

Interface Masters

◀ TECHNOLOGIES ▶

Innovative Network Solutions

ISS

CLI User Manual_Vol1

INTERFACE MASTERS: ISSCLlum_Vol1/20101001

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.

DOCUMENT No.: INTERFACE MASTERS: ISSCLlum_Vol1/20101001

Contents

	FIGURES	9
CHAPTER 1:	INTRODUCTION	11
	1.1 PURPOSE	11
	1.2 SCOPE	11
	1.3 DOCUMENT CONVENTIONS	12
	1.3.1 Industry Standard CLI	12
	1.4 CONTENT ORGANIZATION AND TRACEABILITY	12
	1.4.1 Volume-Wise Split Details	12
	1.4.2 Updates Traceability Matrix	14
	1.5 KEY CONVENTIONS	17
	1.5.1 Keyboard Shortcuts	17
	1.5.2 Others	17
CHAPTER 2:	COMMAND LINE INTERFACE	19
	2.1 CONTEXT SENSITIVE HELP	20
	2.2 CLI COMMAND MODES	21
	2.3 USER EXEC MODE	23
	2.4 PRIVILEGED EXEC MODE	23
	2.5 GLOBAL CONFIGURATION MODE	23
	2.6 SWITCH CONFIGURATION MODE	23
	2.7 INTERFACE CONFIGURATION MODE	23
	2.7.1 Physical Interface Mode	23
	2.7.2 Port Channel Interface Mode	23
	2.7.3 VLAN Interface Mode	24
	2.7.4 Tunnel Interface Mode	24
	2.7.5 Out of Band Interface Mode	24
	2.8 CONFIG-VLAN MODE	24
	2.9 LINE CONFIGURATION MODE	24
	2.10 BOOT CONFIGURATION MODE	24
	2.11 REDUNDANCY CONFIGURATION MODE	24
	2.12 PROFILE CONFIGURATION MODE	25
	2.13 PROTOCOL SPECIFIC MODES	25
	2.13.1 PIM Component Mode	25
	2.13.2 Router Configuration Mode	25
	2.13.3 VRRP Router Configuration Mode	25
	2.13.4 VRRP Interface Configuration Mode	25
	2.13.5 DHCP Pool Configuration Mode	26
	2.13.6 Crypto Transform Configuration Mode	26
	2.13.7 MPLS LDP mode	26
	2.13.8 MPLS LDP Entity mode	26
	2.13.9 RSVP Configuration Mode	26
	2.13.10 RSVP Interface Configuration Mode	26
	2.13.11 Route Map Configuration Mode	27
	2.13.12 SNMP Configuration Mode	27
	2.13.13 Client Information Configuration Mode	27
	2.13.14 IPv6 DHCP Pool Configuration Mode	27
	2.13.15 Vendor Specific Information Configuration Mode	27
	2.13.16 ECFM Configuration Mode	27
	2.13.17 MSTP Configuration mode	28
	2.13.18 Service Instance Configuration Mode	28

	2.13.19 TE Service Instance Mode	28
	2.13.20 Protection Group Configuration Mode	28
	2.13.21 DiffSrv ClassMap Configuration mode.....	28
	2.13.22 DiffSrv Policy-Map Configuration Mode	28
	2.13.23 DiffSrv Policy-Map Class Configuration Mode	29
	2.13.24 ACL Standard Access List Configuration Mode	29
	2.13.25 ACL Extended Access List Configuration Mode.....	29
	2.13.26 ACL MAC Configuration Mode	29
CHAPTER 3:	SYSTEM COMMANDS	31
	3.1 HELP	33
	3.2 CLEAR SCREEN.....	34
	3.3 ENABLE	35
	3.4 DISABLE.....	36
	3.5 CONFIGURE TERMINAL.....	37
	3.6 CONFIGURE.....	38
	3.7 RUN SCRIPT	39
	3.8 LISTUSER.....	40
	3.9 LOCK.....	41
	3.10 USERNAME.....	42
	3.11 ENABLE PASSWORD	44
	3.12 LINE	45
	3.13 ALIAS - REPLACEMENT STRING.....	46
	3.14 ALIAS – INTERFACE EXEC CONFIGURE	47
	3.15 ACCESS-LIST PROVISION MODE.....	48
	3.16 ACCESS-LIST COMMIT	49
	3.17 EXEC-TIMEOUT	50
	3.18 LOGOUT.....	51
	3.19 END	52
	3.20 EXIT	53
	3.21 SHOW PRIVILEGE	54
	3.22 SHOW LINE.....	55
	3.23 SHOW ALIASES	56
	3.24 SHOW USERS	57
	3.25 SHOW HISTORY.....	58
CHAPTER 4:	SYSTEM FEATURES	59
	4.1 DEFAULT MODE.....	62
	4.2 DEFAULT RESTORE-FILE	63
	4.3 DEFAULT VLAN ID	64
	4.4 DEFAULT IP ADDRESS	65
	4.5 IP ADDRESS	67
	4.6 SWITCHPORT.....	69
	4.7 DEFAULT IP ADDRESS ALLOCATION PROTOCOL	70
	4.8 IP ADDRESS - RARP/DHCP	72
	4.9 BASE-MAC.....	74
	4.10 LOGIN AUTHENTICATION	75
	4.11 LOGIN AUTHENTICATION-DEFAULT <LIST-NAME>	76
	4.12 AUTHORIZED-MANAGER IP-SOURCE.....	77
	4.13 IP HTTP PORT	79
	4.14 SET IP HTTP	80
	4.15 ARCHIVE DOWNLOAD-SW	81
	4.16 INTERFACE-CONFIGURATION AND DELETION	82
	4.17 MTU FRAME SIZE	85
	4.18 SYSTEM MTU	86
	4.19 LOOPBACK LOCAL	87
	4.20 BRIDGE PORT-TYPE.....	88

4.21	SYSTEM-SPECIFIC PORT-ID	91
4.22	SET CUSTOM-PARAM	92
4.23	MAC-ADDR	93
4.24	SNMP TRAP LINK-STATUS	94
4.25	WRITE	95
4.26	COPY	96
4.27	COPY STARTUP-CONFIG	97
4.28	COPY RUNNING-CONFIG STARTUP-CONFIG	98
4.29	COPY LOGS	99
4.30	FIRMWARE UPGRADE.....	100
4.31	COPY - FILE	101
4.32	CLOCK SET.....	102
4.33	ERASE	103
4.34	CLI CONSOLE.....	104
4.35	FLOWCONTROL.....	105
4.36	TUNNEL MODE	106
4.37	TUNNEL CHECKSUM.....	107
4.38	TUNNEL PATH-MTU-DISCOVERY	108
4.39	TUNNEL UDLR	109
4.40	SHUTDOWN - PHYSICAL/VLAN/PORT-CHANNEL/TUNNEL INTERFACE.....	110
4.41	DEBUG INTERFACE	112
4.42	DEBUG-LOGGING	113
4.43	INCREMENTAL-SAVE	114
4.44	AUTO-SAVE TRIGGER.....	115
4.45	ROLLBACK	116
4.46	SHUTDOWN OSPF OSPF3 BGP ISIS.....	117
4.47	START OSPF OSPF3 BGP ISIS.....	118
4.48	SET SWITCH MAXIMUM - THRESHOLD	119
4.49	SET SWITCH TEMPERATURE - THRESHOLD.....	120
4.50	SET SWITCH POWER - THRESHOLD	121
4.51	MAC-LEARN-RATE	122
4.52	SYSTEM CONTACT	123
4.53	SYSTEM LOCATION	124
4.54	CLEAR INTERFACES - COUNTERS	125
4.55	CLEAR COUNTERS.....	126
4.56	SHOW IP INTERFACE.....	127
4.57	SHOW AUTHORIZED-MANAGERS.....	129
4.58	SHOW INTERFACES	130
4.59	SHOW INTERFACES - COUNTERS.....	134
4.60	SHOW SYSTEM-SPECIFIC PORT-ID	137
4.61	SHOW CUSTOM-PARAM.....	138
4.62	SHOW INTERFACE MTU	139
4.63	SHOW INTERFACE BRIDGE PORT-TYPE	141
4.64	SHOW NVRAM.....	143
4.65	SHOW ENV	145
4.66	SHOW SYSTEM INFORMATION	147
4.67	SHOW FLOW-CONTROL	148
4.68	SHOW DEBUG-LOGGING	149
4.69	SHOW DEBUGGING	150
4.70	SHOW CLOCK	151
4.71	SHOW RUNNING-CONFIG	152
4.72	SHOW HTTP SERVER STATUS.....	158
4.73	SHOW SYSTEM ACKNOWLEDGEMENT	159
4.74	SHOW MAC-LEARN-RATE.....	160
4.75	PORT-ISOLATION IN_VLAN_ID	161
4.76	SHOW PORT-ISOLATION	162

	4.77 ENTITY MIB	163
	4.77.1 set entity physical-index	164
	4.77.2 show entity logical.....	166
	4.77.3 show entity physical	167
	4.77.4 show entity lp-mapping	168
	4.77.5 show entity alias-mapping.....	169
	4.77.6 show entity phy-containment.....	170
	4.78 TARGET SPECIFIC COMMANDS.....	171
	4.78.1 reload	172
	4.78.2 monitor session - source	173
	4.78.3 monitor session - destination.....	175
	4.78.4 no monitor session.....	176
	4.78.5 negotiation.....	177
	4.78.6 speed	178
	4.78.7 duplex.....	179
	4.78.8 storm-control.....	180
	4.78.9 rate-limit-output.....	181
	4.78.10 show monitor - local / range / all.....	182
	4.78.11 show monitor records.....	185
	4.78.12 show monitor	186
	4.79 BCM SPECIFIC COMMANDS.....	187
	4.79.1 storm-control.....	188
	4.79.2 rate-limit-output.....	189
	4.80 CXE SPECIFIC COMMANDS	190
	4.80.1 storm-control.....	191
	4.81 MARVELL 6095 SPECIFIC COMMANDS	192
	4.81.1 storm-control.....	193
	4.81.2 rate-limit-output.....	194
	4.82 XCAT SPECIFIC COMMANDS.....	195
	4.82.1 storm-control.....	196
	4.82.2 rate-limit-output.....	197
CHAPTER 5:	VCM	199
	5.1 IP VRF	200
	5.2 IP VRF FORWARDING	202
	5.3 SWITCH	203
	5.4 MAP SWITCH.....	204
	5.5 SET OWNER	206
	5.6 SHOW IP VRF	207
	5.7 SHOW SWITCH.....	208
	5.8 SHOW OWNER	210
	5.9 SHOW SWITCH MAP INFO.....	211
	5.10 SISP	212
	5.10.1 shutdown switch-instance-shared-port	213
	5.10.2 switch-instance-shared-port	214
	5.10.3 map sisp.....	215
	5.10.4 show switch-instance-shared-port	216
	5.10.5 show switch-instance-shared-port vlan info	217
CHAPTER 6:	RADIUS	219
	6.1 RADIUS-SERVER HOST	220
	6.2 DEBUG RADIUS	222
	6.3 SHOW RADIUS SERVER	223
	6.4 SHOW RADIUS STATISTICS.....	224
CHAPTER 7:	TACACS	225
	7.1 TACACS-SERVER HOST	226

	7.2	TACACS USE-SERVER ADDRESS	228
	7.3	TACACS-SERVER RETRANSMIT	229
	7.4	DEBUG TACACS	230
	7.5	SHOW TACACS.....	231
CHAPTER 8:	SSH		233
	8.1	IP SSH	234
	8.2	SSH.....	235
	8.3	DEBUG SSH	236
	8.4	SHOW IP SSH.....	237
CHAPTER 9:	SSL		239
	9.1	IP HTTP SECURE	240
	9.2	SSL GEN CERT-REQ ALGO RSA SN	242
	9.3	SSL SERVER-CERT	243
	9.4	DEBUG SSL	244
	9.5	SHOW SSL SERVER-CERT	245
	9.6	SHOW IP HTTP SECURE SERVER STATUS	247
CHAPTER 10:	SNTP		249
	10.1	SNTP	251
	10.2	SET SNTP CLIENT	253
	10.3	SET SNTP CLIENT VERSION	254
	10.4	SET SNTP CLIENT ADDRESSING MODE	255
	10.5	SET SNTP CLIENT PORT	257
	10.6	SET SNTP CLIENT CLOCK-FORMAT	258
	10.7	SET SNTP CLIENT TIME ZONE	259
	10.8	SET SNTP CLIENT CLOCK-SUMMER-TIME	260
	10.9	SET SNTP CLIENT AUTHENTICATION-KEY	261
	10.10	SET SNTP UNICAST-SERVER AUTO-DISCOVERY	262
	10.11	SET SNTP UNICAST-POLL-INTERVAL	263
	10.12	SET SNTP UNICAST-MAX-POLL-TIMEOUT	264
	10.13	SET SNTP UNICAST-MAX-POLL-RETRY	265
	10.14	SET SNTP UNICAST-SERVER	266
	10.15	SET SNTP BROADCAST-MODE SEND-REQUEST	267
	10.16	SET SNTP BROADCAST-POLL-TIMEOUT	268
	10.17	SET SNTP BROADCAST-DELAY-TIME	269
	10.18	SET SNTP MULTICAST-MODE SEND-REQUEST	270
	10.19	SET SNTP MULTICAST-POLL-TIMEOUT	271
	10.20	SET SNTP MULTICAST-DELAY-TIME	272
	10.21	SET SNTP MULTICAST-GROUP-ADDRESS	273
	10.22	SET SNTP ANYCAST-POLL-INTERVAL	274
	10.23	SET SNTP ANYCAST-POLL-TIMEOUT	275
	10.24	SET SNTP ANYCAST-POLL-RETRY-COUNT	276
	10.25	SET SNTP ANYCAST-SERVER	277
	10.26	SHOW SNTP CLOCK	278
	10.27	SHOW SNTP STATUS.....	279
	10.28	SHOW SNTP UNICAST-MODE STATUS.....	280
	10.29	SHOW SNTP BROADCAST-MODE STATUS	281
	10.30	SHOW SNTP MULTICAST-MODE STATUS	282
	10.31	SHOW SNTP ANYCAST-MODE STATUS.....	283
	10.32	DEBUG SNTP	284
CHAPTER 11:	SNMPV3		285
	11.1	ENABLE SNMPSUBAGENT	288
	11.2	DISABLE SNMPSUBAGENT	289
	11.3	ENABLE SNMPAGENT	290
	11.4	DISABLE SNMPAGENT	291

11.5	SNMP COMMUNITY INDEX	292
11.6	SNMP GROUP	294
11.7	SNMP ACCESS	296
11.8	SNMP ENGINEID	298
11.9	SNMP PROXY NAME	299
11.10	SNMP MIBPROXY NAME	301
11.11	SNMP VIEW	302
11.12	SNMP TARGETADDR	305
11.13	SNMP TARGETPARAMS.....	307
11.14	SNMP USER.....	310
11.15	SNMP NOTIFY	312
11.16	SNMP FILTERPROFILE	314
11.17	SNMP-SERVER ENABLE TRAPS SNMP AUTHENTICATION	315
11.18	SNMP-SERVER TRAP UDP-PORT	316
11.19	SNMP-SERVER TRAP PROXY-UDP-PORT	317
11.20	SNMP AGENT PORT	318
11.21	SNMP TCP ENABLE	319
11.22	SNMP TRAP TCP ENABLE	320
11.23	SNMP-SERVER TCP-PORT	321
11.24	SNMP-SERVER TRAP TCP-PORT	322
11.25	SNMP-SERVER ENABLE TRAPS	323
11.26	SHOW SNMP AGENTX INFORMATION	324
11.27	SHOW SNMP AGENTX STATISTICS.....	325
11.28	SHOW SNMP.....	326
11.29	SHOW SNMP COMMUNITY	327
11.30	SHOW SNMP GROUP	328
11.31	SHOW SNMP GROUP ACCESS.....	329
11.32	SHOW SNMP ENGINEID	330
11.33	SHOW SNMP PROXY	331
11.34	SHOW SNMP MIBPROXY	332
11.35	SHOW SNMP VIEWTREE.....	333
11.36	SHOW SNMP TARGETADDR	334
11.37	SHOW SNMP TARGETPARAM	335
11.38	SHOW SNMP USER	336
11.39	SHOW SNMP NOTIF.....	337
11.40	SHOW SNMP INFORM STATISTICS	338
11.41	SHOW SNMP-SERVER TRAPS	339
11.42	SHOW SNMP-SERVER PROXY-UDP-PORT	340
11.43	SHOW SNMP TCP.....	341
11.44	SHOW SNMP FILTER.....	342
CHAPTER 12:	SYSLOG	343
12.1	LOGGING	345
12.2	LOGGING SYNCHRONOUS.....	347
12.3	MAILSERVER	349
12.4	SENDER MAIL-ID.....	350
12.5	CMDBUFFS	351
12.6	CLEAR LOGS.....	352
12.7	SYSLOG MAIL.....	353
12.8	SYSLOG LOCAL STORAGE.....	354
12.9	SYSLOG FILENAME-ONE	355
12.10	SYSLOG FILENAME-TWO.....	356
12.11	SYSLOG FILENAME-THREE.....	357
12.12	SYSLOG RELAY - PORT	358
12.13	SYSLOG PROFILE	359
12.14	LOGGING-FILE	360

	12.15 LOGGING SERVER	361
	12.16 SYSLOG RELAY	362
	12.17 SYSLOG RELAY TRANSPORT TYPE	363
	12.18 SHOW LOGGING	364
	12.19 SHOW EMAIL ALERTS	365
	12.20 SHOW SYSLOG ROLE	366
	12.21 SHOW SYSLOG MAIL	367
	12.22 SHOW SYSLOG LOCALSTORAGE	368
	12.23 SHOW LOGGING-FILE	369
	12.24 SHOW LOGGING-SERVER	370
	12.25 SHOW MAIL-SERVER	371
	12.26 SHOW SYSLOG RELAY-PORT	372
	12.27 SHOW SYSLOG PROFILE	373
	12.28 SHOW SYSLOG RELAY TRANSPORT TYPE	374
	12.29 SHOW SYSLOG FILE-NAME	375
	12.30 SHOW SYSLOG INFORMATION	376
CHAPTER 13:	TCP	377
	13.1 SHOW TCP STATISTICS	378
	13.2 SHOW TCP CONNECTIONS	379
	13.3 SHOW TCP LISTENERS	381
	13.4 SHOW TCP RETRANSMISSION DETAILS	382
CHAPTER 14:	UDP	383
	14.1 SHOW UDP STATISTICS	384
	14.2 SHOW UDP CONNECTIONS	386
CHAPTER 15:	POE	389
	15.1 SET POE	390
	15.2 POWER INLINE MAC-ADDRESS	391
	15.3 POWER INLINE	392
	15.4 POWER INLINE PRIORITY	393
	15.5 SHOW POWER DETAIL	394
	15.6 SHOW POWER INLINE	395
	15.7 SHOW POE MAC-ADDRESS-LIST	397
CHAPTER 16:	L2 DHCP SNOOPING	399
	16.1 IP DHCP SNOOPING - GLOBAL COMMAND	400
	16.2 IP DHCP SNOOPING VERIFY MAC-ADDRESS	401
	16.3 IP DHCP SNOOPING - VLAN INTERFACE COMMAND	402
	16.4 IP DHCP SNOOPING TRUST	403
	16.5 SHOW IP DHCP SNOOPING GLOBALS	404
	16.6 SHOW IP DHCP SNOOPING VLAN	405
	16.7 DEBUG IP DHCP SNOOPING	406
CHAPTER 17:	IPDB	407
	17.1 IP BINDING	408
	17.2 IP SOURCE BINDING	410
	17.3 IP VERIFY SOURCE	412
	17.4 SHOW IP BINDING	413
	17.5 SHOW IP SOURCE BINDING	414
	17.6 SHOW IP BINDING COUNTERS	416
	17.7 SHOW IP VERIFY SOURCE	417
	17.8 DEBUG IP BINDING DATABASE	419

Figures

Figure 2-1: Command Modes Access Path 30

Chapter 1

Introduction

1.1 Purpose

Interface Masters ISS is a pre-integrated OEM ready software for managed Layer 2/Layer 3 switches, which performs switching between Ethernet ports at wire speed. **Interface Masters ISS** provides the basic bridging functionality and also offers advanced features such as link aggregation, GVRP/GMRP, IGMP Snooping and Network Access Control.

