of 64000 bps)  
Guaranteed bandwidth : 0 (in multiples of 64000 bps)  
Drop Threshold1      : 14 (in log2 units of actual bytes)  
Drop Threshold2      : 17 (in log2 units of actual bytes)  
Drop Threshold3      : 17 (in log2 units of actual bytes)  
Weight factor        : 4  
Weight shift         : 4
```

```

First fair-queue assigned : 0
Number of fair-queues used : 0
RED Curve ID : 0
Number of bytes accepted : 0
Number of bytes discarded : 0

Traffic class 22 is active
Output port : 0
Maximum bandwidth : 15625 (in multiples of 64000 bps)
Guaranteed bandwidth : 0 (in multiples of 64000 bps)
Drop Threshold1 : 14 (in log2 units of actual bytes)
Drop Threshold2 : 17 (in log2 units of actual bytes)
Drop Threshold3 : 17 (in log2 units of actual bytes)
Weight factor : 4
Weight shift : 4
First fair-queue assigned : 0
Number of fair-queues used : 0
RED Curve ID : 0
Number of bytes accepted : 0
Number of bytes discarded : 0

Traffic class 23 is active
Output port : 1
Maximum bandwidth : 15625 (in multiples of 64000 bps)
Guaranteed bandwidth : 1 (in multiples of 64000 bps)
Drop Threshold1 : 14 (in log2 units of actual bytes)
Drop Threshold2 : 17 (in log2 units of actual bytes)
Drop Threshold3 : 17 (in log2 units of actual bytes)
Weight factor : 4
Weight shift : 4
First fair-queue assigned : 0
Number of fair-queues used : 0
RED Curve ID : 0
Number of bytes accepted : 0
Number of bytes discarded : 0

Traffic class 24 is active
Output port : 1
Maximum bandwidth : 15625 (in multiples of 64000 bps)
Guaranteed bandwidth : 0 (in multiples of 64000 bps)
Drop Threshold1 : 14 (in log2 units of actual bytes)
Drop Threshold2 : 17 (in log2 units of actual bytes)
Drop Threshold3 : 17 (in log2 units of actual bytes)
Weight factor : 4
Weight shift : 4
First fair-queue assigned : 0
Number of fair-queues used : 0
RED Curve ID : 0
Number of bytes accepted : 0
Number of bytes discarded : 0

Traffic class 77 is active
Output port : 3
Maximum bandwidth : 15625 (in multiples of 64000 bps)
Guaranteed bandwidth : 0 (in multiples of 64000 bps)
Drop Threshold1 : 20 (in log2 units of actual bytes)
Drop Threshold2 : 18 (in log2 units of actual bytes)

```

```
Drop Threshold3           : 24 (in log2 units of actual bytes)
Weight factor             : 6
Weight shift              : 4
First fair-queue assigned : 1
Number of fair-queues used : 2
RED Curve ID              : 2
Number of bytes accepted  : 0
Number of bytes discarded : 0
```

**Related  
Command**

- **qos traffic-class** – Creates a traffic class and selects its output port
- **bandwidth** – Configures the maximum bandwidth for this traffic class in multiples of 64000 bps
- **min-reserved-bandwidth** – Configures the guaranteed bandwidth for this policy in multiples of 64000 bps
- **queue-threshold** – Configure the three queue drop thresholds for this traffic class in log2 units of the actual bytes
- **set random-detect** – Associates the RED curve with the traffic class
- **fair-queue** – Enables flowgroups and sets the number of flowgroups for this traffic-class
- **weight** – Sets the traffic class weight factor or the weight shift

## 66.2.29 show qos random-detect

This command displays RED curve information.

```
show qos random-detect [<RED-curve (1-126)>]
```

**Mode** Privileged/User EXEC Mode

**Example** iss# show qos random-detect

```
DiffServ RED configurations:
-----
Quality of Service has been enabled

RED Curve 2 is active
Curve start           : 14 (in multiples of 16 KB)
Curve stop            : 17 (in multiples of 16 KB)
QRange                : 18 (in log2 units of actual bytes)
Probability at Start+QRange : 200
```

**Related Command** `qos set random-detect` – Configures the RED (Random Early Detection) parameters

## 66.2.30 show qos interface

This command displays interface related QoS information.

```
show qos interface [<interface-type> <interface-id>]
```

**Mode** Privileged/User EXEC Mode

**Example** `iss# show qos interface gigabitethernet 0/1`

```
DiffServ Port configurations:
```

```
-----  
Quality of Service has been enabled
```

```
Port 1  
Maximum bandwidth           : 1 (in multiples of 64000 bps)  
Drop Threshold1             : 14 (in log2 units of actual bytes)  
Drop Threshold2             : 17 (in log2 units of actual bytes)  
Drop Threshold3             : 17 (in log2 units of actual bytes)  
RED Curve ID                 : 127
```

- Related Command**
- `qos bandwidth` – Configures the maximum bandwidth for the port in multiples of 64000 bps
  - `qos queue threshold` – Configures the three queue drop levels for this port in log2 units of the actual bytes
  - `qos set random-detect` – Associates the RED curve with the port

## 66.2.31 show qos statistics

This command displays QoS statistics.

### show qos statistics

**Mode** Privileged/User EXEC Mode

**Example** `iss# show qos statistics`

```
Quality of Service is enabled

DiffServ Statistics
-----
Number of packets offered to WFHBD
: 2950
Number of packets accepted by WFHBD
: 2950
Number of packets rejected by WFHBD
: 0
Number of bytes offered to WFHBD
: 466383
Number of bytes accepted by WFHBD
: 466383
Number of bytes rejected by WFHBD
: 0
Wrong port accepted packets count
: 0
Wrong port rejected packets count
: 0
Fair flow group accepted packets count
: 0
Number of Unfair flow group packets discarded
: 0
Packets discarded for exceeding threshold 2 count (port+traffic
class) : 0
Packets discarded for exceeding threshold 3 count (port+traffic
class) : 0
Number of packets accepted as belonging to a fair traffic class
: 0
Number of packets accepted without any active accept/reject
decision : 2950
Number of packets discarded by port RED
: 0
Number of packets discarded by traffic class RED
: 0
```

## 66.3 Marvell 6095 Specific Commands

This section describes the CLI commands executable only in Marvell 6095 target for configuring QoS feature supported by ISS.

The list of CLI commands for the configuration of QoS is as follows:

- shutdown qos
- qos
- priority-map
- queue-map
- qos scheduling policy
- qos match
- qos override
- qos tagifboth match
- map
- map vlan
- show qos global info
- show priority-map
- show queue-map
- show qos port config
- show qos port override config
- show qos scheduling policy

## 66.3.1 shutdown qos

This command shuts down the QoS subsystem. The resources allocated to the QoS module are released back into the system. If the user does not require the services of the QoS module at run time, uses this command to shut it down. The no form of the command starts the QoS subsystem.

**shutdown qos**

**no shutdown qos**

**Mode** Global Configuration Mode

**Package** Workgroup

**Default** QoS subsystem is started and enabled.

**Example** `iss(config)# shutdown qos`

**Related Commands** `show qos global info` - Displays QoS related global configurations.

## 66.3.2 qos

This command enables or disables the QoS subsystem.

**qos {enable | disable}**

**Syntax Description**      **enable** - Enables QoS subsystem. QoS module programs the hardware and starts protocol operation.

**disable** - Disables QoS subsystem. QoS module stops protocol operation by deleting the hardware configuration.

**Mode**                      Global Configuration Mode

**Package**                  Workgroup

**Default**                  enable

**Example**                  `iss(config)# qos disable`

**Related Commands**      `show qos global info` - Displays QoS related global configurations.

### 66.3.3 priority-map

This command adds a priority map entry. A priority map is used to map an incoming priority to a regenerated priority for an ingress port or VLAN. These entries are stored in a priority table. The no form of the command deletes a priority map entry.

```
priority-map <priority-map-Id(1-65535)>
```

```
no priority-map <priority-map-Id(1-65535)>
```

|               |                             |   |                                                                                                                                                                    |
|---------------|-----------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b> | <priority-map-Id(1-65535)>> | - | Configures the priority map index for the incoming packet received over ingress Port/VLAN with specified incoming priority. This value ranges between 1 and 65535. |
|---------------|-----------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|             |                           |
|-------------|---------------------------|
| <b>Mode</b> | Global Configuration Mode |
|-------------|---------------------------|

|                |           |
|----------------|-----------|
| <b>Package</b> | Workgroup |
|----------------|-----------|

|                |                              |
|----------------|------------------------------|
| <b>Example</b> | iss(config)# priority-map 25 |
|----------------|------------------------------|



QoS subsystem should have been started.

|                        |                                                             |
|------------------------|-------------------------------------------------------------|
| <b>Related Command</b> | <b>show priority-map</b> - Displays the priority map entry. |
|------------------------|-------------------------------------------------------------|

## 66.3.4 queue-map

This command creates a map for a queue with regenerated priority. The no form of the command deletes a queue map entry.

```
queue-map regn-priority { vlanPri | ipDscp } <integer(0-63)> queue-id
<integer(0-3)>
```

```
no queue-map regn-priority { vlanPri | ipDscp } <integer(0-63)>
```

|                           |                                     |                                                                                                                                                  |
|---------------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>regn-priority</b>                | - Configures the regenerated-priority, for an incoming packet, that needs to be mapped to an outbound queue. This value ranges between 0 and 63. |
|                           | <b>vlanPri</b>                      | - Configures the type of regen-priority as VLAN priority.                                                                                        |
|                           | <b>ipDscp</b>                       | - Configures the type of regen-priority as IP Differentiated Services Code Point.                                                                |
|                           | <b>queue-id&lt;integer(0-3)&gt;</b> | - Configures the queue identifier that uniquely identifies a queue relative to an interface. This value ranges between 0 and 3.                  |

**Mode** Global Configuration Mode

**Package** Workgroup

**Example** `iss(config)# queue-map regn-priority vlanPri 2 queue-id 1`

**Related Command** `show queue-map` - Displays the configured queue map.

## 66.3.5 qos scheduling policy

This command sets packet scheduling algorithm for the device.

```
qos scheduling policy { strict | wrr }
```

|                           |                                                                                              |                                                              |
|---------------------------|----------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| <b>Syntax Description</b> | <b>strict</b>                                                                                | - Configures the scheduling algorithm as strict priority.    |
|                           | <b>wrr</b>                                                                                   | - Configures the scheduling algorithm as weightedRoundRobin. |
| <b>Mode</b>               | Global Configuration Mode                                                                    |                                                              |
| <b>Package</b>            | Workgroup                                                                                    |                                                              |
| <b>Default</b>            | Wrr                                                                                          |                                                              |
| <b>Example</b>            | <pre>iss(config)# qos scheduling policy strict</pre>                                         |                                                              |
| <b>Related Command</b>    | <b>show qos scheduling policy</b> - Displays the packet scheduling algorithm for the device. |                                                              |

## 66.3.6 qos match

This command enables VLAN priority /IP DSCP priority classification on this port. The no form of the command disables VLAN priority/IP DSCP priority classification on this port.