This document describes in detail the Base CLI commands supported by **Interface Masters ISS**. It is intended to be a reference manual for users and system administrators who will configure **Interface Masters ISS** through the CLI interface.

1.2 Scope

The scope of this document is limited to **Interface Masters ISS** release 6.1.0 and above. This document details all the Base CLI commands provided by the **Interface Masters ISS** software. Commands that are not applicable for a specific hardware platform are indicated wherever necessary.

1.3 Document Conventions

- The syntax of the CLI command is given in **Courier New 10 bold**.
- Elements in (< >) indicate the field required as input along with a CLI command, for example, < integer (100-1000)>.
- Elements in square brackets ([]) indicate optional fields for a command.
- Text in {} refers to either or group for the tokens given inside separated by a | symbol.
- The CLI command usage is given in Courier New 10 regular.
- Outputs and messages for CLI commands are given in Courier New 10 regular.
- The no form of the command resets a particular configuration to its default value or revokes the effect. This is explicitly explained in the description of the commands for which it is applicable.
- Any action that can change the switch configuration, conditionals and requirements for a command and information associated with significant details and functionality of a command is listed using the  symbol.

1.3.1 Industry Standard CLI

CLI commands are focused on performing specific operations. In order to provide a consistent, composable user experience, the CLI commands of Interface Masters protocols and solutions, have been modified to adhere to the Industry Standard CLI syntax. This enhancement is available for the code base using release after Interface Masters ISS 6.1.0.

The following approach is followed for updating the Industry Standard commands to this document.

- **Newly added commands** - A complete standardized implementation of the existing command is documented immediately after the relevant old command.
- **Newly added parameters** in the existing commands - If the existing command is modified for one or more parameters or values only, then the update is done inline by modifying the syntax with the new tokens.

1.4 Content Organization and Traceability

1.4.1 Volume-Wise Split Details

CLI Volume No:	Chapter No:	Chapter Title
I	1	Introduction
	2	Command Line Interface
	3	System Commands
	4	System Features
	5	VCM

CLI Volume No:	Chapter No:	Chapter Title
	6	RADIUS
	7	TACACS
	8	SSH
	9	SSL
	10	SNTP
	11	SNMPv3
	12	Syslog
	13	TCP
	14	UDP
	15	PoE
	16	L2 DHCP Snooping
17	IPDB	
II	18	STP
	19	LA
	20	LLDP
	21	PNAC
	22	MRP
	23	ELMI
	24	ELPS
	25	ERPS
	26	PBB
	27	PBB-TE
III	28	VLAN
	29	ECFM
	30	IPSecv6
	31	VRRP
IV	32	IP
	33	IPV6
	34	OSPF
	35	OSPFv3
	36	RRD
	37	RRD6
	38	MPLS
	39	Route Map
	40	NAT

CLI Volume No:	Chapter No:	Chapter Title
V	41	DHCP
	42	DHCPv6
	43	RIP
	44	RIPv6
	45	BGP
	46	ISIS
VI	47	IGMP Snooping
	48	MLD Snooping
	49	IGMP
	50	IGMP Proxy
	51	PIM
	52	PIMV6
	53	DVMRP
	54	IPv4 Multicasting
	55	TAC
	56	RMON
	57	RMON2
	58	DSMON
	59	EOAM
	60	FM
	61	RM
	62	PTP
63	Layer 4 Switching	
VII	64	QoS
	65	ACL
	66	Diffserv

1.4.2 Updates Traceability Matrix

Document Revision No / Product Release Version	Change Description
27.0 / ISS 6.3.0	Module: DCBX Change Type: Addition of New Module Document Volume No: 7. Section 64.3

Document Revision No / Product Release Version	Change Description
	Module: CN Change Type: Addition of New Module Document Volume No: 7. Section 64.3.2
	Module: L2 DHCP Snooping Change Type: Addition of New Module Document Volume No: 1. Section 16
	Module: PTP Change Type: Addition of New Module Document Volume No: 6. Section 62
	Module: IPDB Change Type: Addition of New Module Document Volume No: 1. Section 17
	Module: ACL Change Type: Updated for Traffic Rate Limit feature in Linux Environment Document Volume No: 7. Section 65.1.4, 65.1.10, 65.1.14, 65.1.16, 65.1.19, 65.1.22, 65.1.25 and 65.1.31
	Module: OSPFv2 Change Type: Updated for High Availability feature Document Volume No: 4. Section 34.58
	Module: OSPFv3 Change Type: Updated for High Availability feature Document Volume No: 4. Section 35.63
	Module: ERPS Change Type: Addition of New Module Document Volume No: 2. Section 25
28.0 / ISS 6.3.0	Module: PBB Change Type: Obsolete the show sizing parameters and set sizing parameters commands Document Volume No: 2. Section 26.4 and 26.39
	Module: ACL Change Type: Spell error in syntax is corrected for the traffic rate limit

Document Revision No / Product Release Version	Change Description
	<p>related commands Document Volume No: 7. Section 65.1.11, 65.1.13 and 65.1.14</p>
	<p>Module: ACL Change Type: Updated for inclusion of copy-to-cpu ipv6 command in Metro package for Linux environment Document Volume No: 7. Section 65.1.16</p>
	<p>Module: IGMP Snooping Change Type: Updated for Querier Functionality feature Document Volume No: 6. Section 47.18 to 47.20, 47.27</p>
	<p>Module: ISIS Change Type: Addition of New Module including GR feature, v4 and v6 support. Document Volume No: 5. Section 46</p>
	<p>Module: VLAN Change Type: Updated for private VLAN feature Document Volume No: 3. Section 28.40, 28.131 to 28.135</p>
	<p>Module: PIMv4 Change Type: Updated for High Availability feature Document Volume No: 6. Section 51.16, 51.30, 51.40, 51.41</p>
	<p>Module: PIMv6 Change Type: Updated for High Availability feature Document Volume No: 6 . Section 52.23, 52.33, 52.34</p>
	<p>Module: System Features Change Type: Updated for High Availability feature Document Volume No: 1. Section 4.75, 4.76</p>

1.5 Key Conventions

1.5.1 Keyboard Shortcuts

Up Arrow / Down Arrow	Displays the previously executed command.
Ctrl + C	Exits from the ISS prompt.
Backspace / Ctrl + H	Removes a single character.
TAB	Completes a command without typing the full word.
Left Arrow / Right Arrow	Traverses the current line.

1.5.2 Others

- **?** - helps to list the available command
- **q** - exits and returns to the ISS prompt
- **history** - displays the command history list

Chapter

2

Command Line Interface

This section describes the configuration of **Interface Masters ISS** using the Command Line Interface.

The Command Line Interface (CLI) can be used to configure the Intelligent Switch Solution from a console attached to the serial port of the switch or from a remote terminal using TELNET.

The **Interface Masters ISS** CLI supports a simple login authentication mechanism. The authentication is based on a user name and password provided by the user during login. The user "root" is created by default with password "admin123".

- A new user can be created or an existing user can be deleted, and the own password or password of the other users can be modified, only if login as a root user.

When **Interface Masters ISS** is started, the user name and password has to be given at the login prompt to access the CLI shell:

Interface Masters Intelligent Switch Solution

ISS Login:root

Password:*****

iss>

The **user-exec** mode is now available to the user. CLI command modes provide a detailed description of the various modes available for ISS.

ISS

-  The command prompt always displays the current mode.
-  CLI commands need not be fully typed. The abbreviated forms of CLI commands are also accepted by the **Interface Masters ISS** CLI. For example, commands like "show ip global config" can be typed as "sh ip gl co".
-  CLI commands are case insensitive.
-  CLI commands will be successful only if the dependencies are satisfied for a particular command that is issued. The general dependency is that the module specific commands are available only when the respective module is 'enabled'. Appropriate error messages will be displayed, if the dependencies are not satisfied.
 - The Ethernet type of an interface is determined during System Startup. While configuring interface-specific parameters, its Ethernet type needs to be specified correctly. A fastethernet interface cannot be configured as a gigabit-ethernet interface and vice-versa.

2.1 Context Sensitive Help

Interface Masters CLI framework offers context sensitive help; The user can type a question mark (?) anytime during a session to get help. The help can be invoked in several ways. It is not displayed as a whole and is available only for the specific token from where it is invoked.

Examples of possible scenarios are given below.

1. User keys in a character followed immediately by a question mark (?). This displays the current possible tokens without help string.

```
iss(config)# bo?
bootfile
```

2. User enters a keyword at the command prompt and enters a question mark (?) after hitting a space. This displays the next possible tokens along with the corresponding help string..

```
iss(config)# service ?
dhcp                DHCP related configuration
dhcp-relay          DHCP relay related configuration
dhcp-server         DHCP server related configuration
timestamps          Timestamp configuration for logged
                    messages
```

Some of the basic concepts implemented for the context sensitive help are:

1. The next possible tokens are listed only in the lexical order and not in the order as available in the syntax or command structure.
2. All possible tokens are listed along with the help string, even though the command is ambiguous. Any ambiguous command errors and value range errors are taken care only during the execution of the command.

Interface

3. The help tokens provided within <> brackets denotes that the user should input values of specified format. For example, <string(32)> represents that the user should input a string of size varying from 1 to 32.
4. The help tokens provided within () brackets denotes that the user should input only the values represented. For example, (1-4094) represents that the user should input value within the mentioned range alone.
5. The format is directly provided as help token for some non-keyword such as IP address, IP mask , MAC address and so on. For example, aa:aa:aa:aa:aa:aa represents that a MAC address of this format should be provided.
6. Only the most commonly used format is provided as help token for some non keywords such as IPv6 address. But the command supports most of the valid formats. For example, AAAA::BBBB represents the IPv6 address, but the command will accept the format AAAA:B::BBBB.
7. The help token <CR> along with help string explaining the operation of the command is displayed, if the command can be executed at that point (errors are handled only during the execution).

2.2 CLI command modes

The following table format lists the different CLI command modes.

Command Mode	Access Method	Prompt	Exit method
User EXEC	This is the initial mode to start a session.	iss>	The logout method is used.
Privileged EXEC	The User EXEC mode command enable is used to enter the Privileged EXEC mode.	iss#	To return from the Privileged EXEC mode to User EXEC mode the disable command is used.
Global Configuration	The Privileged EXEC mode command configure terminal is used to enter the Global Configuration mode	iss(config)#	To exit to the Privileged EXEC mode the end command is used.
Switch Configuration	The Global Configuration mode command switch <context_name> is used to enter the Switch Configuration mode.	iss(config-switch)#	To exit to the Global Configuration mode, the exit command is used and to exit to the Privileged EXEC mode, the end command is used.
Interface Configuration	The Global Configuration mode command interface <interface-type><interface-id> is used to enter the Interface configuration	iss(config-if)#	To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is

Command Mode	Access Method	Prompt	Exit method
	mode.		used.
Config-VLAN	The Global configuration mode command vlan vlan-id is used to enter the Config-VLAN mode.	iss(config-vlan) #	To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.
Line Configuration	The global configuration mode command line is used to enter the Line Configuration mode.	iss(config-line) #	To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.
Profile Configuration	The Global Configuration mode command ip mcast profile <profile-id> [description (128)] is used to enter the Profile Configuration mode.	iss(config-profile) #	To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.
Service Instance Configuration Mode	The Switch configuration mode command service-instance is used to enter the Config-SI mode.	iss(config-switch-si) #	To exit to the Switch configuration mode, the exit command is used.
TE Service Instance Mode	The Switch configuration mode command backbone traffic-engineering service-instance is used to enter the TE Service Instance Mode.	iss(config-switch-tesi) #	To exit to the Switch configuration mode, the exit command is used.
Protection group configuration mode	The Switch configuration mode command aps [linear] group <group-number> is used to enter the Protection group configuration mode.	iss(config-switch-pg) #	To exit to the Switch configuration mode, the exit command is used.

Interface

2.3 User EXEC Mode

After logging into the device, the user is automatically in the User EXEC mode. In general, the User EXEC commands are used to temporarily change terminal settings, perform basic tests and list system information.

2.4 Privileged EXEC Mode

Because many of the privileged commands set operating parameters, privileged access is password protected to prevent unauthorized use. The password is not displayed on the screen and is case sensitive. The Privileged EXEC mode prompt is the device name followed by the pound (#) sign.

2.5 Global Configuration Mode

Global Configuration commands apply to features that affect the system as a whole, rather to any specific interface.

2.6 Switch Configuration Mode

The switch configuration mode is used to perform switch specific operations for multiple instances. To enter into switch configuration mode from the global configuration mode, **switch <context_name>** command is used. To exit to the global configuration mode the **exit** command is used and to exit to the privileged EXEC mode the **end** command is used.

2.7 Interface Configuration Mode

To enter into Interface configuration mode from the Global Configuration mode, **interface <interface-type><interface-id>** command is used. To exit to the global configuration mode the **exit** command is used and to exit to the privileged EXEC mode the **end** command is used.

2.7.1 Physical Interface Mode

The Physical Interface mode is used to perform interface specific operations. To return to the global configuration mode the **exit** command is used.

2.7.2 Port Channel Interface Mode

The Port Channel Interface mode is used to perform port-channel specific operations. To return to the global configuration mode the **exit** command is used.

ISS

2.7.3 VLAN Interface Mode

The VLAN Interface mode is used to perform L3-IPVLAN specific operations. To return to the global configuration mode the **exit** command is used.

2.7.4 Tunnel Interface Mode

The Tunnel Interface mode is used to perform Tunnel specific operations. To return to the global configuration mode the **exit** command is used.

2.7.5 Out of Band Interface Mode

The Out of Band Interface mode is used to perform OOB interface specific operations. To return to the global configuration mode the **exit** command is used.

2.8 Config-VLAN Mode

This mode is used to perform VLAN specific operations. To enter into Config-VLAN mode from the global configuration mode, **vlan vlan-id** command is used. To return to the global configuration mode the **exit** command is used.

2.9 Line Configuration Mode

Line configuration commands modify the operations of a terminal line. These commands are used to change terminal parameter settings line by line or range of lines. To enter into Line Configuration mode from the global configuration mode, **line** command is used. To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.

2.10 Boot Configuration Mode

This mode is used to generate the Slot information (module type). The **reload** command is used to restart the switch.

2.11 Redundancy Configuration Mode

This mode is used to modify the redundancy parameters. To return to the global configuration mode the **exit** command is used.

Interface

2.12 Profile Configuration Mode

The profile configuration mode is used to perform profile specific operations. To enter into profile configuration mode from the global configuration mode, `ip mcast profile <profile-id> [description (128)]` command is used. To exit to the global configuration mode the `exit` command is used and to exit to the privileged EXEC mode the `end` command is used.

2.13 Protocol Specific Modes

2.13.1 PIM Component Mode

PIM component mode configures the PIM component. To enter into PIM Component mode from the Global Configuration mode, `ip pim comp<componentid>` command is used. To exit to the Global Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode the `end` command is used.

2.13.2 Router Configuration Mode

Router configuration mode is used to configure router protocol. To enter into Router configuration mode from the Global configuration mode, `router<router protocol>` command is used. To exit to the Global Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode the `end` command is used.

2.13.3 VRRP Router Configuration Mode

This mode is used for configuring the virtual router. To enter to this mode, the command `router vrrp` from the Global configuration mode is used. To exit to the Global Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode the `end` command is used.

2.13.4 VRRP Interface Configuration Mode

VRRP interface config mode is used to configure VRRP interfaces. To enter into this mode, `interface Vlan <vlan id>` command from VRRP router config mode is used. To exit to the Virtual Router Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode the `end` command is used.

ISS

2.13.5 DHCP Pool Configuration Mode

This mode is used to configure the network pool / host configurations of a subnet pool.

The Global configuration mode command `ip dhcp pool <integer(1-2147483647)>` creates a DHCP Server address pool and places the user in DHCP pool configuration mode. The prompt seen at this mode is `iss(dhcp-config)#`.

To return to the global configuration mode the `exit` command is used.