```
qos match { vlanPri | ipDscp }
```

```
no qos match { vlanPri | ipDscp }
```

|                    |                |                                            |
|--------------------|----------------|--------------------------------------------|
| <b>Syntax</b>      | <b>vlanPri</b> | - Configures VLAN priority on the port.    |
| <b>Description</b> | <b>ipDscp</b>  | - Configures IP DSCP priority on the port. |

|             |                              |
|-------------|------------------------------|
| <b>Mode</b> | Interface Configuration Mode |
|-------------|------------------------------|

|                |           |
|----------------|-----------|
| <b>Package</b> | Workgroup |
|----------------|-----------|

|                |                                      |
|----------------|--------------------------------------|
| <b>Default</b> | Both vlanPri and ipDscp are enabled. |
|----------------|--------------------------------------|

|                |                                  |
|----------------|----------------------------------|
| <b>Example</b> | iss(config-if)# qos match ipDscp |
|----------------|----------------------------------|

|                        |                                                                    |
|------------------------|--------------------------------------------------------------------|
| <b>Related Command</b> | <b>show qos port config</b> - Displays the QoS port configuration. |
|------------------------|--------------------------------------------------------------------|

## 66.3.7 qos override

This command enables VLAN ID/Source MAC/Destination MAC priority classification on this port. The no form of the command disables VLAN ID/Source MAC/Destination MAC priority classification on this port.

```
qos { vlan-id | src-mac | dest-mac } override
```

```
no qos { vlan-id | src-mac | dest-mac } override
```

|                           |                 |   |                                                                                     |
|---------------------------|-----------------|---|-------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>vlan-id</b>  | - | Configures the VLAN Identifier as priority classification on this port.             |
|                           | <b>src-mac</b>  | - | Configures the Source MAC address as the priority classification on this port.      |
|                           | <b>dest-mac</b> | - | Configures the Destination MAC address as the priority classification on this port. |

**Mode** Interface Configuration Mode

**Package** Workgroup

|                |          |   |         |
|----------------|----------|---|---------|
| <b>Default</b> | vlan-id  | - | enabled |
|                | src-mac  | - | enabled |
|                | dest-mac | - | enabled |

**Example** `iss(config-if)# qos 1 override`

**Related Command** `show qos port override config` - Displays the QoS port override configuration.

## 66.3.8 qos tagifboth match

This command configures which priority classification (VLAN priority or IP DSCP priority) to tag on the packet that carries both priorities is received on the port.

```
qos tagifboth match { vlanPri | ipDscp }
```

|                           |                                                                    |                                                                             |
|---------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>vlanPri</b>                                                     | - Configures the VLAN priority as the priority classification on this port. |
|                           | <b>ipDscp</b>                                                      | - Configures the IP DSCP as the priority classification on this port.       |
| <b>Mode</b>               | Interface Configuration Mode                                       |                                                                             |
| <b>Package</b>            | Workgroup                                                          |                                                                             |
| <b>Default</b>            | vlanPri                                                            |                                                                             |
| <b>Example</b>            | iss(config-if)# qos tagifboth match vlanPri                        |                                                                             |
| <b>Related Command</b>    | <b>show qos port config</b> - Displays the QoS port configuration. |                                                                             |

## 66.3.9 map

This command adds a priority map entry for mapping incoming priority to a regenerated priority.

```
map [interface <iftype> <ifnum>] in-priority-type vlanPri in-priority
<integer(0-7)> regen-priority <integer(0-7)>
```

|                           |                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>iftype</b>                          | <ul style="list-style-type: none"> <li>- Configures the specified type of interface. The interface can be:           <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> </li> </ul> |
|                           | <b>ifnum</b>                           | <ul style="list-style-type: none"> <li>- Configures the interface number for the specified interface identifier. This is a unique value that represents the specific interface.<br/>           This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.<br/>           For example: 0/1 represents that the slot number is 0 and port number is 1.<br/>           Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</li> </ul>                                                                                                                                                                                                                                                             |
|                           | <b>in-priority-type</b>                | <ul style="list-style-type: none"> <li>- Configures the Incoming priority type.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                           | <b>vlanPri</b>                         | <ul style="list-style-type: none"> <li>- Configures the priority of the vlan.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                           | <b>in-priority&lt;integer(0-7)&gt;</b> | <ul style="list-style-type: none"> <li>- Configures the incoming priority value. This value ranges between 0 and 7.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                           | <b>regen-</b>                          | <ul style="list-style-type: none"> <li>- Configures the regenerated priority. This value ranges</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|                        |                                                                                                                                                                                      |                  |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
|                        | <code>priority&lt;integer (0-7)&gt;</code>                                                                                                                                           | between 0 and 7. |
| <b>Mode</b>            | Priority Map Configuration Mode                                                                                                                                                      |                  |
| <b>Package</b>         | Workgroup                                                                                                                                                                            |                  |
| <b>Default</b>         | In-priority-type                                                                                                                                                                     | vlanPri          |
|                        | in-priority                                                                                                                                                                          | - 0              |
|                        | regen-priority                                                                                                                                                                       | - 0              |
| <b>Example</b>         | <pre>iss(config-pri-map)# map interface gig 0/1 in-priority-type vlanPri in-priority 0 regen-priority 7</pre>                                                                        |                  |
| <b>Related Command</b> | <ul style="list-style-type: none"><li>• <code>priority-map</code> - Adds a priority map entry.</li><li>• <code>show priority-map</code> - Displays the priority map entry.</li></ul> |                  |

## 66.3.10 map vlan

This command adds a priority map entry for mapping incoming priority to regenerated priority.

```
map vlan <integer(1-4094)> in-priority-type { vlan-id | src-mac | dest-mac }
[unicast <aa:aa:aa:aa:aa:aa>] regen-priority <integer(0-7)>
```

|                           |                                            |                                                                                                                                                                                                                                                              |
|---------------------------|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>vlan&lt;integer(1-4094)&gt;</b>         | - Configures the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created.<br>This value ranges between 1 and 4094.                                                                                               |
|                           | <b>in-priority-type</b>                    | - Configures the type of the incoming priority. This can be any one of the following: <ul style="list-style-type: none"> <li>• vlan-id – VLAN Identifier.</li> <li>• src-mac – Source MAC address.</li> <li>• dest-mac – Destination MAC address.</li> </ul> |
|                           | <b>unicast&lt;aa:aa:aa:aa:aa:aa&gt;</b>    | - Configures the unicast MAC address                                                                                                                                                                                                                         |
|                           | <b>regen-priority &lt;integer(0-7)&gt;</b> | - Configures the regenerated priority. This value ranges between 0 and 7.                                                                                                                                                                                    |

**Mode** Priority Map Configuration Mode

**Package** Workgroup

**Example**

```
iss(config-pri-map)# map vlan 1 in-priority-type 1 unicast
00:01:02:03:04:05 regen-priority 5
```



- Priority Map Entry should have been created.
- For **vlan-id** in-priority-type, VLAN should have already been created.
- For **src-mac** and **dest-mac** in-priority-type, static unicast MAC address in the forwarding database should have already been created.

**Related Command**

- **priority-map** - Adds a priority map entry.
- **show priority-map** - Displays the priority map entry.

## 66.3.11 show qos global info

This command displays QoS related global configurations such as system control and trace flag.

**show qos global info**

**Mode** Privileged EXEC Mode

**Package** Workgroup

**Example** iss# show qos global info

```
QoS Global Information
```

```
-----
```

```
System Control           : Start  
System Control           : Enable  
Trace Flag               : 0
```

- Related Commands**
- **shutdown qos** - Shuts down the QoS subsystem.
  - **qos** - Enables or disables the QoS subsystem.

## 66.3.12 show priority-map

This command displays the priority map entry such as PriorityMapId, IfIndex, InType, InPriority and RegenPriority.

```
show priority-map [<priority-map-id(1-65535)>]
```

|                           |                                         |   |                                                                                                                                  |
|---------------------------|-----------------------------------------|---|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>&lt;priority-map-id(1-65535)&gt;</b> | - | Displays the output priority map index for the incoming packet received over ingress Port/VLAN with specified incoming priority. |
|---------------------------|-----------------------------------------|---|----------------------------------------------------------------------------------------------------------------------------------|

|             |                      |
|-------------|----------------------|
| <b>Mode</b> | Privileged EXEC Mode |
|-------------|----------------------|

|                |           |
|----------------|-----------|
| <b>Package</b> | Workgroup |
|----------------|-----------|

|                |                        |
|----------------|------------------------|
| <b>Example</b> | iss# show priority-map |
|----------------|------------------------|

```
QoS Priority Map Entries
```

```
-----
```

```
PriorityMapId      : 1
IfIndex           : 0
InType            : VlanPriority
InPriority         : 0
RegenPriority      : 0
```

```
PriorityMapId      : 2
IfIndex           : 0
InType            : VlanPriority
InPriority         : 1
RegenPriority      : 1
```

```
PriorityMapId      : 3
IfIndex           : 0
InType            : VlanPriority
InPriority         : 2
RegenPriority      : 2
```

```
PriorityMapId      : 4
IfIndex           : 0
InType            : VlanPriority
InPriority         : 3
RegenPriority      : 3
```

```
PriorityMapId           : 5
IfIndex                : 0
InType                 : VlanPriority
InPriority              : 4
RegenPriority           : 4

PriorityMapId           : 6
IfIndex                : 0
InType                 : VlanPriority
InPriority              : 5
RegenPriority           : 5

PriorityMapId           : 7
IfIndex                : 0
InType                 : VlanPriority
InPriority              : 6
RegenPriority           : 6

PriorityMapId           : 8
IfIndex                : 0
InType                 : VlanPriority
InPriority              : 7
RegenPriority           : 7
```



If executed without the optional parameters, this command displays all the available Priority Map information.

**Related  
Commands**

**priority-map** - Adds a priority map entry.

## 66.3.13 show queue-map

This command displays the configured queue map.

### show queue-map

**Mode** Privileged EXEC Mode

**Package** Workgroup

**Example** iss# show queue-map