2.13.6 Crypto Transform Configuration Mode

Crypto Transform Configuration Mode is used to configure IPsecv6. To enter in to this mode `crypto ipsecv6` command from Global Configuration Mode is used. To exit to the Global Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode the `end` command is used.

2.13.7 MPLS LDP mode

MPLS LDP mode is used to configure LDP parameters. To enter into this mode, `mpls ldp` command from the Global Configuration mode is used. To exit to the MPLS LDP mode the `exit` command is used and to exit to the Privileged EXEC mode the `end` command is used.

2.13.8 MPLS LDP Entity mode

MPLS LDP Entity mode is used to configure LDP Entity parameters. To enter into this mode, `entity <entity_index (1-16)>` command from the MPLS LDP mode is used. To exit to the Global Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode the `end` command is used.

2.13.9 RSVP Configuration Mode

RSVP Configuration mode is used to configure RSVP parameters. To enter into this mode, `rsvp` command from the Global Configuration mode is used. To exit to the Global Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode the `end` command is used.

2.13.10 RSVP Interface Configuration Mode

RSVP Configuration mode is used to configure RSVP interfaces. To enter into this mode, `interface {vlan <vlan-id (1-4094)> | <interface-type> <interface-id>}` command from the RSVP Configuration mode is used. To exit to the RSVP Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode the `end` command is used.

Interface

2.13.11 Route Map Configuration Mode

Route Map Configuration mode is used to configure Route Map parameters. To enter into this mode, **route-map** <name(1-20)> [{**permit** | **deny** }] [<seqnum(1-10)>] command from the Global Configuration mode is used. To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.

2.13.12 SNTP Configuration Mode

SNTP Configuration mode is used to configure SNTP parameters. To enter into this mode, **sntp** command from the Global Configuration mode is used. The prompt seen at this mode is **iss(config-sntp)#**. To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.

2.13.13 Client Information Configuration Mode

Client Information Configuration mode is used to configure DHCPv6 client information at the server side. To enter into this mode, **ipv6 dhcp authentication server client-id** command is used from the Global Configuration mode. The prompt seen at this mode is **iss(config-d6clnt)#**. The **exit** command is used to exit to the Global Configuration mode and the **end** command is used to exit to the Privileged EXEC mode.

2.13.14 IPv6 DHCP Pool Configuration Mode

IPv6 DHCP Pool Configuration mode is used to configure DHCPv6 server address pool information. To enter into this mode, **ipv6 dhcp pool** command is used from the Global Configuration mode. The prompt seen at this mode is **iss(config-d6pool)#**. The **exit** command is used to exit to the Global Configuration mode and the **end** command is used to exit to the Privileged EXEC mode.

2.13.15 Vendor Specific Information Configuration Mode

Vendor Specific Information Configuration mode is used to configure vendor specific information. To enter into this mode, **vendor-specific** command is used from the IPv6 DHCP Pool Configuration mode. The prompt seen at this mode is **iss(d6pool-vendor)#**. The **exit** command is used to exit to the IPv6 DHCP Pool Configuration mode and the **end** command is used to exit to the Privileged EXEC mode.

2.13.16 ECFM Configuration Mode

This mode is used to perform the ECFM specific operations. To return to the global configuration mode the **exit** command is used.

ISS

2.13.17 MSTP Configuration mode

This mode is used to configure the MSTP specific parameters for the switch. The Global configuration mode command **spanning tree mst configuration** is used to enter the MSTP Configuration mode and. the prompt seen at this mode is **iss (config-mst) #**.

To return to the global configuration mode the **exit** command is used.

2.13.18 Service Instance Configuration Mode

The Service Instance Configuration mode is used to perform ISID specific operations. This mode is available inside Switch mode when ISS is running in MI (Multiple Instance) mode. To enter into this mode, **service instance <service-instance>** command from the Switch Configuration mode is used. To exit to the Service Instance Configuration mode, the **exit** command is used.

2.13.19 TE Service Instance Mode

The TE Service Instance mode is used to configure an ESP in a TESI. To enter into this mode, **backbone traffic-engineering service-instance <pbte-sid>** command from the Switch configuration mode is used. To exit to the Switch configuration mode, the **exit** command is used.

2.13.20 Protection Group Configuration Mode

The Protection group configuration mode is used to configure the parameters related to a particular protection group. The command **aps [linear] group <group-number>** is used in the Switch configuration mode to enter into the Protection group configuration mode. The command **exit** is used to exit to the Switch configuration mode.

2.13.21 DiffSrv ClassMap Configuration mode

The class-map global configuration command creates a class map to be used for matching the packets to the class whose index is specified and to enter the class-map configuration mode The Global configuration mode command **class-map <short (1-65535)>** is used to enter the DiffSrv ClassMap Configuration mode and. the prompt seen at this mode is **iss (config-cmap) #**.

To return to the global configuration mode the **exit** command is used.

2.13.22 DiffSrv Policy-Map Configuration Mode

In the Policy-Map Configuration mode the user can create or modify a policy map.

The Global configuration mode command **policy-map <short (1-65535)>** is used to enter the DiffSrv PolicyMap Configuration mode and the prompt seen at this mode is **iss (config-pmap) #**.

Interface

To return to the global configuration mode the **exit** command is used.

2.13.23 DiffSrv Policy-Map Class Configuration Mode

The Policy-Map Class Configuration command defines a traffic classification for the policy to act on. The class-map-num that is specified in the policy map ties the characteristics for that class and its match criteria as configured by using the **class-map** global configuration command to the class map. Once the **class** command is entered, the switch enters policy-map class configuration mode.

The DiffSrv Policy mode command **policy-map <short (1-65535)>** is used to enter the DiffSrv Policy-Map Class Configuration mode and the prompt seen at this mode is **iss(config-pmap-c) #**.

To return to the global configuration mode the **exit** command is used.

2.13.24 ACL Standard Access List Configuration Mode

Standard access lists create filters based on IP address and network mask only (L3 filters only).

The Global configuration mode command **ip access-list standard <(1-1000)>** creates IP ACLs and is used to enter the ACL Standard Access List Configuration mode. The prompt seen at this mode is **iss(config-std-nacl) #**.

To return to the global configuration mode the **exit** command is used.

2.13.25 ACL Extended Access List Configuration Mode

The Extended Access lists enables to specify filters based on the type of protocol, range of TCP/UDP ports as well as IP address and network mask (Layer 4 filters).

The Global configuration mode command **ip access-list extended <(1001-65535)>** is used to enter the ACL Extended Access List Configuration mode and the prompt seen at this mode is **iss(config-ext-nacl) #**.

To return to the global configuration mode the **exit** command is used.

2.13.26 ACL MAC Configuration Mode

The MAC access-list global configuration command creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user.

The Global configuration mode command **mac access-list extended <(1-65535)>** is used to enter the ACL MAC Configuration mode and the prompt seen at this mode is **iss(config-ext-macl) #**.

To return to the global configuration mode the **exit** command is used.

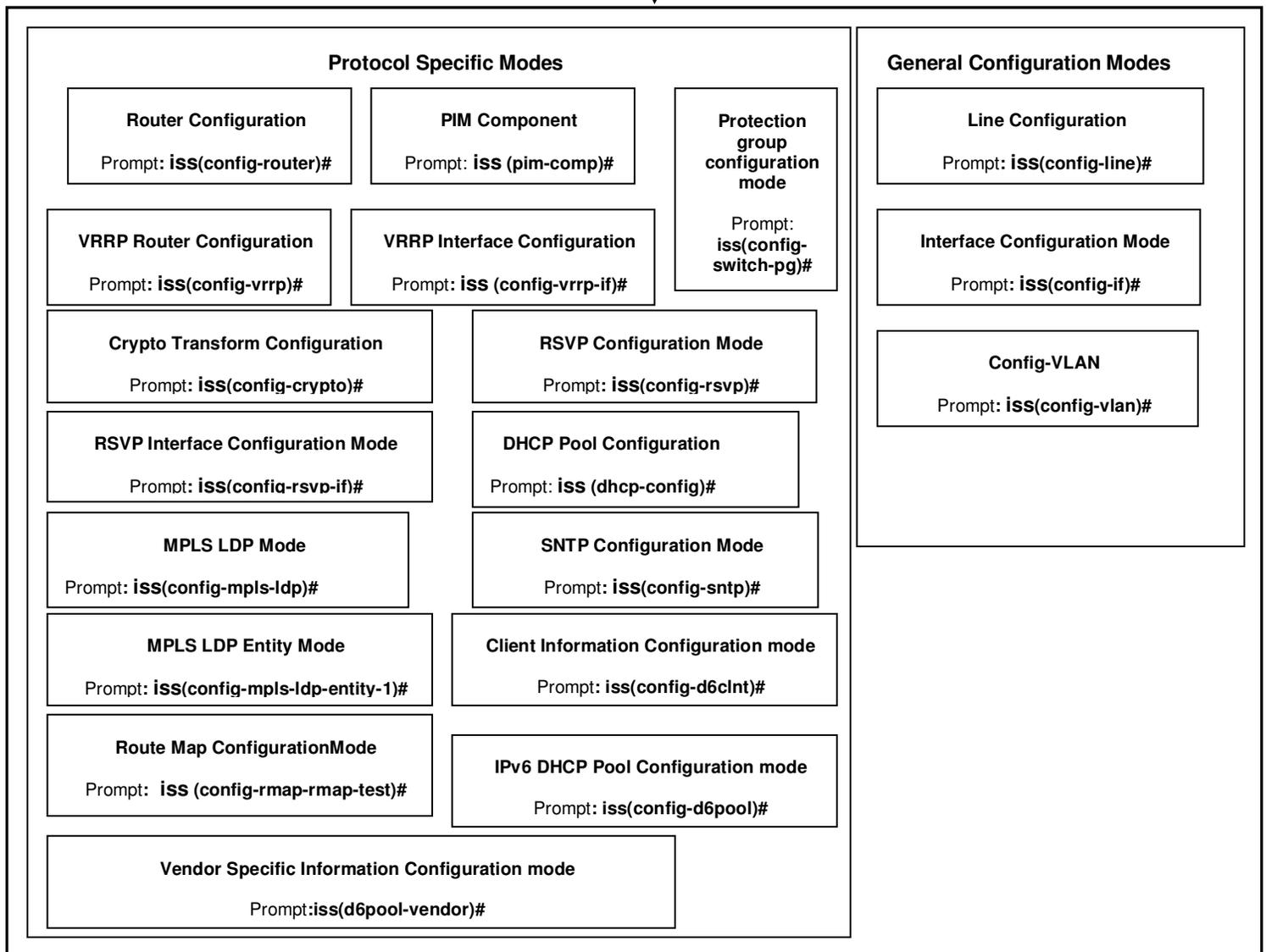
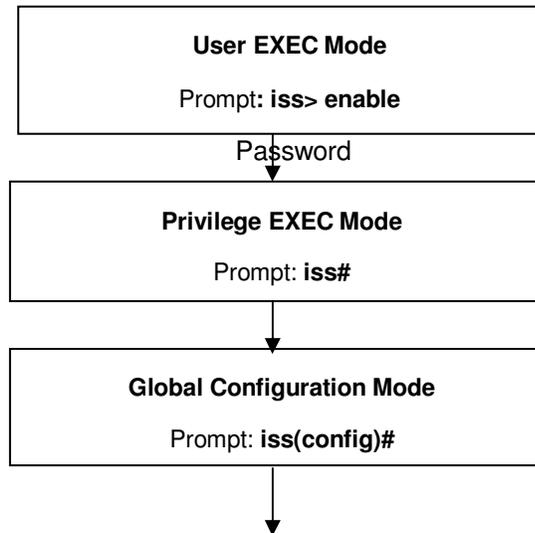


Figure 2-1: Command Modes Access Path

Chapter

3

System Commands

The System Commands describes the commands used to manage access permissions, mode access and terminal configurations on ISS.

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

- help
- clear screen
- enable
- disable
- configure terminal / configure
- run script
- listuser
- lock
- username
- enable password
- line
- alias - replacement string / alias – interface | exec | configure
- access-list provision mode
- access-list commit
- exec-timeout

ISS

- logout
- end
- exit
- show privilege
- show line
- show aliases
- show users
- show history

3.1 help

This command displays a brief description for the given command.

To display help description for commands with more than one word, do not provide any space between the words,

For example: configure terminal command must be executed as

```
iss # help configureterminal
```

help [command]

Mode All Modes

Package Workgroup, Enterprise and Metro

Example iss# help enable

ISS

3.2 clear screen

This command clears all the contents from the screen.

clear screen

Mode All Modes

Package Workgroup, Enterprise and Metro

Example iss# clear screen

3.3 enable

This command enters into default level privileged mode.

If required, the user can specify the privilege level by enabling level with a password (login password) protection to avoid unauthorized user.

enable [**<0-15> Enable Level**]

Syntax Description	Enable level	-	<p>Sets the privilege level to enter the system. The level ranges from 0 to 15</p> <ul style="list-style-type: none"> Users with Privilege Level 0 can access only the following commands: <ul style="list-style-type: none"> - enable - disable - exit - help - logout <p>This is the most restricted level.</p> Users with Privilege Level 1 can access all user-level commands with iss> prompt. System allows to configure additional privilege levels (from level 2 to 14) to meet the needs of the users while protecting the system from unauthorized access. Users with Privilege Level 15 can access all commands. It is the least restricted level.
Mode	User EXEC Mode		
Package	Workgroup, Enterprise and Metro		
Default	Enable level	-	15
Example	iss# enable 15		
Related Commands	<ul style="list-style-type: none"> Disable –Turns off privileged commands enable password – Modifies enable password parameters 		

ISS

3.4 disable

This command turns off privileged commands. The privilege level varies between 0 and 15.

disable [<0-15> Privilege level to go to]

Mode User EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# disable 1



The privilege level value should be lesser than the privilege level value given in the enable command

Related Command

- **enable** – Enters to privileged EXEC mode

3.5 configure terminal

This command enters to Global Configuration Mode which allows the user to execute all the commands that supports global configuration mode.

configure terminal

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# configure terminal

- Related Commands**
- **end** – Exits from Configuration mode
 - **exit** – Exits the current configuration mode

ISS

3.6 configure

This command enters the configuration mode.

This command is a complete standardized implementation of the existing command and operates similar to that of the command `configure terminal`

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example `iss# configure`



- Configuration from memory or network is not supported, when entered into the configuration mode using this command.

Related Command

- **end** - Exits from Configuration mode
- **exit** - Exits the current configuration mode to the next highest configuration mode

3.7 run script

This command runs CLI commands from the specified script file.

```
run script [flash: | slot0: | volatile:] <script file> [<output file>]
```

Syntax	flash: slot0: 	- Specifies the source of the script file.
Description	volatile:	<ul style="list-style-type: none">• flash - The script file is read from the Flash memory.• slot0 - The script file is read from the PCMCIA card or CompactFlash memory. <p>This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported</p> <ul style="list-style-type: none">• volatile - The script file is read from the volatile memory. <p>This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.</p>
	script file	- Specifies the script file to be executed
	output file	- Specifies the output file
Mode	Privileged EXEC Mode.	
Package	Workgroup, Enterprise and Metro	
Example	iss# run script flash sample.js	

ISS

3.8 listuser

This command lists all the default and newly created users, along with their permissible mode.

listuser

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# listuser

```
USER                MODE
root                /
guest               /
```

Related Command

- **show users** – Displays information about terminal lines

3.9 lock

This command locks the CLI console. It allows the user/system administrator to lock the console to prevent unauthorized users from gaining access to the CLI command shell. Enter the login password to release the console lock and access the CLI command shell.

lock

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	<code>iss# lock</code>

3.10 username

This command creates a user and sets the enable password for that user with the privilege level. The no form of the command deletes a user and disables the enable password for that user.

```
username <user-name> [password [ 0 | 7 | LINE ] <passwd>] [privilege <1-15>]
no username < user-name >
```

Syntax Description	<user-name>	-	Specifies the login user name to be created
	password	-	Specifies the password to be entered by the user to login to the system, and password encryption to be used. The password encryption options are: <ul style="list-style-type: none"> • 0 - Uses the unencrypted password • 7 - Uses the hidden password • LINE - Uses the Line password This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
	privilege	-	Applies restriction to the user for accessing the CLI commands. This values ranges between 1 and 15. For example, a user ID configured with privilege level as four can access only the commands having privilege ID lesser than or equal to four.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config)# username products password prod123 privilege 15
- The user products is created with the privilege level 15. Hence, the user will be visible to view all the commands.
```

```
iss(config)# username support password supp123 privilege 1
- The user support is created with the privilege level 1. Hence, the user will be visible to view only the below commands:
    ▪ Show - Show commands related to all the features.
    ▪ Enable - Enables the privilege level.
    ▪ Disable - Disables the privilege level.
    ▪ Exit
    ▪ Logout
    ▪ Clear
    ▪ Debug
    ▪ No Debug
```



Privilege ID is set as zero for all the show commands and is set as 15 for all the configuration commands, in the def files. That is, root users can access all the commands and other users can access only the show commands. Users can change the privilege IDs of the commands in the def file to customize and segregate the commands as per the needs.

Related Command

- `enable password` – Modifies enable password parameters
- `enable` – Enters to privileged EXEC mode
- `luser` – Lists all the users

ISS

3.11 enable password

This command modifies enable password parameters and the no form of the command disables enable password parameters.

```
enable password [level (1-15)] <LINE 'enable' password>
```

```
no enable password [level (1-15)]
```

Syntax Description	level	- Represents the privilege level for which the password is to be set. The level ranges from 1 to 15.
	<LINE 'enable' password>	Represents the password to be given.
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss(config)# enable password level 1 adm123	
Related Command	<ul style="list-style-type: none"> • username – Creates a user and sets the password for that user with the privilege level • enable – Enters to privileged EXEC mode 	

3.12 line

This command identifies a specific line for configuration and enters the line configuration mode and allows the user to execute all the commands that supports line configuration mode.