```
QoS Queue Map Entries
```

```
-----
```

| PriorityType | Priority Value | Mapped Queue |
|--------------|----------------|--------------|
| -----        |                |              |
| VlanPri      | 0              | 1            |
| VlanPri      | 1              | 0            |
| VlanPri      | 2              | 0            |
| VlanPri      | 3              | 1            |
| VlanPri      | 4              | 2            |
| VlanPri      | 5              | 2            |
| VlanPri      | 6              | 3            |
| VlanPri      | 7              | 3            |
| IpDscp       | 0              | 0            |
| IpDscp       | 1              | 0            |
| IpDscp       | 2              | 0            |
| IpDscp       | 3              | 0            |
| IpDscp       | 4              | 0            |
| IpDscp       | 5              | 0            |
| IpDscp       | 6              | 0            |
| IpDscp       | 7              | 0            |
| IpDscp       | 8              | 0            |
| IpDscp       | 9              | 0            |
| IpDscp       | 10             | 0            |
| IpDscp       | 11             | 0            |
| IpDscp       | 12             | 0            |
| IpDscp       | 13             | 0            |

---

|        |    |   |
|--------|----|---|
| IpDscp | 14 | 0 |
| IpDscp | 15 | 0 |
| IpDscp | 16 | 1 |
| IpDscp | 17 | 1 |
| IpDscp | 18 | 1 |
| IpDscp | 19 | 1 |
| IpDscp | 20 | 1 |
| IpDscp | 21 | 1 |
| IpDscp | 22 | 1 |
| IpDscp | 23 | 1 |
| IpDscp | 24 | 1 |
| IpDscp | 25 | 1 |
| IpDscp | 26 | 1 |
| IpDscp | 27 | 1 |
| IpDscp | 28 | 1 |
| IpDscp | 29 | 1 |
| IpDscp | 30 | 1 |
| IpDscp | 31 | 1 |
| IpDscp | 32 | 2 |
| IpDscp | 33 | 2 |
| IpDscp | 34 | 2 |
| IpDscp | 35 | 2 |
| IpDscp | 36 | 2 |
| IpDscp | 37 | 2 |
| IpDscp | 38 | 2 |
| IpDscp | 39 | 2 |
| IpDscp | 40 | 2 |
| IpDscp | 41 | 2 |
| IpDscp | 42 | 2 |
| IpDscp | 43 | 2 |
| IpDscp | 44 | 2 |
| IpDscp | 45 | 2 |
| IpDscp | 46 | 2 |
| IpDscp | 47 | 2 |
| IpDscp | 48 | 3 |
| IpDscp | 49 | 3 |
| IpDscp | 50 | 3 |

---

|        |    |   |
|--------|----|---|
| IpDscp | 51 | 3 |
| IpDscp | 52 | 3 |
| IpDscp | 53 | 3 |
| IpDscp | 54 | 3 |
| IpDscp | 55 | 3 |
| IpDscp | 56 | 3 |
| IpDscp | 57 | 3 |
| IpDscp | 58 | 3 |
| IpDscp | 59 | 3 |
| IpDscp | 60 | 3 |
| IpDscp | 61 | 3 |
| IpDscp | 62 | 3 |
| IpDscp | 63 | 3 |

**Related  
Commands**

**queue-map** - Creates a map for a queue with regenerated priority.

## 66.3.14 show qos port config

This command displays the QoS port configuration.

```
show qos port config [interface <iftype> <ifnum>]
```

|                    |                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>      | <b>&lt;iftype&gt;</b>                                                                                                                               | <ul style="list-style-type: none"> <li>- Displays the interface type for the specified type of interface. The interface can be:           <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> </li> </ul> |
| <b>Description</b> | <b>&lt;ifnum&gt;</b>                                                                                                                                | <ul style="list-style-type: none"> <li>- Displays the interface number for the specified interface identifier. This is a unique value that represents the specific interface.<br/>           This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.<br/>           For example: 0/1 represents that the slot number is 0 and port number is 1.<br/>           Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</li> </ul>                                                                                                                                                                                                                                                                                    |
| <b>Mode</b>        | Privileged EXEC Mode                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Package</b>     | Workgroup                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Example</b>     | <pre>iss# show qos port config</pre> <p style="text-align: center; color: blue;">Priority Config Table</p> <p style="text-align: center;">-----</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Port  | VlanPri | IpDscp  | Vlan/IP |
|-------|---------|---------|---------|
| Gi0/1 | Enabled | Enabled | VlanPri |
| Gi0/2 | Enabled | Enabled | VlanPri |
| Gi0/3 | Enabled | Enabled | VlanPri |
| Gi0/4 | Enabled | Enabled | VlanPri |
| Gi0/5 | Enabled | Enabled | VlanPri |
| Gi0/6 | Enabled | Enabled | VlanPri |
| Gi0/7 | Enabled | Enabled | VlanPri |
| Gi0/8 | Enabled | Enabled | VlanPri |

```
iss# show qos port config interface gigabitethernet 0/1
```

#### Priority Config Table

| Port  | VlanPri | IpDscp  | Vlan/IP |
|-------|---------|---------|---------|
| Gi0/1 | Enabled | Enabled | VlanPri |

#### Related Commands

- **qos match** – Enables VLAN priority/IP DSCP priority classification on this port.
- **qos tagifboth match** - Chooses either VLAN priority or IP DSCP priority classification on this port, when a packet with both the priorities is received on the port.

## 66.3.15 show qos port override config

This command displays the QoS port override configuration. Information such as port, vlan id, source mac address and destination mac address are displayed.

```
show qos port override config [interface <iftype> <ifnum>]
```

|                           |                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>&lt;iftype&gt;</b> | - Displays the interface type for the specified type of interface. The interface can be: <ul style="list-style-type: none"> <li>• fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> |
|                           | <b>&lt;ifnum&gt;</b>  | - Displays the interface number for the specified interface identifier. This is a unique value that represents the specific interface.<br><br>This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.<br><br>For example: 0/1 represents that the slot number is 0 and port number is 1.<br><br>Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.                                                                                                                                                                                                                                                                                                 |

**Mode** Privileged EXEC Mode

**Package** Workgroup

**Example** iss# show qos port override config