```
line {console | vty | <line-number(0-16)>} [<ending-line-number(3-16)>]
```

Syntax Description	console	- Console
	vty	- Virtual terminal line
	<line-number(0-16)>	- Specifies the ID of a specific telnet session or initial telnet session in a configured series of telnet sessions. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
	<ending-line-number(3-16)>	- Specifies the ID of the last telnet session in a configured series of telnet sessions. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss(config)# line console	
Related Commands	<ul style="list-style-type: none"> • end – Exits from Configuration mode and enters Privileged Exec mode • exit – Exits the current configuration mode • show line – TTY line information 	

ISS

3.13 alias - replacement string

This command replaces the given token by the given string and the no form of the command removes the alias created for the given string.

```
alias <replacement string> <token to be replaced>
```

```
no alias <alias>
```

Syntax Description <replacement string>/ <alias> - Represents the string for which a replacement is needed.

 <token to be replaced> - Specifies an abbreviated/ short form of the replacement string

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss# alias products pdt

Related Command • **show aliases** – Displays the aliases

3.14 alias – interface | exec | configure

This command replaces the given token / command with the given string.

This command is a standardized implementation of the existing command. It operates similar to that of the command alias-replacement , except that it allows the user to type a command with multiple tokens without quotes.

```
alias {interface | exec | configure} <alias-name> { command <max 10 tokens> | token }
```

Syntax	interface	-	Specifies the commands executed in interface configuration mode. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
Description	exec	-	Specifies the commands executed in privileged EXEC / user EXEC mode. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
	configure	-	Specifies the commands executed in configuration mode (That is, global, line, profile, vlan, switch and protocol specific configuration modes). This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
	<alias-name>	-	Specifies the alternate name to be used for the command or token.
	command <max 10 tokens>	-	Specifies the command and token values for which alias name should be configured.
	token	-	Specifies the token for which alias name should be configured.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# alias ln line`



- Alias name can be set only for the commands having equal to or less than 10 tokens.

Related Command

- `show aliases` - Displays the aliases

ISS

3.15 access-list provision mode

This command removes the limit on number of unicast MAC entries indications to control.

```
access-list provision mode { consolidated | immediate }
```

Syntax Description **consolidated** - Configures the provision mode as consolidated.

immediate - Configures the provision mode as immediate.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults immediate

Example `iss(config)# access-list provision mode consolidated`

3.16 access-list commit

This command triggers provisioning of active filter rules to hardware based on configured priority. This command is applicable only when provision mode is consolidated. Traffic flow would be impacted when filter-rules are reprogrammed to hardware.

access-list commit

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Example	<code>iss# access-list commit</code>

ISS

3.17 exec-timeout

This command sets a time (in seconds) for EXEC line disconnection. The no form of this command resets the EXEC timeout to its default value.

```
exec-timeout <integer (1-18000)>
```

```
no exec-timeout
```

Syntax	<code>integer</code>	-	Configures the EXEC line disconnection time. The value ranges between 1 and 18000 seconds.
Description			
Mode	Line Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	<code>integer</code>	-	1800 seconds
Example	<code>iss(config-line)# exec-timeout 100</code>		
Related Command	<ul style="list-style-type: none"> • <code>line</code> - Configures a console/virtual terminal line 		

3.18 logout

This command exits from Privileged EXEC/ User EXEC mode to ISS Login Prompt in case of console session.

logout

Mode	User EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	<code>iss# logout</code>



In case of a telnet session, this command terminates the session.

ISS

3.19 end

This command exits from the current mode to the Privileged EXEC mode

end

Mode All modes

Package Workgroup, Enterprise and Metro

Example iss# end

Related Command

- **exit** – Exits the current configuration mode

3.20 exit

This command exits from the current configuration mode.

exit

Mode	All modes
Package	Workgroup, Enterprise and Metro
Example	iss# exit
Related Command	<ul style="list-style-type: none">• end – Exits from Configuration mode

ISS

3.21 show privilege

This command shows the current user privilege level.

show privilege

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show privilege
Current privilege level is 15

Related Commands:

- **enable** - Enters to Privileged EXEC Mode

3.22 show line

This command displays TTY line information such as EXEC timeout.

```
show line {console | vty <line>}
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show line console

Current Session Timeout (in secs) = 1800

- Related Command**
- **line** - Configures a console/virtual terminal line
 - **exec-timeout** - Sets a time (in seconds) for EXEC line disconnection.

ISS

3.23 show aliases

This command displays all the aliases.

show aliases

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show aliases

```
show -> sh  
previllege -> pr
```

Related Command

- **alias-replacement string** – Replaces the given token by the given string

3.24 show users

This command displays the information about the current user.

show users

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show users

```
Line           User           Peer-Address
0 con         root          Local Peer
```

Related Command

- **listuser** – Lists all valid users, along with their permissible mode

ISS

3.25 show history

This command displays a list of recently executed commands.

show history

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Example	iss# show history

```
1 show ip int
2 show debug-logging
3 show users
4 show line
5 show line console
6 c s
7 show aliases
8 show privilege
9 listuser
10 show users
11 show history
```

Chapter

4

System Features

ISS offers a rich set of system features to a user, such as login services, copying / writing facilities, duplex / negotiation support, and many other capabilities. Some features have special hardware requirements and others have special design considerations.

CFA (Common Forwarding Agent) is a proprietary module, which acts as a common forwarder of packets between the Network Protocol Module(s), the Data-Link Layer Protocol Layer Module(s) and the Device Drivers. CFA provides central management of the generic parameters of all the interfaces in the system.

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

- default mode
- default restore-file
- default vlan id
- default ip address
- ip address
- switchport
- default ip address allocation protocol
- ip address - rarp/dhcp
- base-mac
- login authentication / login authentication-default | <list-name>
- authorized-manager ip-source
- ip http port

ISS

- set ip http
- archive download-sw
- interface-configuration and deletion
- mtu frame size / system mtu
- bridge port-type
- system-specific port-id
- set custom-param
- mac-addr
- snmp trap link-status
- write
- copy
- copy startup-config / copy running-config startup-config
- copy logs
- firmware upgrade
- copy - file
- clock set
- erase
- cli console
- flowcontrol
- tunnel mode
- tunnel checksum
- tunnel path-mtu-discovery
- tunnel udld
- shutdown - physical/VLAN/port-channel/tunnel Interface
- debug interface
- debug-logging
- incremental-save
- auto-save trigger
- rollback
- shutdown ospf | ospf3 | bgp | isis
- start ospf | ospf3 | bgp | isis
- set switch maximum - threshold
- set switch temperature - threshold
- set switch power - threshold
- mac-learn-rate

- system contact
- system location
- clear interfaces - counters
- clear counters
- show ip interface
- show authorized-managers
- show interfaces
- show interfaces - counters
- show system-specific port-id
- show custom-param
- show interface mtu
- show interface bridge port-type
- show nvram
- show env
- show system information
- show flow-control
- show debug-logging
- show debugging
- show clock
- show running-config
- show http server status
- show system acknowledgement
- show mac-learn-rate

ISS

4.1 default mode

This command configures the mode by which the default interface gets its IP address.

This configuration takes effect only on switch restart.

```
default mode { manual | dynamic }
```

Syntax Description **manual** - Assigns static IP address to the default interface. The IP address and IP mask configured by user are assigned to the default interface.

dynamic - Assigns dynamic IP address to the default interface. That is, IP address provided by the server in the network is assigned to the default interface on switch reboot. The IP address is fetched through the dynamic IP address configuration protocols such as DHCP client, RARP client, and BOOTP client.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults manual

Example `iss(config)# default mode dynamic`

- Related Commands**
- `show nvram` - Displays the current information stored in the NVRAM
 - `default ip address allocation protocol` - Configures the protocol by which the default interface acquires its IP address
 - `default ip address` - Configures the IP address and subnet mask for the default interface.
 - `ip address -rarp/dhcp` - Configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server. The no form of the command resets the IP address for the interface to its default value.

4.2 default restore-file

This command configures the path of the default restoration file from which the configuration should be restored in the flash when the system is restarted.

default restore-file <filename>

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults iss.conf

Example `iss(config)# default restore-file /home/iss/restore.conf`

Related Commands

- **show nvram** - Displays the current information stored in the NVRAM

ISS

4.3 default vlan id

This command sets the default VLAN ID to be used at reboot of the switch. This value is stored in NVRAM and ranges between 1 and 4094.

default vlan id <count (1-4094)>

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 1

Example `iss(config)# default vlan id 32`

Related Commands

- `show nvram` - Displays the current information stored in the NVRAM.

4.4 default ip address

This command configures the IP address and subnet mask for the default interface.

```
default ip address <ip-address> [ subnet-mask <subnet mask> ] [ interface
<interface-type> <interface-id> ]
```

Syntax	<ip address>	-	Sets the IP address for the default interface / specified interface. If the network in which the switch is implemented contains a server such as DHCP server, dynamically allocating IP address, the configured IP address should not be within the range of the addresses that will be allocated by the server to the other switches. This precaution avoids creation of IP address conflicts between the switches.
Description	subnet-mask <subnet mask>	-	Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed
	<interface-type>	-	<p>Sets the IP address and / or subnet mask for the specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> • 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. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan – Internal LAN created on a bridge per IEEE 802.1ap.
	<interface-id>	-	<p>Sets the IP address and / or subnet mask for the 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.</p> <p>For example: 0/1 represents that the slot number is 0 and port number is 1.</p> <p>Only i-lan ID is provided, for interface type i-lan. For example: 1 represents i-lan ID.</p>
Mode	Global Configuration Mode		

ISS

Package Workgroup, Enterprise and Metro

Defaults ip address - 10.0.0.1

subnet-mask - 255.0.0.0

Example

```
iss(config)# default ip address 20.0.0.1 subnet-mask 255.0.0.0
interface gigabitethernet 0/1
```

Related Command

- **show nvram** - Displays the current information stored in the NVRAM

4.5 ip address

This command sets the IP address for an interface. The no form of the command resets the IP address of the interface to its default value.

```
ip address <ip-address> <subnet-mask> [secondary]
```

```
no ip address [<ip_addr>]
```

Syntax Description	<ip-address>	<ul style="list-style-type: none"> - Sets the IP address for an interface. If the network in which the switch is implemented contains a server such as DHCP server, dynamically allocating IP address, the configured IP address should not be within the range of the addresses that will be allocated by the server to the other switches. This precaution avoids creation of IP address conflicts between the switches.
	<subnet-mask>	<ul style="list-style-type: none"> - Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed.
	secondary	<ul style="list-style-type: none"> - Sets the configured IP address as an additional IP address for the interface (that is, the configured address is used as secondary address instead of primary address). <p>The configuration of this feature is not supported on OOB interface.</p>

Mode Interface Configuration Mode
 This command is applicable in VLAN Interface Mode / OOB Interface Mode.

Package Workgroup, Enterprise and Metro

Defaults IP address specified in issnvram.txt is taken as default for the default VLAN identifier.
 IP address is assigned as 0.0.0.0 and subnet mask as 255.255.255.255 for other interfaces.

Example `iss(config-if)# ip address 10.0.0.3 255.255.255.0 secondary`



- The interface should be shutdown before executing this command.
- If the IP address of the interface to which you are connected is modified, then the connection to the switch will be lost.
- When the same network interface is used for OOB and NFS mounting, the operation done on OOB will have impact on NFS.

ISS

**Related
Command**

- **show nvram** - Displays the current information stored in the NVRAM.
- **show ip interface** - Displays the IP interface configuration for all interfaces available in the switch.
- **shutdown - physical/VLAN/port-channel/tunnel Interface** - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.

4.6 switchport

This command configures the port as switch port. The no form of the command resets the port as router port.

- Only switch port related commands are made available for the interface, when the port is configured as switch port.
- Only router port related commands are made available for the interface, when the port is configured as router port.

switchport

no switchport

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults switchport

Example `iss(config-if)# switchport`



The interface should be shutdown before executing this command.

Related Commands

- **release** - Releases, on the specified interface, the DHCP lease obtained for an IP address from a DHCP server.
- **renew** - Renews the DHCP lease for the interface specified.
- **ip dhcp relay circuit-id** – Configures circuit ID value for an interface.
- **ip dhcp relay remote-id** – Configures remote ID value for an interface.
- **show ip interface** - Displays the IP interface configuration for all interfaces available in the switch.
- **switchport filtering-utility-criteria** - Creates filtering utility criteria for the port.
- **switchport pvid** - Configures the PVID on the specified port.
- **switchport acceptable-frame-type** - Configures the type of VLAN dependant BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.
- **switchport ingress-filter** - Enables ingress filtering feature on the port.
- **switchport map protocols-group** - Maps the configured protocol group to a particular VLAN ID for an interface.

- **switchport priority default** - Configures the default ingress user priority for a port.
- **switchport mode** - Configures the mode of operation for a switch port.
- **switchport protected** - Enables switchport protection feature for a port.

4.7 default ip address allocation protocol

This command configures the protocol used by the default interface for acquiring its IP address. This configuration takes effect only on rebooting the system.

```
default ip address allocation protocol {bootp | rarp | dhcp}
```

Syntax Description	bootp	- Allows the client device to obtain its own IP address, address of a server host and name of a boot file to be executed from a BOOTP server.
	rarp	- Allows the client device to dynamically find its IP address from RARP server, when it has only its hardware address such as MAC address.
	dhcp	- Allows the client device to obtain configuration parameters such as network address, from the DHCP server.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults dhcp

Example `iss(config)# default ip address allocation protocol bootp`



- This command executes only if the default mode is configured as dynamic
- If the default interface is configured as OOB and if the same network interface is used for OOB and NFS mounting, then the operation done on OOB will have impact on NFS

Related Commands

- **default mode** - Configures the mode by which the default interface acquires its IP address
- **show nvram** - Displays the current information stored in the NVRAM

4.8 ip address - rarp/dhcp

This command configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server. The no form of the command resets the IP address for the interface to its default value.

```
ip address { dhcp | rarp}[client-id { FastEthernet | GigabitEthernet | Port-
channel | Vlan } <interface_list>] [hostname <host_name>]
```

no ip address

Syntax Description	dhcp	-	Allows the client device to obtain configuration parameters such as network address, from the DHCP server.
	rarp	-	Allows the client device to dynamically find its IP address from RARP server, when it has only its hardware address such as MAC address.
	client-id	-	<p>Sets the client identifier that specifies the interface type and hexadecimal MAC address of the specified interface. The various interface types that can be specified are:</p> <ul style="list-style-type: none"> • 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. • GigabitEthernet - A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • Port-channel - Logical interface that represents an aggregator which contains several ports aggregated together. • Vlan - Logical interface that specifies a group of hosts which can communicate with each other as in same broadcast domain. • <interface list> - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3. <p>Feature not supported - This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.</p>

hostname - Sets the name of the host from which the IP address is to be acquired dynamically.
Feature not supported - This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Interface Configuration Mode
This command is applicable only in VLAN Interface Mode/OOB Interface Mode.

Package Workgroup, Enterprise and Metro

Defaults dhcp

Example `iss(config-if)# ip address dhcp`



When the same network interface is used for OOB and NFS mounting, the operation done on OOB will have impact on NFS.

Related Commands

- **show ip dhcp client stats** - Displays the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server.
- **release** - Releases, on the specified interface, the DHCP lease obtained for an IP address from a DHCP server.
- **renew** - Renews the DHCP lease for the interface specified

4.9 base-mac

This command configures the base MAC address for the switch in the NVRAM.

This command configures the base unicast MAC address of the switch in the NVRAM. The switch uses this address as its hardware address. Layer 3 modules use the switch MAC address as the source MAC address in the transmitted packets. This configuration takes effect only when the switch is restarted.

base-mac <mac_address>

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 00:01:02:03:04:05

Example `iss(config)# base-mac 00:89:fe:34:55:33`

Related Command

- **show nvram** - Displays the current information stored in the NVRAM
- **show spanning-tree - Summary, Blockedports, Pathcost, redundancy** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree active** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree interface** - Displays the port related spanning tree information for the specified interface.
- **show spanning-tree root** - Displays the spanning tree root information.
- **show spanning-tree bridge** - Displays the spanning tree bridge information.
- **show spanning-tree - layer 2 gateway port** - Displays spanning tree information for all L2GPs enabled in the switch.
- **name** - Configures the name for the MST region.
- **show spanning-tree mst - CIST or specified mst Instance** - Displays multiple spanning tree information for all MSTIs in the switch.
- **show spanning-tree vlan - Summary, Blockedports, Pathcost** - Displays PVRST related information for the specified VLAN.
- **show spanning-tree vlan - bridge** - Displays the PVRT related information of the bridge for the specified VLAN ID.
- **show spanning-tree vlan - root** - Displays the PVRT related information of the root, for the specified VLAN ID.
- **show spanning-tree vlan - interface** - Displays interface specific PVRST information for the specified VLAN.

4.10 login authentication

This command sets the authentication method for user logins. The no form of the command resets the authentication method for user logins to its default values.

Few network routers and other network equipment allows access to a server or a managing computer to determine if the user attempting to log in has the proper rights or is in the user database.

Changing login authentication from default to another value may disconnect the telnet session.

```
login authentication [{radius | tacacs }] [local]
```

```
no login authentication
```

Syntax Description	radius	<ul style="list-style-type: none"> - Sets the RADIUS server to be used as an authentication server. Enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.
	tacacs	<ul style="list-style-type: none"> - Sets the TACACS server to be used as an authentication server. Communicates with the authentication server commonly used in networks.
	local	<ul style="list-style-type: none"> - Sets locals authentication. The user identification, authentication, and authorization method is chosen by the local system administration and does not necessarily comply with any other profiles.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Local

Example `iss(config)# login authentication radius`

- Related Commands**
- **username** - Creates a user and sets the enable password for that user with the privilege level
 - **no enable password** - Deletes a user and disables enable password parameters
 - **show system information** - Displays system information

4.11 login authentication-default | <list-name>

This command sets the authentication method for user logins to default values. The no form of the command sets the authentication method for user logins to default values.