```
Priority Override Config Table
```

```
-----
Port   Vlan-ID  SRC-MAC  DEST-MAC
```

---

|       |         |         |         |
|-------|---------|---------|---------|
| ----- | -----   | -----   | -----   |
| Gi0/1 | Enabled | Enabled | Enabled |
| Gi0/2 | Enabled | Enabled | Enabled |
| Gi0/3 | Enabled | Enabled | Enabled |
| Gi0/4 | Enabled | Enabled | Enabled |
| Gi0/5 | Enabled | Enabled | Enabled |
| Gi0/6 | Enabled | Enabled | Enabled |
| Gi0/7 | Enabled | Enabled | Enabled |
| Gi0/8 | Enabled | Enabled | Enabled |

**Related  
Commands**

**qos - override** - Enables VLAN ID/Source MAC/Destination MAC priority classification on this port.

## 66.3.16 show qos scheduling policy

This command displays the packet scheduling algorithm for the device.

**show qos scheduling policy**

**Mode** Privileged EXEC Mode

**Package** Workgroup

**Example** iss# show qos scheduling policy  
*Scheduling Policy: Weighted Round Robin*

**Related Commands** `qos scheduling policy` - Sets packet scheduling algorithm for the device.

---

## 66.4 xCAT Specific Commands

This section describes the CLI commands executable only in xCAT target for configuring DiffServ feature supported by ISS.

The list of CLI commands for the configuration of DiffServ is as follows:

- set qos
- class-map
- policy-map
- match
- class
- set cos
- shutdown qos
- cosq scheduling algorithm
- traffic class
- show policy-map
- show class-map
- show cosq algorithm
- show cosq weights-bw

## 66.4.1 set qos

This command enables differentiated services on the device. The disable option is used to disable the QoS feature on the device.

```
set qos { enable | disable }
```

**Syntax Description**

|               |                                   |
|---------------|-----------------------------------|
| <b>enable</b> | - Enables differentiated services |
|---------------|-----------------------------------|

|                |                                    |
|----------------|------------------------------------|
| <b>disable</b> | - Disables differentiated services |
|----------------|------------------------------------|

**Mode** Global Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Defaults** disable

**Example** `iss(config)# set qos enable`



- QoS must be globally enabled prior to the execution of the class-map and policy-map mode commands.
- When set as 'enabled', DiffServ Module programs the hardware and starts Protocol Operation.
- When set as 'disabled', it stops protocol operation by deleting the hardware configuration.

**Related Commands**

- `show policy-map` - Displays the quality of service (QoS) policy maps
- `show class-map` - Displays quality of service (QoS) class maps

## 66.4.2 class-map

This command creates a class map that is meant to be used for matching the packets to the class whose index is specified. This command is also used to enter the class-map configuration mode. The no form of this command is used to delete an existing class map and to return to global configuration mode.

```
class-map <class-map-number (1-65535) >
```

```
no class-map <class-map-number (1-65535) >
```

**Syntax Description**      **class-map-number**      -      QoS class map number

**Mode**                      Global Configuration Mode

**Package**                  Workgroup, Enterprise and Metro

**Example**                  `iss(config)# class-map 5`



- Differentiated services must have been enabled in the device.
- The `class-map` command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-interface basis.
- The `match` command is available from the class-map configuration mode.

**Related Command**      `show class-map` - Displays quality of service (QoS) class maps

### 66.4.3 policy-map

This command is used to enter the policy-map configuration mode. In the policy-map configuration mode the user can create or modify a policy map. The no form of this command deletes an existing policy map and returns to the global configuration mode.

```
policy-map <policy-map-number (1-65535)>
```

```
no policy-map <policy-map-number (1-65535)>
```

**Syntax Description**     **policy-map-number** - QoS Policy map number

**Mode**                 Global Configuration Mode

**Package**             Workgroup, Enterprise and Metro

**Example**             iss(config)# policy-map 6



- Differentiated services must have been enabled in the device.
- The following two commands are available from the policy-map configuration mode:
  1. **class**
  2. **exit** - Exits from the policy map configuration mode and returns to the global configuration mode.

**Related Command**     **show policy-map** - Displays quality of service (QoS) policy maps

## 66.4.4 match

This command specifies the fields in the incoming packets that are to be examined for the classification of the packets. The IP access group / MAC access group can be used as match criteria.

```
match access-group { mac-access-list | ip-access-list } <acl-index-num (1-65535) >
```

|                           |                        |                                                                                                                                                                                                 |
|---------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <b>mac-access-list</b> | - Access list created based on MAC addresses for non-IP traffic                                                                                                                                 |
|                           | <b>ip-access-list</b>  | - Access list created based on IP addresses. The IP-access list can either be defined as a standard IP-access list or an extended IP-access list.                                               |
|                           | <b>acl-index-num</b>   | - Specifies the ACL index range. The ACL index range for an IP standard ACL is 1 to 1000 and IP extended ACL is 1001 to 65535.<br><br>The ACL index range for a MAC extended ACL is 1 to 65535. |

**Mode** Class Map Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss (config-cmap)# match access-group mac-access-list 5`



- Differentiated services must have been enabled in the device.
- MAC access list and IP access list must have been configured.

**Related Commands**

- **class-map** - Creates a class map to be used for matching the packets with the class whose name/index is specified
- **show class-map** - Displays QoS Class maps

## 66.4.5 class

This command defines a traffic classification for the policy to act. The class-map-number that is specified in the policy map ties the characteristics for that class to the class map and its match criteria, as configured by using the class-map global configuration command. On execution of the class command, the switch enters the policy-map class configuration mode.

The no form of this command un-maps the class-map from the current policy-map configuration.

```
class <class-map-number (1-65535)>
```

```
no class <class-map-number (1-65535)>
```

**Syntax Description**      **class-map-number**      -      Class Map Number

**Mode**                      Policy-Map Configuration Mode

**Package**                  Workgroup, Enterprise and Metro

**Example**                  `iss (config-pmap)# class 5`



- Differentiated services must have been enabled in the device.
- The policy-map global configuration command must be executed prior to using the class command. After a policy map is specified, the user can either configure a policy for new classes or modify a policy for any existing classes in that policy map.
- The following configuration commands are available from the policy map class configuration mode:

```
set cos
```

- Related Commands**
- **policy-map** - Enters the policy map configuration mode
  - **show policy-map** - Displays the QoS policy maps

## 66.4.6 set cos

This command defines the in-profile action by setting a class of service (CoS), Differentiated Services Code Point (DSCP), or IP-precedence value in the packet.

The no form of the command deletes the configured values.

```
set {cos <new-cos(0-7)> | ip dscp <new-dscp(0-63)> | ip precedence <new-
precedence(0-7)>}
```

```
no set {cos <new-cos(0-7)> | ip { dscp <new-dscp(0-63)> | precedence <new-
precedence(0-7)>}}
```

|                           |                      |   |                                                            |
|---------------------------|----------------------|---|------------------------------------------------------------|
| <b>Syntax Description</b> | <b>cos</b>           | - | New COS value assigned to the classified traffic           |
|                           | <b>ip dscp</b>       | - | New DSCP value assigned to the classified traffic          |
|                           | <b>ip precedence</b> | - | New IP-precedence value assigned to the classified traffic |

**Mode** Policy-Map Class Configuration Mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss (config-pmap-c)# set cos 5`



To attach policy maps that contain the following elements to an ingress interface

- set policy-map class configuration commands must be used. Moreover, the police policy-map class configuration command can be used to mark down (reduce) the DSCP value at the ingress interface.
- Access control list (ACL) classification.
- Per-port per-VLAN classification.

- Related Commands**
- **class** - Defines a traffic classification for the policy set
  - **policy-map** - Used to enter the policy map configuration mode
  - **class-map** - Creates a class map
  - **show policy-map** - Displays the QoS policy map configuration

## 66.4.7 shutdown qos

This command shuts down the Quality-of-Service operation. The no form of the command starts and enables the Quality-of-Service operation.

**shutdown qos**

**no shutdown qos**

|                 |                                        |
|-----------------|----------------------------------------|
| <b>Mode</b>     | Global Configuration Mode              |
| <b>Package</b>  | Workgroup, Enterprise and Metro        |
| <b>Defaults</b> | QoS is started and enabled by default  |
| <b>Example</b>  | <code>iss(config)# shutdown qos</code> |



- When shutdown, all the pools used by DiffServ module will be released to the system.
- When started, the resources required by DiffServ module are allocated and the module starts running.

|                         |                                                                                                                                                                                                                         |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Related Commands</b> | <ul style="list-style-type: none"><li>• <code>show policy-map</code> - Displays the quality of service (QoS) policy maps</li><li>• <code>show class-map</code> - Displays quality of service (QoS) class maps</li></ul> |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 66.4.8 cosq scheduling algorithm

This command sets cosq scheduling algorithm.

```
cosq scheduling algorithm { strict | rr | wrr | wfq | strict-rr | strict-wrr |
strict-wfq | deficit }
```

|                           |                   |                                 |
|---------------------------|-------------------|---------------------------------|
| <b>Syntax Description</b> | <b>strict</b>     | - strict                        |
|                           | <b>rr</b>         | - round robin                   |
|                           | <b>wrr</b>        | - weighted round robin          |
|                           | <b>wfq</b>        | - weighted fair queing          |
|                           | <b>strict-rr</b>  | - strict - round robin          |
|                           | <b>strict-wrr</b> | - strict - weighted round robin |
|                           | <b>strict-wfq</b> | - strict - weighted fair queing |
|                           | <b>deficit</b>    | - deficit                       |

**Mode** Interface Configuration mode

**Package** Workgroup, Enterprise and Metro

**Example** `iss(config-if)# cosq scheduling algorithm strict`

**Related Commands**

- **show cosq algorithm** - Displays the CoSq algorithm used for the interface.
- **show cosq weights-bw** - Displays the CoSq weights and the bandwidth for the interface.

## 66.4.9 traffic class

This command sets weight and bandwidth for traffic classes.

```
traffic-class <integer(0-7)> weight <integer(0-15)> [ minbandwidth <integer(1-262143)>]
```

|                           |                      |   |                              |
|---------------------------|----------------------|---|------------------------------|
| <b>Syntax Description</b> | <b>traffic-class</b> | - | Configures cosq numbers      |
|                           | <b>weight</b>        | - | Configures cosq weights      |
|                           | <b>minbandwidth</b>  | - | Configures minimum bandwidth |

**Mode** Interface Configuration mode

**Package** Workgroup, Enterprise and Metro

**Defaults** **weight** - 1

**Example** `iss(config-if)# traffic-class 1 weight 7 minbandwidth 1234`

**Related Commands**

- **show cosq algorithm** - Displays the CoSq algorithm used for the interface.
- **show cosq weights-bw** - Displays the CoSq weights and the bandwidth for the interface.

## 66.4.10 show policy-map

This command displays the quality of service (QoS) policy maps, which defines the classification criteria for the incoming traffic. Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

```
show policy-map [<policy-map-num(1-65535)> [class <class-map-num(1-65535)>]]
```

|                           |                       |                     |
|---------------------------|-----------------------|---------------------|
| <b>Syntax Description</b> | <b>policy-map-num</b> | - Policy map number |
|                           | <b>class</b>          | - Class map number  |

**Mode** Privileged/User EXEC Mode

**Package** Workgroup, Enterprise and Metro

**Example** iss# show policy-map 24

```
DiffServ Configurations:
-----
Quality of Service has been enabled
Policy Map 24 is not active
Class Map: 20
-----
Protocol                               : 255
In Profile Entry
-----
In profile action                       : policed-precedence 5
Out Profile Entry
-----
Metering on
burst bytes/token size                  : 6
Refresh count                           : 1000
Out profile action                       : drop
No Match Entry
-----
No match action                         : policed-precedence 5
```

**Related Commands**

- **policy-map** - Used to enter the policy map configuration mode

- **class** - Defines a traffic classification for the policy to act
- **set cos** - Defines the in-profile action by setting a CoS, DSCP or IP-precedence value in the packet

## 66.4.11 show class-map

This command displays quality of service (QoS) class maps, which defines the match criteria to classify traffic.