This command operates similar to that of the command login authentication.

```
login authentication { default | <list-name> }
```

```
no login authentication { default | <list-name> }
```

Syntax	default	- Sets the default authentication.
Description	list-name	- Uses the list created with the user name command. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss(config)# login authentication default	
Related Commands	<ul style="list-style-type: none"> • username - Creates a user and sets the enable password for that user with the privilege level • no enable password - Deletes a user and disables enable password parameters • show system information - Displays system information 	

4.12 authorized-manager ip-source

This command configures an IP authorized manager and the no form of the command removes manager from authorized managers list.

```
authorized-manager ip-source <ip-address> [{<subnet-mask> | / <prefix-length(1-32)>}] [interface [<interface-type <0/a-b, 0/c, ...>] [<interface-type <0/a-b, 0/c, ...>]] [vlan <a,b or a-b or a,b,c-d>] [cpu0] [service [snmp] [telnet] [http] [https] [ssh]]
```

```
no authorized-manager ip-source < ip-address > [{<subnet-mask > | / <prefix-length(1-32)>}]
```

Syntax	<ip-address>	- Sets the network or host address from which the switch is managed. An address 0.0.0.0 indicates 'Any Manager'."
Description	<subnet-mask>	- Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed.
	<prefix-length(1-32)>	- Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. The value ranges between 1 and 32.
	interface	- Configures the network or host address for the specified interface. The details to be provided are: <ul style="list-style-type: none"> • <interface-type> - Sets the type of interface. The interface can be: <ol style="list-style-type: none"> 1. 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. 2. gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. 3. extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. 4. i-lan – Internal LAN created on a bridge per IEEE 802.1ap. • <0/a-b, 0/c, ...> - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan. Only i-lan ID is provided, for interface type i-lan. Use comma as a separator

without space while configuring list of interfaces.
 Example: 0/1,0/3 or 1,3.

- vlan <a,b or a-b or a,b,c-d>** Sets the list of VLANs or a single specific VLAN in which the IP authorized manager can reside.
- cpu0** - Configures the access rights for the manager of the switch through OOB Port.
- service** - Configures the type of service to be used by the IP authorized manager. The values can be:
- ssh - Logs into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled.
 - http - Defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page
 - https – Transmits data securely over the World Wide Web. S-HTTP is designed to transmit individual messages in a secured manner.
 - snmp - Manages complex networks. SNMP works by sending messages, called PDUs, to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in MIBs and return this data to the SNMP requesters

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults All services are allowed for the configured manager

Example
 iss(config)# authorized-manager ip-source 10.203.113.5
 255.255.255.255 interface gigabitethernet 0/1 vlan 1 service
 snmp

Related Command

- **show authorized managers** - Displays the configured authorized managers

4.13 ip http port

This command sets the HTTP port. This port is used to configure the router using the Web interface. The value ranges between 1 and 65535. The no form of the command resets the HTTP port to its default value.

```
ip http port <port (1-65535)>
```

```
no ip http port
```

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	80
Example	iss(config)# ip http port 90

HTTP port number configuration takes effect only when HTTP is disabled and enabled again.

Related commands	<ul style="list-style-type: none">• <code>set ip http</code> - Enables/disables HTTP• <code>show http server status</code> - Displays the http server status
-------------------------	---

ISS

4.14 set ip http

This command enables/disables HTTP in the switch.

```
set ip http {enable | disable}
```

Syntax **enable** - Enables HTTP in the switch.
Description

disable - Disables HTTP in the switch.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults enable

Example iss(config)# set ip http disable

Related
Commands

- **ip http port** - Sets the HTTP port
- **show http server status** - Displays the http server status

4.15 archive download-sw

This command performs an image download operation using TFTP or SFTP from a remote location.

```
archive download-sw /overwrite [ /reload ] { tftp://ip-address/filename |
sftp://<user-name>:<pass-word>@ip-address/filename | flash:filename }
```

Syntax Description	overwrite	<ul style="list-style-type: none"> - Overwrites the software image in flash with the downloaded one. This option should be specified only if the flash device have sufficient space to hold two images
	reload	<ul style="list-style-type: none"> - Reloads the software after image download. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
	tftp://ip-address/filename	<ul style="list-style-type: none"> - Configures the source URL and filename that is to be used to overwrite / update the existing image. The file is transferred using TFTP. Filenames and directory names are case sensitive
	sftp://<user-name>:<pass-word>@ip-address/filename	<ul style="list-style-type: none"> - Configures the source URL, user name, password and filename that is to be used to overwrite / update the existing image. The file is transferred using SFTP. Filenames and directory names are case sensitive
	flash:filename	<ul style="list-style-type: none"> - Configures the name of the flash file that should be used to overwrite / update the existing image. Filenames are case sensitive
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss# archive download-sw /overwrite tftp://20.0.0.1/ISS.exe	
	Filenames and directory names are case sensitive	

4.16 interface-configuration and deletion

This command allows to configure interface such as out of band management, port channel, tunnel and so on. The no form of the command deletes interface such as VLAN, port-channel, tunnel interface and so on.

WGS enabled in the switch

```
interface {cpu0 | VlanMgmt | port-channel <port-channel-id (1-65535)> | tunnel
<tunnel-id (0-128)> | <interface-type> <interface-id> | linuxvlan <interface-
name> }
```

```
no interface { vlanMgmt | Port-Channel <port-channel-id(1-65535)> | tunnel
<tunnel-id (0-128)> | linuxvlan <interface-name> }
```

WGS disabled in the switch

```
interface {cpu0 | vlan <vlan-id (1-4094)> [switch <switch-name>] | port-
channel <port-channel-id (1-65535)> | tunnel <tunnel-id (0-128)> | <interface-
type> <interface-id> | linuxvlan <interface-name> | loopback <interface-id (0-
100)> | sisp <interface-id (1-65535)> | virtual <integer (1-65535)> |
mplstunnel <tunnel-id (1-100)> }
```

```
no interface { vlan <vlan-id (1-4094)> [switch <switch-name>] | port-channel
<port-channel-id(1-65535)> | tunnel <tunnel-id (0-128)> | <interface-type>
<interface-id> | linuxvlan <interface-name> | loopback <interface-id (0-100)>
| sisp <interface-id(1-65535)> | virtual <integer (1-65535)> | mplstunnel
<tunnel-id (1-100)>}
```

Syntax	cpu0	-	Configures the access rights for the manager of the switch through OOB Port.
Description	VlanMgmt	-	Configures the management VLAN interface
	vlan<vlan-id (1-4094)>	-	Configures 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.
	switch<switch-name>	-	Specifies the name of the switch context. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported

<code>port-channel<port-channel-id (1-65535)></code>	<ul style="list-style-type: none"> - Configures the port to be used by the host to configure the router. This value ranges between 1 and 65535. The port channel identifier can be created or port channel related configuration can done, only if the LA feature is enabled in the switch.
<code>tunnel<tunnel-id (0-128)></code>	<ul style="list-style-type: none"> - Configures the tunnel. This value ranges between 0 and 128.
<code><interface-type></code>	<ul style="list-style-type: none"> - Configures the specified type of interface. The interface can be: <ul style="list-style-type: none"> • 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. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
<code><interface-id></code>	<p>Configures 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>
<code>linuxvlan<interface-name></code>	<ul style="list-style-type: none"> - Configures the interface name of the Linux VLAN Interface
<code>loopback<interface-id (0-100)></code>	<ul style="list-style-type: none"> - Configures the loopback identifier. The value ranges between 0 and 100.
<code>sisp<interface-id (1-65535)></code>	<ul style="list-style-type: none"> - Configures the SISP identifier. This value ranges between 1 and 65535. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported

ISS

virtual<integer (1-65535)>¹ - Configures the virtual interface identifier. This value ranges between 1 and 65535.

mplstunnel<tunnel -id (1-100)> - Configures the MPLS tunnel interface identifier. This value ranges between 1 and 100.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# interface tunnel 2`



- The command **no shutdown** must be executed for the activation of the tunnel
- MPLS must be enabled on the interface in which the MPLS tunnel will be stacked
- Logical interfaces cannot be created in the switch, if the base bridge mode is configured as transparent bridging.

Related Commands

- **shutdown port-channel** - Shuts down LA in the switch and releases the allocated resources to the switch.
- **set port-channel** - Configures the admin status of LA in the switch.
- **port-channel load-balance** - Configures the load balancing policy for all port channels created in the switch.
- **channel-group** - Adds the port as a member of the specified port channel that is already created in the switch.
- **show etherchannel** - Displays Etherchannel information for all port-channel groups created in the switch.
- **show lacp** - Displays LACP counter / neighbor information for all port-channels.
- **show interfaces** - Displays the interface status and configuration
- **base bridge-mode** - Configures the mode in which the VLAN feature should operate on the switch.

¹ This option is available, only when PBB feature is enabled

4.17 mtu frame size

This command configures the maximum transmission unit frame size for the interface. The value ranges between 90 and 9216.

This value defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub-layer and should not include size of the encapsulation or header added by the interface. This value represents the IP MTU over the interface, if IP is operating over the interface.

mtu <frame-size (90-9216)>

Mode	Interface Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	1500

Example `iss(config-if)# mtu 900`



- This configuration can be done, only if the interface is administratively down.
- The MTU value should not be greater than 1522 for fastEthernet interface.

Related Commands

- **show interfaces** - Displays the interface status and configuration
- **show interface mtu** - Displays the global maximum transmission unit
- **shutdown-physical/VLAN/port-channel/tunnel Interface** – Enables the physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.

ISS

4.18 system mtu

This command configures the maximum transmission unit frame size for all interfaces. The no form of this command sets the maximum transmission unit to the default value in all interfaces.

This command is a standardized implementation of the existing command. It operates similar to that of the command mtu frame size

```
system mtu <frame-size(90-9216)>
```

```
no system mtu
```

Syntax	frame-size	-	Maximum transmission unit frame size to be set for all interfaces, This value ranges between 90 and 9216.
Description			

Mode	Global configuration mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	1500
-----------------	------

Example	iss(config)# system mtu 200
----------------	-----------------------------



- The interface must be brought administratively down, prior to changing the MTU.

Related Commands	<ul style="list-style-type: none"> • show interfaces - Displays the interface status and configuration • show interface mtu - Displays the global maximum transmission unit
-------------------------	---

4.19 loopback local

This command enables loopback on a physical interface. The no form of this command disables the loopback on a physical interface.

```
loopback local  
no loopback local
```

Mode	Global configuration mode
Package	Workgroup, Enterprise and Metro
Example	<code>iss(config)# loopback local</code>

4.20 bridge port-type

This command configures the bridge port type for an interface.

```
bridge port-type { providerNetworkPort | customerNetworkPort {port-based | s-
tagged | c-tagged} | customerEdgePort | propCustomerEdgePort |
propCustomerNetworkPort | propProviderNetworkPort | customerBridgePort |
customerBackbonePort }
```

Syntax	providerNetworkPort	-	Sets the bridge port type as provider network port. This option is applicable in provider bridges and provider backbone b-component bridge modes. The port is connected to a single provider.
Description	customerNetworkPort	-	Sets the bridge port type as customer network port. It has the following options: <ul style="list-style-type: none"> • port-based • s-tagged • c-tagged
	customerEdgePort	-	Sets the bridge port type as Customer Edge Port. The port is in a PEB that is connected to a single customer. The packets received on this port are initially classified to a CVLAN. CVLAN classification is done based on the VID in the C-tag present in the packet or from the PVID of the port. Service instance selection is done for a frame based on the entry present in the C-VID registration table for the pair (C-VID, reception port).
	propCustomerEdgePort	-	Sets the bridge port type as Proprietary Customer Edge Port. The port is connected to a single customer, where multiple services can be provided based on only proprietary SVLAN classification tables. S-VLAN classification is not done based on C-VID registration table on the port.
	propCustomerNetworkPort	-	Sets bridge port type as Proprietary Customer Network Port. The port is connected to a single customer, where multiple service can be provided based on CVLANs by assigning one of the proprietary SVLAN classification tables to the port. The services can also be assigned using other proprietary SVLAN classification tables, where CVLAN is not the index

of the table.

- propProviderNetworkPort** - Sets bridge port type as Proprietary Provider Network Port.
- The port is connected to a Q-in-Q bridge located inside the provider network. The port acts as a part of S-VLAN component. The packets to be tagged and sent out of the port contain 0x8100 as its ethertype. The packets received with standard Q tag is considered as S-Tagged packets.
- customerBridgePort** - Sets bridge port type as Customer Bridge Port.
- The port is to be used in customer bridges and in provider (Q-in-Q) bridges. This port type is not valid in PCBs and PEBs.
- customerBackbonePort** - Sets bridge port type as Backbone Edge Bridge Port that can receive and transmit I-tagged frames for multiple customers, and assign B-VIDs and translate I-SID on the basis of the received I-SID. CBPs are applicable only on PBB B Components.

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults providerNetworkPort for provider core and edge bridges.
customerBridgePort for customer bridges.

Example `iss(config-if)# bridge port-type providerNetworkPort`



- Tunneling must be enabled to change port type from Provider Network Port.
- Tunneling must be disabled to change port type to Provider Network Port.
- Port must be administratively down for changing to another port type.
- Bridge port-type is supported only in the following Bridge Modes:
 - Provide Edge Bridge
 - Provider Core Bridge
 - Provider Backbone Bridge I Component
 - Provider Backbone Bridge B Component
- In case of Provider Bridge or Customer Bridge, bridge port type will always be

customerBridgePort.

- **customerEdgePort** is valid only in Provider Edge Bridge.
- All other port types excluding **customerBridgePort** and **customerEdgePort** are valid in both Provide Edge Bridge and Provider Core Bridge.
- Bridge port type can be set only for switch ports and not for router ports, IVR interfaces and I-LAN interfaces.
- The port type cannot be set for a port-channel port, if physical ports are aggregated in the port-channel.
- The port type cannot be set for a port that is part of a port-channel.
- **show interface bridge port-type** - Displays the Bridge Port Type of interfaces in the switch
- **switchport acceptable-frame-type** - Configures the type of VLAN dependant BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.
- **switchport ingress-filter** - Enables ingress filtering feature on the port.
- **tunnel mode** – Configures the tunnel interface with the associated parameters.
- **switchport** - Configures the port as switch port.

Related Commands

4.21 system-specific port-id

This command configures the system specific index for the port. It provides a different numbering space other than the IfIndex to identify ports. The value ranges between 1 and 16384. If no other value has been configured, 0 is set by default.

system-specific port-id <integer (1-16384)>

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 0

Example `iss(config-if)# system-specific port-id 50`

**Related
Commands** `show system-specific port-id` - Displays the custom-param configurations.

ISS

4.22 set custom-param

This command configures the custom parameters for a particular port. The no form of the command deletes the custom parameter configurations.

```
set custom-param {type <integer> length <integer> value <string> | attribute
<integer (1-4)> value <integer (0-4294967295)>}
```

```
no custom-param [type <integer>] [attribute <integer (1-4)>]
```

Syntax	type	-	Sets the type of the TLV information.
Description	length	-	Sets the length of the TLV information.
	value	-	Sets the value of the TLV information.
	attribute	-	Sets the opaque attribute ID configured on the port.. The value ranges between 1 and 4.
	value	-	Sets the value for the Opaque attribute. The value ranges between 0 and 4294967295.
Mode	Interface Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	value	-	0
Example	iss(config-if)# set custom-param attribute 2 value 40		
Related Commands	show custom-param - Displays the custom-param configurations.		

4.23 mac-addr

This command configures unicast MAC address for the interface.

mac-addr <aa:aa:aa:aa:aa:aa>

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults MAC address of the switch is assigned as MAC address for the interface.

Example `iss(config-if)# mac-addr 00:22:33:44:55:66`



- The MAC address can be set only when `ifMainAdminStatus` for the interface is down.
- The object is valid only for interfaces that have the `ifMainType` set as `ethernetCsmacd(6)` or `ieee8023ad(161)`.

Related Commands `show interfaces` - Displays the interface status and configuration.

ISS

4.24 snmp trap link-status

This command enables trap generation on the interface. The no form of this command disables trap generation on the interface.

The interface generated linkUp or linkDown trap. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and is not ready for traffic flow.

```
snmp trap link-status
```

```
no snmp trap link-status
```

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults SNMP trap link status is enabled

Example `iss(config-if)# snmp trap link-status`

Related Command `show interfaces` - Displays the interface status and configuration

4.25 write

This command writes the running-config to a flash file, startup-configuration file or to a remote site.

```
write { flash:filename | startup-config | tftp://ip-address/filename |
sftp://<user-name>:<pass-word>@ip-address/filename }
```

Syntax Description	flash:filename	- Configures the name of the file to which the configuration should be wrote. This file is present in the flash.
	startup-config	- Starts the switch with the saved configuration on reboot.
	tftp	<ul style="list-style-type: none"> - Configures the TFTP related details for writing the configuration to a file in TFTP server. • ip-address - The IP address or host name of the server in which configuration should be maintained. • filename - The name of the file in which the configuration should be written. <p>Filenames and directory names are case sensitive</p>
	sftp	<ul style="list-style-type: none"> - Configures the SFTP related details for writing the configuration to a file in SFTP server. • user-name - The user name of remote host or server. • Pass-word - The password for the corresponding user name of remote host or server • ip-address - The IP address or host name of the server in which configuration should be maintained. • filename - The name of the file in which the configuration should be written. <p>Filenames and directory names are case sensitive</p>
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss# write startup-config	
Related Commands	<ul style="list-style-type: none"> • show nvram - Displays the current information stored in the NVRAM • show system information - Displays system information 	

ISS

4.26 copy

This command copies the configuration from a remote site to flash.

```
copy { tftp://ip-address/filename startup-config | sftp://<user-name>:<password>@ip-address/filename startup-config | flash: filename startup-config }
```

Syntax	tftp://ip-address/filename startup-config	<ul style="list-style-type: none"> - Configures the address from which the file is to be copied and the file name from which configuration is to be copied. This option configures the TFTP server details <p>Filenames and directory names are case sensitive</p>
Description	sftp://<user-name>:<password>@ip-address/filename	<ul style="list-style-type: none"> - Configures the name of the file in remote location to be copied (downloaded) into configuration file (iss.conf). <p>This option configures the SFTP server details.</p> <p>Filenames and directory names are case sensitive</p>
	flash: filename startup-config	<ul style="list-style-type: none"> - Configures the name of the file in flash. The configuration in the flash file are used. <p>Filenames are case sensitive</p>
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss # copy flash:clcliser startup-config	

4.27 copy startup-config

This command takes a backup of the initial configuration in flash or at a remote location.

```
copy startup-config {flash: filename | tftp://ip-address/filename |
sftp://<user-name>:<pass-word>@ip-address/filename }
```

Syntax	flash: filename	-	Configures the name of the file in which the initial configuration should be stored. This file is available in the Flash.
Description	tftp://ip-address/filename	-	<ul style="list-style-type: none"> - Configures the TFTP details for taking back up of initial configuration in TFTP server. • ip-address - The IP address or host name of the server. • filename - The name of the file in which the initial configuration should be stored. <p>Filenames and directory names are case sensitive</p>
	sftp://<user-name>:<pass-word>@ip-address/filename	-	<ul style="list-style-type: none"> - Configures the SFTP details for taking back up of initial configuration in SFTP server. • user-name - The user name of remote host or server • Pass-word - The password for the corresponding user name of remote host or server • ip-address - The IP address or host name of the server • filename - The name of the file in which the initial configuration should be stored. <p>Filenames and directory names are case sensitive</p>
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		
Example	iss# copy startup-config flash:clcliser		

ISS

4.28 copy running-config startup-config

This command copies running configuration to the startup configuration file in NVRAM.

This command is a complete standardized implementation of the existing command. It operates similar to that of the command copy startup-config

copy running-config startup-config

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# copy running-config startup-config

4.29 copy logs

This command writes the system logs to a remote site.

```
copy logs {tftp://ip-address/filename | sftp://<user-name>:<pass-word>@ip-
address/filename}
```

Syntax	<code>tftp://ip-</code>	-	Configures the TFTP details for taking back up of system logs in TFTP server.
Description	<code>address/filename</code>		<ul style="list-style-type: none"> • ip-address – the IP address or host name of the TFTP server. • filename – The name of the file in which the system logs should be stored <p>Filenames and directory names are case sensitive</p>
	<code>sftp://<user-</code>	-	Configures the SFTP details for taking back up of system logs in SFTP server.
	<code>name>:<pass-</code>		<ul style="list-style-type: none"> • user-name - The user name of remote host or server. • Pass-word – The password for the corresponding user name of remote host or server. • ip-address - The IP address or host name of the server. • filename - The name of the file in which the system logs should be stored. <p>Filenames and directory names are case sensitive</p>
	<code>word>@ip-</code>		
	<code>address/filename</code>		
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		
Example	<code>iss # copy logs tftp://10.0.0.10/clcliser</code>		

ISS

4.30 firmware upgrade

This command performs firmware upgrade using TFTP from a remote location.

```
firmware upgrade {tftp://ip-address/filename} {flash:normal | flash:fallback}
```

Syntax	<code>tftp://ip-</code>	-	Configures the file to be used for firmware upgrade and its source URL.
Description	<code>address/filename</code>		
			<ul style="list-style-type: none"> • ip-address - IP address or host name of the TFTP server • filename - The name of the file to be used for firmware upgrade. <p>Filenames and directory names are case sensitive</p>
	<code>flash:normal</code>	-	Sets the flash in normal image.
	<code>flash: fallback</code>	-	Sets the fallback image in Flash

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss # firmware upgrade tftp://12.0.0.100/Ramdisk.bin
flash:normal
```



In stacking environment case, this command copies the image to the attached peers.

4.31 copy - file

This command copies a file from a source remote site /flash to a destination remote site/flash. The entire copying process takes several minutes and differs from protocol to protocol and from network to network.

```
copy { tftp://ip-address/filename | sftp://<user-name>:<pass-word>@ip-
address/filename | flash: filename}{ tftp://ip-address/filename |
sftp://<user-name>:<pass-word>@ip-address/filename | flash: filename}
```

Syntax	tftp://ip-	-	Configures the TFTP details to / from which file to be copied.
Description	address/filename		<ul style="list-style-type: none"> • ip-address - IP address or host name of the TFTP server • filename - Name of the file to be copied or file to which information is to be copied <p>Filenames and directory names are case sensitive</p>
	sftp://<user-	-	Configures the SFTP details to / from which file to be copied.
	name>:<pass-		<ul style="list-style-type: none"> • user-name - User name of remote host or server • Pass-word – Password for the corresponding user name of remote host or server • ip-address - IP address or host name of the server • filename - Name of the file to be copied or file to which information is to be copied <p>Filenames and directory names are case sensitive</p>
	word>@ip-		
	address/filename		
	flash: filename	-	Configures the name of the file to be copied. This file is present in Flash.
			Filenames are case sensitive
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		
Example	iss# copy tftp://12.0.0.2/clclire1 flash:clcliser		

ISS

4.32 clock set

This command manages the system clock.

```
clock          set          hh:mm:ss          <day          (1-31)>
{january|february|march|april|may|june|july|august|september|october|november|
december} <year (1970 - 2035)>
```

Syntax Description	hh:mm:ss	-	Sets the current time. The format is hour, minutes and seconds.
	<day (1-31)>	-	Sets the current day. It ranges between 1 and 31.
	january	-	Sets the month as January.
	february	-	Sets the month as February
	march	-	Sets the month as march
	april	-	Sets the month as april
	may	-	Sets the month as may
	june	-	Sets the month as June
	july	-	Sets the month as July
	august	-	Sets the month as August
	september	-	Sets the month as September
	october	-	Sets the month as October
	november	-	Sets the month as November
	december	-	Sets the month as December
	<year (1970 - 2035)>	- -	Sets the year. It ranges between 1970 and 2035

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# clock set 18:04:10 18 Oct 2005

Related Command

- **show clock** - Displays the system clock

4.33 erase

This command clears the contents of the startup configuration or sets parameters in NVRAM to default values.

```
erase {startup-config | nvram: | flash:filename}
```

Syntax Description	startup-config	- Clears the startup configuration file
	nvram	- Clears the content from NVRAM
	flash:filename	- Clears the content from the local system flash file.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example `iss # erase nvram:`



- The Delete functionality is supported only for VxWorks and Linux

Related Commands

- `show nvram` - Displays the current information stored in the NVRAM
- `show system information`- Displays system information
-

ISS

4.34 cli console

This command enables the console CLI through a serial port. The no form of the command disables console CLI.

cli console

no cli console

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Defaults Enabled

Example `iss # cli console`



This command takes effect only on system restart.

Related Commands `show nvram` - Displays the current information stored in the NVRAM.

4.35 flowcontrol

This command is used to set the send or receive flow-control value for an interface.

If flowcontrol send is on for a device and if it detects any congestion at its end, then it notifies the link partner or the remote device of the congestion by sending a pause frame.

If flowcontrol receive is on for the remote device and it receives a pause frame, then it stops sending any data packets. This prevents any loss of data packets during the congestion period.

PAUSE is a flow control mechanism that is implied on full duplex Ethernet link segments. The mechanism uses MAC control frames to carry the PAUSE commands.

```
flowcontrol { send | receive} { on | off | desired}
```

Syntax Description	send	-	Sets the interface to send flow control packets to a remote device
	receive	-	Sets the interface to receive flow control packets from a remote device
	on	-	If used with receive allows an interface to operate with the attached device to send flow control packets If used with send the interface sends flowcontrol packets to a remote device if the device supports it
	off	-	Turns-off the attached devices (when used with receive) or the local ports (when used with send) ability to send flow-control packets to an interface or to a remote device respectively
	desired	-	Allows a local port to operate with an attached device that is required to send flow control packets or that may send the control packets, when used with receive option. Allows the local port to send administrative status to a remote device if the remote device supports it, when used with send option.
Mode	Interface Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	The default flow control for the interfaces are flowcontrol receive off flowcontrol send off		
Example	iss(config-if)# flowcontrol send on		
Related Commands	<ul style="list-style-type: none"> • show interfaces - Displays the interface status and configuration • show flow-control - Displays the flowcontrol information 		

4.36 tunnel mode

This command configures the tunnel interface with the associated parameters. The no form of the command deletes the tunnel interface and its associated parameters.

```
tunnel mode {gre|sixToFour|isatap|compat|ipv6ip} [config-id <ConfId(1-2147483647)>] source <TnlSrcIP/IfName> [dest <TnlDestIP>]
```

```
no tunnel mode {gre|sixToFour|isatap|compat|ipv6ip} [config-id <ConfId(1-2147483647)>] source <TnlSrcIP/IfName/IfIndex> [dest <TnlDestIP>]
```

Syntax Description	gre	- Sets the tunnel in Generic Router Encapsulation mode.
	sixToFour	- Sets the tunnel in six to four encapsulation mode.
	isatap	- Sets the tunnel in ISATAP Encapsulation mode.
	compat	- Sets the tunnel in IPv6 auto compatible encapsulation mode.
	ipv6ip	- Sets the tunnel in IPv6 over IPv6 configured encapsulation mode.
	config-id<ConfId(1-2147483647)>	- Sets an identifier to distinguish between multiple tunnels of the same encapsulation method, with same end-points. This value ranges between 1 and 2147483647.
	source<TnlSrcIP/IfName>	- Sets the local end point address of the tunnel
	dest<TnlDestIP>	- Sets the remote end point address of the tunnel

Mode Interface Configuration Mode (Tunnel interface mode)

Example iss(config-if)# tunnel mode ipv6ip config-id 1 source vlan1 dest 10.203.113.114

Related Command

- **show interfaces** - Displays the interface status and configuration

4.37 tunnel checksum

This command enables end-to-end checksumming of packets. The no form of the command disables end-to-end checksumming of packets.

tunnel checksum

no tunnel checksum

Mode Interface Configuration Mode (Tunnel interface mode)

Package Workgroup, Enterprise and Metro

Defaults disabled

Example `iss(config-if)# tunnel checksum`



This command is applicable only for GRE Encapsulation Method.

Related Command `show interfaces` - Displays the interface status and configuration

ISS

4.38 tunnel path-mtu-discovery

This command enables Path MTU discovery on Tunnel. The no form of the command disables Path MTU discovery on Tunnel.

```
tunnel path-mtu-discovery [age-timer {<integer (5-254)> | infinite}]
```

```
no tunnel path-mtu-discovery
```

Syntax Description	<integer (5-254)>	Configures timeout in minutes, after which the estimate of the PMTU is considered stale. This value ranges between 5 and 254.
	infinite	- Configures the PMTU timeout as infinite. Does not detect any increase in PMTU.

Mode Interface Configuration Mode (Tunnel interface mode)

Package Workgroup, Enterprise and Metro

Defaults Disabled

Example `iss(config-if)# tunnel path-mtu-discovery age-timer 5`

Related Command `show interfaces` - Displays the interface status and configuration

4.39 tunnel udlr

This command associates tunnel with a unidirectional interface. The no form of the command associates tunnel with a Bidirectional interface.

```
tunnel udlr {receive-only | send-only}
```

```
no tunnel udlr
```

Syntax	<code>receive-only</code>	- Sets the uni-directional tunnel as incoming only.
Description	<code>send-only</code>	- Sets the uni-directional tunnel as outgoing only.

Mode Interface Configuration Mode (Tunnel interface mode)

Package Workgroup, Enterprise and Metro

Example `iss (config-if)# tunnel udlr receive-only`

Related Command `show interfaces` - Displays the interface status and configuration

4.40 shutdown - physical/VLAN/port-channel/tunnel Interface

This command disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface. The no form of the command enables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.

shutdown

no shutdown

Mode Interface Configuration Mode for physical interface / port-channel/tunnel interface/OOB Interface
 VLAN Interface Mode for VLAN interface

Package Workgroup, Enterprise and Metro

Defaults The Physical Interface eth0 is enabled
 The interface VLAN 1 is enabled
 The Port-channel interface is disabled

Example `iss(config-if)# shutdown`



- All functions on the specified interface are disabled by the shutdown command
- If OOB interface is enabled, then the Physical Interface eth0 is disabled
- When the same network interface is used for OOB and NFS mounting, the operation done on OOB will have impact on NFS. For example, when interface eth0 is used for OOB and NFS mounting, executing shutdown command on the OOB interface will make the admin down and the NFS communication will be lost.

- Related Commands**
- `show spanning-tree - Summary, Blockedports, Pathcost, redundancy` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
 - `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
 - `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
 - `show spanning-tree - layer 2 gateway port` - Displays spanning tree information for all L2GPs enabled in the switch.
 - `show spanning-tree mst - CIST or specified mst Instance` -

Displays multiple spanning tree information for all MSTIs in the switch.

- **show interfaces** - Displays the interface status and configuration

ISS

4.41 debug interface

This command sets the debug traces for all the interfaces. The no form of the command resets the configured debug traces.

```
debug interface [track] [enetpkt dump] [ippkt dump] [arppkt dump] [trcerror] [os]
[failall] [buffer] [all]
```

```
no debug interface [track] [enetpkt dump] [ippkt dump] [arppkt dump] [trcerror]
[os] [failall] [buffer] [all]
```

Syntax description	track	-	Generates debug messages for all track messages.
	enetpkt dump	-	Generates debug messages for ethernet packet dump messages.
	ippkt dump	-	Generates debug messages for IP protocol related packet dump messages.
	arppkt dump	-	Generates debug messages for address resolution protocol related packet dump messages.
	trcerror	-	Generates debug messages for trace error messages.
	os	-	Generates debug messages for for OS resources. For example, when there is a failure in mem pool creation / deletion, this trace level is used
	failall	-	Generates debug messages for all failures including packet validation.
	buffer	-	Generates debug messages for buffer trace levels where packet buffer is used.i.e in cases wher packet is enqueued
	all	-	Generates debug messages for all kinds of traces.

Mode Privilege EXEC mode

Package Workgroup, Enterprise and Metro

Example iss# debug interface track

4.42 debug-logging

This command configures the displays of debug logs. The no form of the command displays debug logs in the console. Debug logs are directed to the console screen or to a buffer file, which can later be uploaded, based on the input.

```
debug-logging { console | file }
```

```
no debug-logging
```

Syntax Description	console	- Displays the debug logs in the console
	file	- Stores the debug logs in the file

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss(config)# debug-logging console

Related Commands

- **show debug-logging** - Displays the debug logs stored in file

ISS

4.43 incremental-save

This command enables/disables the incremental save feature.

```
incremental-save { enable | disable }
```

Syntax **enable** - Enables the incremental save feature.
Description

disable - Disables the incremental save feature.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults enable

Example `iss(config)# incremental-save enable`

Related **show nvram** - Displays the current information stored in the NVRAM.
Commands

4.44 auto-save trigger

This command enables / disables the auto save trigger function.

```
auto-save trigger { enable | disable }
```

Syntax	enable	- Enables the auto save trigger function.
Description	disable	- Disables the auto save trigger function.
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Defaults	disable	
Example	iss(config)# auto-save trigger enable	
Related Commands	show nvram - Displays the current information stored in the NVRAM.	

ISS

4.45 rollback

This command enables/disables the rollback function.

```
rollback { enable | disable }
```

Syntax	enable	- Enables the rollback function.
Description		

	disable	- Disables the rollback function.
--	----------------	-----------------------------------

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	enable
-----------------	--------

Example	iss(config)# rollback enable
----------------	------------------------------

Related Commands	show nvram - Displays the current information stored in the NVRAM.
-------------------------	---

4.46 shutdown ospf | ospf3 | bgp | isis

This command shutdowns the specified module.

```
shutdown { ospf | ospf3 | bgp | isis }
```

Syntax Description	ospf	- Open Shortest Path First module
	ospf3	- Open Shortest Path First version 3 module
	bgp	- Border Gateway Protocol module
	isis	- Intermediate System to Intermediate System module

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss(config)# shutdown ospf

Related Commands **start ospf |ospf3 |bgp |isis** - Starts the specified module

ISS

4.47 start ospf | ospf3 | bgp | isis

This command starts the specified module.

```
start { ospf | ospf3 | bgp | isis }
```

Syntax Description	ospf	- Open Shortest Path First module
	ospf3	- Open Shortest Path First version 3 module
	bgp	- Border Gateway Protocol module
	isis	- Intermediate System to Intermediate System module

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss(config)# start ospf

Related Commands **shutdown ospf |ospf3 |bgp |isis** - Shutdown the specified module

4.48 set switch maximum - threshold

This command sets the switch maximum threshold values of RAM, CPU, and Flash. This threshold value is represented in percentage and ranges between 1 and 100 percentage.

Trap message will be sent for the specified resource and the syslog message will be displayed, if the current resource usage crosses the maximum threshold limit.

This command is a complete standardized implementation of the existing command.

```
set switch maximum { RAM | CPU | flash } threshold <percentage (1-100)>
```

Syntax Description	RAM	- Sets the maximum threshold value for RAM.
	CPU	Sets the maximum threshold value for CPU.
	flash	- Sets the maximum threshold value for Flash memory.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults	RAM	- 100 percentage
	CPU	- 100 percentage
	flash	- 100 percentage

Example `iss(config)# set switch maximum RAM threshold 98`

Related Command `show env` - Displays the switch related information such as CPU, Flash and RAM usage, and also displays the current power and temperature of the switch

ISS

4.49 set switch temperature - threshold

This command sets the maximum and minimum temperature threshold values of the switch. This threshold value ranges between -14 and 40 degree Celsius.

This command is a complete standardized implementation of the existing command.

```
set switch temperature {min|max} threshold <celsius (-14 - 40)>}
```

Syntax	min	-	Minimum temperature value for the switch.
Description	max	-	Maximum temperature value for the switch.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	min	-	-14 degree Celsius
	max	-	40 degree Celsius
Example	<pre>iss(config)# set switch temperature min threshold -10</pre> <pre>iss(config)# set switch temperature max threshold 37</pre>		
Related Command	show env - Displays the switch related information such as CPU, Flash and RAM usage, and also displays the current power and temperature of the switch		

4.50 set switch power - threshold

This command sets the maximum and minimum threshold values of the switch power supply. This threshold value ranges between 100 and 230 Volts.

This command is a standardized implementation of the existing command.

```
set switch power {min|max} threshold <volts (100-230)>
```

Syntax	min	-	Minimum threshold value for switch power supply.
Description	max	-	Maximum threshold value for switch power supply.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults

min	-	100 Volts
max	-	230 Volts

Example iss(config)# set switch power min threshold 110

```
iss(config)# set switch power max threshold 220
```

Related Command **show env** - Displays the switch related information such as CPU, Flash and RAM usage, and also displays the current power and temperature of the switch

4.51 mac-learn-rate

This command configures the number of MAC entry indications to control plane from hardware, when hardware MAC learning is enabled.

The no form of the command removes the limit on number of unicast MAC entry indications (that is, limit value is set as 0) and resets the configured time interval to default value.