```
show class-map [<class-map-num(1-65535)>]
```

**Syntax Description**     **class-map-num**     -     Displays the configured class map number

**Mode**     Privileged/User EXEC Mode

**Package**     Workgroup, Enterprise and Metro

**Example**     iss# show class-map

```
DiffServ Configurations:
-----
```

```
Class map 20
-----
```

```
Filter-ID                             : 3
Filter-Type                           : IP-Filter
```

**Related Commands**

- **class-map** - Creates a class map that is meant to be used for matching the packets to the class whose index is specified
- **match** - Specifies the fields in the incoming packets that are to be examined for the classification of the packets

## 66.4.12 show cosq algorithm

This command displays the CoSq algorithm used for the interface.

```
show cosq algorithm [ interface <interface-type> <interface-id> ]
```

**Syntax Description**     **interface-type**     -   Interface Type

**interface-id**         -   Interface ID

**Mode**                    Global Configuration Mode

**Package**                Workgroup, Enterprise and Metro

**Example**                iss(config)# show cosq algorithm interface gigabitethernet  
0/1

CoSq Algorithm

```
-----  
Interface            Algorithm  
-----  
Gi0/1                StrictPriority  
.....  
.....  
-----
```

## 66.4.13 show cosq weights-bw

This command displays the CoSq weights and the bandwidth for the interface.

```
show cosq weights-bw [ interface <interface-type> <interface-id> ]
```

**Syntax Description**     **interface-type**     -   Interface Type

**interface-id**        -   Interface ID

**Mode**                    Global Configuration Mode

**Package**                Workgroup, Enterprise and Metro

**Example**                iss(config)# show cosq weights-bw interface gigabitethernet  
0/1

CoSq Weights and Bandwidths

```
-----
```

| Interface | CoSqId | CoSqWeight | MinBw | MaxBw | Flag |
|-----------|--------|------------|-------|-------|------|
| Gi0/1     | 0      | 1          | 0     | 0     | 2    |
| Gi0/1     | 1      | 1          | 0     | 0     | 2    |
| Gi0/1     | 2      | 1          | 0     | 0     | 2    |
| Gi0/1     | 3      | 1          | 0     | 0     | 2    |
| Gi0/1     | 4      | 1          | 0     | 0     | 2    |
| Gi0/1     | 5      | 1          | 0     | 0     | 2    |
| Gi0/1     | 6      | 1          | 0     | 0     | 2    |
| Gi0/1     | 7      | 1          | 0     | 0     | 2    |
| .....     | ...    | ..         | ...   | ...   | ...  |

```
-----
```

# Your Opinion Matters

---

Dear Reader:

We aspire to provide you with important information, delivered efficiently. If this guide has been informative, useful, and effective, your satisfaction is our reward. If not, tell us how it can be improved. Your valuable input will help us understand your information needs better.

Please fill up the form provided below and mail it to us at the address provided on the Copyright page.

**Did you find the INFORMATION provided in this guide:**

Complete  Y  N Accurate  Y  N  
Relevant  Y  N Well-organised  Y  N  
Other: .....

**Did you find the LANGUAGE used in this guide:**

Easy to understand  Y  N Correct  Y  N  
Consistent  Y  N Professional  Y  N  
Other: .....

**Did you find the TONE used in the delivery:**

Appropriate  Y  N Professional  Y  N  
Other: .....

**Did you find the ILLUSTRATIONS provided in the guide:**

Relevant  Y  N Easy to understand  Y  N  
Other: .....

**Did you find the PAGE LAYOUT:**

Aesthetically pleasing  Y  N Crowded  Y  N  
Other: .....

**What improvements do you recommend for this document?**

---

---

---

Document No. INTERFACE MASTERS: ISSCLlum\_Vol7/20101001

Thank you for participating in our quest for total customer satisfaction.



## Revision History

---

|                      |                                              |
|----------------------|----------------------------------------------|
| ISS                  | Revision Number: 28.0                        |
| CLI User Manual_Vol7 | INTERFACE MASTERS:<br>ISSCLlum_Vol7/20101001 |
| 28-09-2010           |                                              |
| Path:                |                                              |

|  |  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--|--|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  |  |  | <p>All ISSCLlums (Base, Enterprise, Metro, BCM, CXE, Marvell 6095 and xCAT) are merged as single user manual split across volumes.</p> <p>It includes the:</p> <ul style="list-style-type: none"> <li>• Content enhancement done in base and Marvell 6095 CLI documents of ISS610.</li> <li>• ACL metro specific syntaxes are added for all targets and Linux environment.</li> <li>• Set sizing parameters and show sizing parameters commands are included in PBB and a note is provided to denote that these commands are obsoleted from the release ISS630.</li> <li>• The comments provided in the BGP section are deleted as the changes mentioned orally by the SME are baselined using the RFC ID 36923.</li> <li>• Updates mentioned in the RFC 38828, 34546, 38995 and 38569</li> </ul> |
|--|--|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|