```
mac-learn-rate {<no of MAC entries(0-2147483647)>} [interval {<milliseconds(1-100000)>}]
```

no mac-learn-rate

Syntax Description	<no of MAC entries(0-2147483647)>	- Configures the maximum number of unicast dynamic MAC (L2) entries that can be learned in the switch within the specified time interval. The configured value takes effect on next timer restart, if this value is changed while the timer is running. This value is used to control the number of MAC entries indicated to control plane from the hardware, when hardware MAC learning is enabled. The value ranges between 0 and 2147483647. The value 0 represents that no limit is set in the switch. This limit value does not impose any restrictions on multicast / broadcast and dynamic / static / protocol (MMRP) MAC learning capability limits.
	interval	- Configures the time interval (in milli-seconds) for maximum number of MAC entries to be learned in the switch. The configured value takes effect from the next timer restart. The value ranges between 1 and 100000 milli-seconds.
Mode	Global Configuration mode	
Package	Workgroup, Enterprise and Metro	
Defaults	<no of MAC entries(0-2147483647)>	- 1000
	interval	- 1000
Example	iss(config)# mac-learn-rate 100 interval 500	
Related Commands	show mac-learn-rate - Displays the maximum limit on number of MAC learning indications to control plane from hardware and the MAC learning limit rate interval.	

4.52 system contact

This command sets the system contact information.

system contact <contact info>

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# system contact support@x.com`

Related Commands `show system information` - Displays system information.

ISS

4.53 system location

This command sets the system location.

system location <location name>

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss(config)# system location Controls

Related Commands **show system information** - Displays system information.

4.54 clear interfaces - counters

This command clears the interface counters.

```
clear interfaces [ <interface-type> <interface-id> ] counters
```

Syntax	interface-type	- Type of interface. This can be:
Description		<ul style="list-style-type: none">• FastEthernet• GigabitEthernet
	interface-id	- Physical interface ID including slot and port number.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss# clear interfaces counters	
Related Command	<ul style="list-style-type: none">• show interfaces - counters - Displays the interface statistics for each port.• show interfaces - Displays the interface status and configuration	

ISS

4.55 clear counters

This command clears the interface counters.

This command is a standardized implementation of the existing command and operates similar to that of the command `clear interfaces - counters`.

clear counters [<interface-type> <interface-id>]

Syntax Description	interface-type	- Type of interface. This can be: <ul style="list-style-type: none"> • FastEthernet • GigabitEthernet
	interface-id	- Physical interface ID including slot and port number.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss# clear counters	
Related Command	<ul style="list-style-type: none"> • show interfaces counters - Displays the interface statistics for each port. • show interfaces - Displays the interface status and configuration 	

4.56 show ip interface

This command displays the IP interface configuration.

```
show ip interface [vrf <vrf-name>] [Vlan <vlan-id(1-4094)> [switch <switch-name>]] [<interface-type><interface-id>] [loopback <loopback-id(0-100)>]
```

Syntax	vrf	-	Name of the VRF instance. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax
Description	Vlan<vlan-id(1-4094)>	-	Displays the IP interface configuration for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
	switch	-	Name of the switch context. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax
	<interface-type>	-	Displays the IP interface configuration for the specified type of interface. The interface can be: <ul style="list-style-type: none"> • 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. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan – Internal LAN created on a bridge per IEEE 802.1ap.
	<interface-id>	-	Displays the IP interface configuration for the 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. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan ID is provided, for interface type i-lan. For example: 1 represents i-lan ID.

ISS

**loopback<loopback-
id(0-100)>** - Displays the IP interface configuration for the specified loopback ID. This is a unique value that represents the specific loopback created. The value ranges between 0 and 100.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Default vrf - default

Example

```
iss# sh ip interface vrf default

vlan1 is up, line protocol is up
Internet Address is 12.0.0.1/8
Broadcast Address 12.255.255.255

vlan2 is up, line protocol is up
Internet Address is 15.0.0.1/8
Broadcast Address 15.255.255.255
```



If executed without the optional parameters this command displays the IP interface statistics and configuration for all the available interfaces.

Related Commands

- **ip address** - Sets the IP address for an interface
- **switchport** - Configures the port as switch port
- **release** - Releases, on the specified interface, the DHCP lease obtained for an IP address from a DHCP server.
- **renew** - Renews the DHCP lease for the interface specified.
- **show interfaces** - Displays the interface status and configuration

4.57 show authorized-managers

This command displays the configured authorized managers related information available in the switch.

```
show authorized-managers [ip-source < ip-address >]
```

Syntax `ip-source< ip-` - Displays the configured authorized manager related
Description `address >` information for the specified network or host address.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example `iss# show authorized-managers`

```
Ip Authorized Manager Table
```

```
-----  
Ip Address        : 10.0.0.4  
Ip Mask           : 255.255.255.255  
Services allowed : SSH  
Ports allowed    : Gi0/1  
Vlans allowed    : 2
```

Related Command `authorized-manager ip-source` - Configures an IP authorized manager

4.58 show interfaces

This command displays the interface status and configuration.

```
show interfaces [{ [<interface-type> <interface-id>] [{ description | storm-
control | flowcontrol | capabilities | status }] | { vlan <vlan-id(1-4094)>
[{{switch <switch-name>}}]} | port-channel <port-channel-id (1-65535)> | tunnel
<tunnel-id (0-128)>}]
```

Syntax	<interface-type>	-	<p>Displays the interface status and configuration for the specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> • 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. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
Description	<interface-id>	-	<p>Displays the interface status and configuration 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.</p> <p>For example: 0/1 represents that the slot number is 0 and port number is 1.</p>
	description	-	<p>Displays the admin status and protocol status for the specified interface.</p>
	storm-control	-	<p>Displays the broadcast, multicast, and unicast storm control suppression levels for the specified interface</p>
	flowcontrol	-	<p>Displays the flow control related statistics information for the specified interface.</p>
	capabilities	-	<p>Displays the interface type, interface speed, duplex operation and flowcontrol status for the specified interface.</p>

- status** - Displays the status, duplex details, speed and negotiation mode of the specified interface.

- vlan<vlan-id(1-4094)>** - Displays the interface status and configuration for the specified VLAN ID. This is a unique value that represents the specific VLAN created.
This value ranges between 1 and 4094.

- switch** - Name of the switch context. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax

- port-channel<port-channel-id (1-65535)>** - Displays the interface status and configuration for the specified port-channel ID. This is a unique value that represents the specific port-channel created. This value ranges between 1 and 65535.

- tunnel<tunnel-id (0-128)>** - Displays the interface status and configuration for the specified tunnel ID. This is a unique value that represents the specific tunnel created.. The value ranges between 0 and 128.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show interfaces gigabitethernet 0/1

```
Gi0/1 up, line protocol is up (connected)
Bridge Port Type: Customer Bridge Port
```

```
Hardware Address is 00:01:02:03:04:22
RARP Client is enabled
MTU 1500 bytes, Full duplex, 100 Mbps, Auto-Negotiation
HOL Block Prevention enabled.
```

```
Invalid flowcontrol Mode
```

```
Link Up/Down Trap is enabled
```

```
Reception Counters
```

```
Octets : 0
Unicast Packets : 0
Discarded Packets : 0
Error Packets : 0
Unknown Protocol : 0
```

```
Transmission Counters
```

```
Octets : 8266
Unicast Packets : 0
Discarded Packets : 0
Error Packets : 0
```

```
iss# show interfaces description
```

Interface	Status	Protocol	Description
Gi0/1	up	up	
Gi0/2	up	up	

```
iss# show interfaces gigabitethernet 0/2 storm-control
```

```
Gi0/2
DLF Storm Control          : Disabled
DLF Storm Control Limit    : 0

Broadcast Storm Control    : Enabled
Broadcast Storm Control    : 0

Multicast Storm Control    : Enabled
Multicast Storm Control    : 0
```

```
iss# show interfaces gigabitethernet 0/2 flow-control
```

Port	Tx FlowControl	Rx FlowControl	Tx Pause	Rx Pause	HC TxPause
Gi0/2	off	off	0	0	0

```
iss# show interfaces gigabitethernet 0/2 capabilities
```

```
Gi0/2
Type      : 10/100/1000 Base TX
Speed     : 10, 100, 1000, Auto
Duplex    : Half, Full
FlowControl : Send, Receive
```

```
iss# show interfaces gigabitethernet 0/2 status
```

Port	Status	Duplex	Speed	Negotiation
Gi0/2	connected	Full	100 Mbps	Auto

```
iss# show interfaces vlan 1
```

```
vlan1 up, line protocol is up (connected)
```

```
iss# show interfaces port-channel 2
```

```
po2 up, line protocol is up (connected)
```

```
iss# show interfaces tunnel 0
```

```
tunnel0 up, line protocol is up (connected)
Hardware is Tunnel
MTU 1480 bytes
Encapsulation TUNNEL
Tunnel Source 12.0.0.2, Destination 12.0.0.3
Tunnel Protocol/transport IPV6IP
Checksumming of packets Disabled
Path MTU Discovery Disabled
```

**Related
Commands**

- **interface** - Enters the interface mode and allows the user to execute all the commands that supports interface configuration mode.
- **Interface-configuration and deletion** - Configures interface such as out of band management, port channel, tunnel and so on
- **Snmp trap link-status** - Enables trap generation on the interface.
- **Storm-control** - Sets storm control rate for broadcast, multicast and DLF packets
- **flowcontrol** - Enables flow-control
- **show flow-control** - Displays the flow-control information
- **mac-addr** - Configures MAC address for the interface.
- **tunnelmode** - Configures the tunnel interface with the associated parameters.
- **tunnel checksum** - Enables end-to-end checksumming of packets.
- **tunnel path-mtu-discovery** - Enables Path MTU discovery on Tunnel.
- **tunnel udlr** - Associates tunnel with a unidirectional interface.
- **shutdown** - **physical/VLAN/port-channel/tunnel interface** - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.

4.59 show interfaces - counters

This command displays the interface statistics for each port.

```
show interfaces [{ <interface-type> <interface-id> | vlan < short (1-4094)>
[switch <switch-name>] | tunnel <tunnel-id(0-128)>}] counters
```

Syntax	<interface-type>	-	<p>Displays the interface incoming and outgoing traffic statistics for the specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> • 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. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
Description	<interface-id>	-	<p>Displays the interface incoming and outgoing traffic statistics 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 internal-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 internal-lan or port-channel ID is provided, for interface types internal-lan and port-channel. For example: 1 represents internal-lan and port-channel ID.</p>
	vlan	-	<p>VLAN identifier. This value ranges between 1 and 4094.</p>
	switch	-	<p>Name of the switch context. This value is a string of size 32.</p> <p>This feature has been included to adhere to the Industry Standard CLI syntax</p>
	tunnel<tunnel-id(0-128)>	-	<p>Displays the interface incoming and outgoing traffic statistics for the tunnel identifier. This is a unique value that represents the specific tunnel created. The value ranges between 0 and 128.</p>

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show interface counters

Port	InOctet	InUcast	InDiscard	InErrs	InHCOctet
Gi0/1	215710	805	1730	1	0
Gi0/2	0	0	0	0	0
Gi0/3	480494016	7507719	384586	0	0
Gi0/4	0	0	0	0	0
Gi0/5	2332132381	103548431	4985914	2	0
Gi0/6	0	0	0	0	0
Gi0/7	0	0	0	0	0
Gi0/8	0	0	0	0	0
Gi0/9	0	0	0	0	0
Gi0/10	0	0	0	0	0
Gi0/11	0	0	0	0	0
Gi0/12	0	0	0	0	0
Gi0/13	0	0	0	0	0
Gi0/14	455116678	7110937	7110935	1	0
Gi0/15	0	0	0	0	0
Gi0/16	0	0	0	0	0
Gi0/17	0	0	0	0	0
Gi0/18	0	0	0	0	0
Gi0/19	0	0	0	0	0
Gi0/20	0	0	0	0	0
Gi0/21	0	0	0	0	0
Gi0/22	0	0	0	0	0
Gi0/23	0	0	0	0	0
Gi0/24	0	0	0	0	0
vlan1	0	0	0	0	0

Port	OutOctet	OutUcast	OutDiscard	OutErrs	OutHCOctet
Gi0/1	516578823	8064080	0	0	0
Gi0/2	0	0	0	0	0
Gi0/3	1403553448	89039198	4486186	0	0
Gi0/4	0	0	0	0	0
Gi0/5	455902325	7123224	45	0	0
Gi0/6	0	0	0	0	0
Gi0/7	0	0	0	0	0
Gi0/8	0	0	0	0	0
Gi0/9	0	0	0	0	0
Gi0/10	0	0	0	0	0
Gi0/11	0	0	0	0	0
Gi0/12	0	0	0	0	0
Gi0/13	0	0	0	0	0
Gi0/14	2810	4	16645905	0	0
Gi0/15	0	0	0	0	0
Gi0/16	0	0	0	0	0
Gi0/17	0	0	0	0	0
Gi0/18	0	0	0	0	0
Gi0/19	0	0	0	0	0
Gi0/20	0	0	0	0	0

ISS

Interface Masters

TECHNOLOGIES
Innovative Network Solutions

Gi0/21	0	0	0	0	0	0
Gi0/22	0	0	0	0	0	0
Gi0/23	0	0	0	0	0	0
Gi0/24	0	0	0	0	0	0
vlan1	78	1	0	0	0	0

4.60 show system-specific port-id

This command displays the system specific index configuration for all interfaces for which this configuration is done.

show system-specific port-id

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show system-specific port-id

```
Interface PortID
-----
Slot0/1      45
```

Related Command **system-specific port-id** - Configures the system specific index for the port.

ISS

4.61 show custom-param

This command displays the custom-param configurations done in the switch.

show custom-param

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show custom-param

```
Slot0/1
AttrID   AttrValue
-----   -
4        5454

Slot0/2
AttrID   AttrValue
-----   -
2        2424

Type     Length  Value
-----   -
2        4       root
5        4       roo
```

Related Command **Set custom-param** - Configures the custom-param for a particular port.

4.62 show interface mtu

This command shows the Maximum Transmission Unit (MTU) of ports in the switch.

```
show interface mtu [{ Vlan <vlan-id (1-4094)> [switch <switch-name>] | port-
channel <port-channel-id (1-65535)> | <interface-type> <interface-id> }]
```

Syntax	Vlan	-	<p>Displays the MTU value for the specified VLAN ID. This is a unique value that represents the specific VLAN created.</p> <p>This value ranges between 1 and 4094.</p>
Description	switch	-	<p>Name of the switch context. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax. Feature not supported</p>
	port-channel<port-channel-id (1-65535)>	-	<p>Displays the MTU value for the specified port-channel ID. This is a unique value that represents the specific port-channel created.. This value ranges between 1 and 65535.</p>
	<interface-type>	-	<p>Displays the MTU value for the specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> • 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. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan – Internal LAN created on a bridge per IEEE 802.1ap.
	<interface-id>	-	<p>Displays the MTU value 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.</p> <p>For example: 0/1 represents that the slot number is 0 and port number is 1.</p> <p>Only i-lan ID is provided, for interface type i-lan. For example: 1 represents i-lan ID.</p>

ISS

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show interface mtu Vlan 1

```
vlan1    MTU size is 1500
```

Related Command **mtu frame size** - Configures the maximum transmission unit frame size for the interface

4.63 show interface bridge port-type

This command displays the bridge port type of all interfaces available in the switch.

```
show interface bridge port-type [{ port-channel <integer (1-65535)> |
<interface-type> <ifnum> }]
```

Syntax Description **port-channel** Displays the bridge port type for the specified port-channel ID. This is a unique value that represents the specific port-channel created. This value ranges between 1 and 65535.

<interface-type> Displays the bridge port type for the specified type of interface. The interface can be:

- 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.
- gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
- extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- i-lan – Internal LAN created on a bridge per IEEE 802.1ap.

<ifnum> Displays the bridge port type for the 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. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan ID is provided, for interface type i-lan. For example: 1 represents i-lan ID.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show interface bridge port-type
Gi0/1 Bridge port type is Customer Bridge Port
Gi0/2 Bridge port type is Customer Bridge Port
Gi0/3 Bridge port type is Customer Bridge Port
Gi0/4 Bridge port type is Customer Bridge Port
```

```
Gi0/5 Bridge port type is Customer Bridge Port
Gi0/6 Bridge port type is Customer Bridge Port
Gi0/7 Bridge port type is Customer Bridge Port
Gi0/8 Bridge port type is Customer Bridge Port
Gi0/9 Bridge port type is Customer Bridge Port
Gi0/10 Bridge port type is Customer Bridge Port
Gi0/11 Bridge port type is Customer Bridge Port
Gi0/12 Bridge port type is Customer Bridge Port
Gi0/13 Bridge port type is Customer Bridge Port
Gi0/14 Bridge port type is Customer Bridge Port
Gi0/15 Bridge port type is Customer Bridge Port
Gi0/16 Bridge port type is Customer Bridge Port
Gi0/17 Bridge port type is Customer Bridge Port
Gi0/18 Bridge port type is Customer Bridge Port
Gi0/19 Bridge port type is Customer Bridge Port
Gi0/20 Bridge port type is Customer Bridge Port
Gi0/21 Bridge port type is Customer Bridge Port
Gi0/22 Bridge port type is Customer Bridge Port
Gi0/23 Bridge port type is Customer Bridge Port
Gi0/24 Bridge port type is Customer Bridge Port
```

**Related
Command**

Bridge port-type - Configures the bridge port type

4.64 show nvram

This command displays the current information stored in the NVRAM.

show nvram

Mode Privileged EXEC Mode
Package Workgroup, Enterprise and Metro
Example iss# show nvram

```

Default IP Address           : 12.0.0.3
Default Subnet Mask         : 255.0.0.0
Default IP Address Config Mode : Manual
Default IP Address Allocation Protocol : DHCP
Switch Base MAC Address     : 00:03:02:03:04:01
Default Interface Name      : Gi0/1
Default RM Interface Name   : lo:3
Config Restore Option       : No restore
Config Save Option          : No save
Auto Save                   : Disable
Incremental Save            : Enable
Roll Back                   : Enable
Config Save IP Address      : 0.0.0.0
Config Save Filename        : iss.conf
Config Restore Filename     : iss.conf
PIM Mode                    : Sparse Mode
IGS Forwarding Mode        : MAC based
Cli Serial Console          : Yes
SNMP EngineID               : 80.00.08.1c.04.46.53
SNMP Engine Boots           : 47
Default VLAN Identifier     : 1

Stack PortCount             : 0
ColdStandby                 : Disable
  
```

Related Commands

- **default mode** - Configures the mode by which the default interface acquires its IP address
- **default restore-file** - Configures the default restoration file
- **default ip address** - Configures the IP address and subnet mask for the default interface
- **ip address** - Sets the IP address for an interface
- **base-mac** - Configures the base MAC address for the switch in the NVRAM
- **login authentication** - Sets the authentication method for user logins
- **write** - Writes the running-config to a file in flash, startup-configuration file or to a remote site
- **erase** - Clears the contents of the startup configuration or sets parameters in NVRAM to default values

- **default vlan id** - Sets default VLAN Identifier in NVRAM to be used at reboot of the switch
- **default ip address allocation protocol** - Configures the protocol by which the default interface acquires its IP address
- **incremental-save** - Enables/disables the incremental save feature.
- **auto-save trigger** - Enables/disables the auto save trigger function.
- **rollback** - Enables/disables the rollback function.
- **cli console** - Enables the console CLI through a serial port

4.65 show env

This command displays the switch related information such as CPU, Flash and RAM usage, and also displays the current power and temperature of the switch.

This command is a complete standardized implementation of the existing command.

show env {all | temperature | fan | RAM | CPU | flash | power}

Syntax	all	- Displays threshold information of all resources such as CPU, Flash, RAM, power and temperature.
Description	temperature	Displays the threshold information of the temperature.
	fan	Displays the threshold information of the fan.
	RAM	Displays the threshold information of the RAM.
	CPU	Displays the threshold information of the CPU.
	flash	Displays the threshold information of the Flash.
	power	Displays the threshold information of the power.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```

iss# show env all
RAM Threshold                : 98%
Current RAM Threshold        : 97%
CPU Threshold                 : 92%
Current CPU Threshold        : 0%
Fan Status 1                  : Operational
Min power supply              : 110v
Max power supply              : 220v
Current power supply          : 230v
Max Temperature               : 37C
Min Temperature               : -10C
Current Temperature           : 40C
Flash Threshold               : 90%
Current Flash Threshold       : 62%

iss# show env RAM
RAM Threshold                : 98%
Current RAM Threshold        : 97%

iss# show env power
Min power supply              : 110v
Max power supply              : 220v
Current power supply          : 230v
    
```

Related Commands

- **set switch maximum - threshold** - Sets the switch maximum threshold values of RAM, CPU, and Flash.

ISS

- **set switch temperature - threshold** - Sets the maximum and minimum temperature threshold values of the switch.
- **set switch power - threshold** - Sets the maximum and minimum threshold values of the switch power supply.

4.66 show system information

This command displays system information.

show system information

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show system information

```
Hardware Version           : 5.5.5
Firmware Version          : 6.1.0
Switch Name                : ISS
System Contact             : Interface Masters Ltd, India
System Location            : Interface Masters Ltd, India
Logging Option             : Console Logging
Login Authentication Mode  : Local
Config Save Status         : Not Initiated
Remote Save Status         : Not Initiated
Config Restore Status      : Not Initiated
```

- Related Commands**
- **write** - Writes the running-config to a file in flash, startup-configuration file or to a remote site
 - **erase** - Clears the contents of the startup configuration or sets parameters in NVRAM to default values
 - **login authentication** - Sets the authentication method for user logins
 - **system contact** - Sets the system contact information
 - **system location** - Sets the system location
 - **debug-logging** - Configures the displays of debug logs.

4.67 show flow-control

This command displays the flow-control information.

show flow-control [interface <interface-type> <interface-id>]

Syntax Description **<interface-type>** - Displays the flow-control information for the specified type of interface. The interface can be:

- 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.
- gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
- extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- i-lan – Internal LAN created on a bridge per IEEE 802.1ap.

<interface-id> Displays the flow-control information for the 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. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan ID is provided, for interface type i-lan. For example: 1 represents i-lan ID.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show flow-control interface gigabitethernet 0/2

```

Port          Tx FlowControl  Rx FlowControl  Tx Pause  Rx Pause  HC
TxPause HC RxPause
-----
Gi0/2        on              on              0         0         0
0
    
```



If this command is executed without the optional parameter it displays the flowcontrol information of the **Interface Masters ISS** router. Otherwise it displays the flowcontrol information of the specified interface.

Related Commands

- **show interfaces** - Displays interface status and configuration
- **flowcontrol** - Enables flowcontrol on an interface

4.68 show debug-logging

This command displays the debug logs stored in file.

show debug-logging

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss(config)# debug-logging file

```
iss(config)# exit
```

```
iss# debug spanning-tree events
```

```
iss# show debug-logging
```

```
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
```

Related Command **debug-logging** - Configures where debug logs are to be displayed

ISS

4.69 show debugging

This command displays state of each debugging option.

show debugging

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show debugging

```
Spanning Tree :
  Spanning tree timers related debugging is on
```

Related Commands

- **debug spanning-tree** - Provides spanning tree debugging support
- **debug dot1x** - Enables debugging of dot1x module
- **debug radius** - Enables RADIUS debugging options
- **debug ip igmp snooping** - Specifies the debug levels for the IGMP snooping module
- **debug ssh** - Sets the given trace levels for SSH
- **debug ssl** - Sets the given debug levels for SSL
- **debug vlan** - Enables the tracing of the VLAN submodule as per the configured debug levels.
- **debug garp** - Enables the tracing of the GARP submodule as per the configured debug levels.
- **debug ip dhcp client** - Enables the tracking of the DHCP client operations as per the configured debug levels.
- **debug ip dhcp relay** - Enables the debug level for tracing the DHCP Relay Module
- **debug ip dhcp server** - Enables the tracking of the DHCP server operations as per the configured debug levels.
- **debug ethernet-oam** - Enables/displays the debug level for the EOAM Module

4.70 show clock

This command displays the system date and time.

show clock

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show clock
Tue Oct 18 18:04:11 2005

Related Command **clock set** - Manages the system clock

4.71 show running-config

This command displays the current operating configuration in the system.

```
show running-config [{ syslog | dhcp | dvmrp | qos | stp [ switch
<context_name> ] | ecfm [switch <context_name>] | la | pnac | igs | mlds |
vlan <vlan-id(1-4094)> [ switch <context_name> ] | interface { port-channel
<port-channel-id(1-65535)> | <interfacetype> <interfacenum> | vlan <vlan-id(1-
4094)> } | ospf | rip | bgp | ipv6 | rip6 | ssh | ssl | acl | ip | pim | pimv6
| vrrp | snmp | radius | rmon | rm | mbsm | ospf3 | mpls | igmp | eoam | fm |
igmp-proxy | elmi | route-map | tacacs | qosxtd | tac | switch <context_name>
}]
```

Syntax Description	syslog	- Displays the configuration done in the syslog module
	dhcp	- Displays the configuration done in the DHCP module
	dvmrp	- Displays the configuration done in the DVMRP module
	qos	- Displays the configuration done in the QoS module
	stp	- Displays the configuration done in the STP module
	switch <context_name>	- Displays the configuration done in the context for the specified module. 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.
	ecfm	- Displays the configuration done in the ECFM module.
	la	- Displays the configuration done in the LA module
	pnac	- Displays the configuration done in the PNAC module

- igs** - Displays the configuration done in the IGS module
- mlds** - Displays the configuration done in the MLDS module
- vlan<vlan-id(1-4094)>** - Displays the configuration done for the specified VLAN ID. This is a unique value that represents the specific VLAN created.
This value ranges between 1 and 4094.
- port-channel
<port-channel-id(1-65535)>** - Displays the configuration done for the specified port channel ID. This is a unique value that represents the specific port channel created.
This value ranges between 1 and 65535.
- <interfacetype>** - Displays the configuration done for the specified type of interface. The interface can be:
- 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.
 - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
 - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
 - i-lan – Internal LAN created on a bridge per IEEE 802.1ap.
- <interfacenum>** - Displays the configuration done for the 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.
For example: 0/1 represents that the slot number is 0 and port number is 1.
Only i-lan ID is provided, for interface type i-lan.
For example: 1 represents i-lan ID.
- ospf** - Displays the configuration done in the OSPF module

- rip** - Displays the configuration done in the RIP module
- bgp** - Displays the configuration done in the BGP module
- ipv6** - Displays the configuration done in the IPv6 module
- rip6** - Displays the configuration done in the RIP6 module
- ssh** - Displays the configuration done in the SSH module
- ssl** - Displays the configuration done in the SSL module
- acl** - Displays the configuration done in the ACL module
- ip** - Displays the configuration done in the IP module
- pim** - Displays the configuration done in the PIM module
- vrrp** - Displays the configuration done in the VRRP module
- snmp** - Displays the configuration done in the SNMP module
- radius** - Displays the configuration done in the RADIUS module
- rmon** - Displays the configuration done in the RMON module
- rm** - Displays the configuration done in the RM module
- mbsm** - Displays the configuration done in the MBSM module
- ospf3** - Displays the configuration done in the OSPFv3 module

mpls	Displays the configuration done in the MPLS module
igmp	- Displays the configuration done in the IGMP module
eoam	- Displays the configuration done in the EOAM module
fm	- Displays the configuration done in the FM module
igmp-proxy	- Displays the configuration done in the IGMP proxy module
elmi	- Displays the configuration done in the ELMI module
route-map	- Displays the configuration done for the route map feature
tacacs	- Displays the configuration done in the TACACS module
qosxtd	- Displays the configuration done in the extended QoS module
tac	- Displays the configuration done in the TAC module

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example The output given below is only a fragment of the whole output. This output differs based on the modules that are configured.

```
iss# show running-config stp
Building configuration...
spanning-tree mode rst
interface gigabitethernet 0/1!
interface gigabitethernet 0/2!
```

```
interface gigabitethernet 0/3!
interface gigabitethernet 0/4!
interface gigabitethernet 0/5!
interface gigabitethernet 0/6!
interface gigabitethernet 0/7!
interface gigabitethernet 0/8!
interface gigabitethernet 0/9!
interface gigabitethernet 0/10!
interface gigabitethernet 0/11!
interface gigabitethernet 0/12!
interface gigabitethernet 0/13!
interface gigabitethernet 0/14!
interface gigabitethernet 0/15!
interface gigabitethernet 0/16!
interface gigabitethernet 0/17!
interface gigabitethernet 0/18!
interface gigabitethernet 0/19!
interface gigabitethernet 0/20!
interface gigabitethernet 0/21!
interface gigabitethernet 0/22!
interface gigabitethernet 0/23!
interface gigabitethernet 0/24!

end

iss# show running-config bgp

Building configuration...

router bgp 100
  bgp router-id 100.20.6.100
  bgp default ipv4-unicast
  redistribute static
  restart-reason softwareRestart
  neighbor 100.20.6.20 remote-as 200
  neighbor 100.20.6.20 update-source 100.20.6.100
```

```
neighbor 100.20.6.20 timers holdtime 240
neighbor 110.20.6.20 remote-as 300
neighbor 110.20.6.20 update-source 110.20.6.100
neighbor 110.20.6.20 timers holdtime 240!
```

end



If executed without the optional parameters this command displays the current active configurations, other than the default configurations of all the modules in all the interfaces.

Related Commands Related commands include the configuration commands of all the modules (given as parameters in the **show running-config** command)

ISS

4.72 show http server status

This command displays the http server status and HTTP port.

show http server status

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show http server status

```
HTTP server status : Enabled
HTTP port is      : 80
```

- Related Commands**
- **ip http port** – Sets the HTTP port
 - **set ip http** – Enables/disables HTTP

4.73 show system acknowledgement

This command displays acknowledgement statement for open sources used in the software.

show system acknowledgement

Mode Privileged EXEC Mode
Package Workgroup, Enterprise and Metro

Example iss# show system acknowledgement

The SSH functionality in this switch is implemented using the open source software from <http://www.openssh.org> developed by Theo de Raadt, Niels Provos, Markus Friedl, Bob Beck, Aaron Campbell and Dug Song. All copyrights listed at <http://www.openssh.org> apply.

The SSL functionality in this switch is implemented using the open source software from <http://www.openssl.org> which include software written by Eric A. Young and Tim J. Hudson. All copyrights listed at <http://www.openssl.org> apply.

This switch includes cryptographic software written by Eric A Young (eay@cryptsoft.com). This product includes software written by Tim J. Hudson (tjh@cryptsoft.com). PLEASE REMEMBER THAT EXPORT/IMPORT AND/OR USE OF STRONG CRYPTOGRAPHY SOFTWARE, PROVIDING CRYPTOGRAPHY HOOKS OR EVEN JUST COMMUNICATING TECHNICAL DETAILS ABOUT CRYPTOGRAPHY SOFTWARE IS ILLEGAL IN SOME PARTS OF THE WORLD. SO, WHEN YOU IMPORT THIS PACKAGE TO YOUR COUNTRY, RE-DISTRIBUTE IT FROM THERE OR EVEN JUST EMAIL TECHNICAL SUGGESTIONS OR EVEN SOURCE PATCHES TO THE AUTHOR OR OTHER PEOPLE YOU ARE STRONGLY ADVISED TO PAY CLOSE ATTENTION TO ANY EXPORT/IMPORT AND/OR USE LAWS WHICH APPLY TO YOU. THE AUTHORS OF OPENSSEAL ARE NOT LIABLE FOR ANY VIOLATIONS YOU MAKE HERE. SO BE CAREFUL, IT IS YOUR RESPONSIBILITY

Math library in this switch is implemented using the Open source software from Sun Microsystems, Inc. All copyrights listed at <http://www.radiks.net/~rhuebner/mathlib.html> apply.

Web Tree View Script (ftiens4.js) and Browser Detection Script (ua.js) in this switch are implemented using source code from <http://www.treeview.net>. All copyright listed at <http://www.treeview.net> apply.

ISS

4.74 show mac-learn-rate

This command displays the maximum limit on number of MAC learning indications to control plane from hardware and the MAC learning limit rate interval.

show mac-learn-rate

Mode Privileged EXEC mode

Package Workgroup, Enterprise and Metro

Example iss# show mac-learn-rate

```
Switch MAC Learn Limit Rate : 1000
```

```
Switch MAC Learn Limit Rate Interval: 1000
```

Related Commands **mac-learn-rate** - Configures the number of MAC entries indication to control plane from hardware, when hardware MAC learning is enabled.

4.75 port-isolation in_vlan_ID

This command enables the vlan traffic to be allowed in these configured egress ports when the ingress is this interface. The no form of the command disables the Port Isolation rule in this ingress interface.

```
port-isolation in_vlan_ID [{add|remove}] port_list
```

```
no port-isolation
```

Syntax	add	-	Configures the addition of the egress ports
Description	remove	-	Configures the removal of the egress ports
	port_list	-	Configures the list of ports through which the traffic is allowed. The ports can be either a physical or link aggregated port.
Mode	Interface configuration mode (We can configure only for physical ports or Link Aggregated port).		
Package	Workgroup, Enterprise and Metro		
Example	<pre>iss(config-if)# port-isolation 4094 add Gi0/1-10</pre>		
Related Commands	show port-isolation - Displays the Port Isolation table		

4.76 show port-isolation

This command displays the Port Isolation table.

show port-isolation [**ingress-port** <ifXtype> <ifnum>]

- | | | |
|---------------------------|---------------------|--|
| Syntax Description | ingress-port | <ul style="list-style-type: none"> - Ingress port refers to a physical or link aggregated port through which a packet ingress. • <ifXtype> Displays the type of interface. The interface can be: <ol style="list-style-type: none"> 1. fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. 2. gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. 3. extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. 4. internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. 5. port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. • <ifnum> Sets the 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 internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. |
|---------------------------|---------------------|--|

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show port isolation

```

Ingress Port      VlanId      StorageType      Egress List
=====
Gi0/1             -           Non-
Volatile         Gi0/2,Gi0/3,Gi0/4,Gi0/5,Gi0/6,Gi0/7,
                  Gi0/8,Gi0/9,Gi0/10,Gi0/11
Gi0/11           1000        Non-Volatile     Gi0/12,Gi0/13,Gi0/14, Gi0/15,
                  Gi0/16, Gi0/17,Gi0/18, Gi0/19,
                  Gi0/20
Gi0/7            -           Volatile         Gi0/12
    
```

Related Commands: **port-isolation in_vlan_ID [{add|remove}] port_list** - Enables the vlan traffic to be allowed in these configured egress ports when the ingress is this interface.

4.77 ENTITY MIB

Entity MIB is a standardized way of representing a single agent, which supports multiple instances of one MIB. With the Entity MIB support in ISS, all the instances of the MIBs registered with agent are identifiable, so that the NMS (Network Management System) can easily communicate with the particular instance / logical entity. Entity MIB also provides the complete hierarchal hardware component view to the user.

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

- set entity physical-index
- show entity logical
- show entity physical
- show entity lp-mapping
- show entity alias-mapping
- show entity phy-containment

4.77.1 set entity physical-index

This command configures the read-write objects of the physical components present in the system.

```
set entity physical-index <integer (1..2147483647)> [asset-id <SnmAdminString (Size (0..32))>] [serial-number <SnmAdminString (Size (0..32))>] [alias-name <SnmAdminString (Size (0..32))>] [uris <OCTET-STRING (Size (0..255))>]
```

```
no entity physical-index <integer (1-2147483647)> [assetId] [serial-number] [alias-name] [uris]
```

Syntax	integer	-	Index of the physical entity. This value ranges between 1 and 2147483647.
Description	asset-id	-	Asset tracking identifier for the physical entity. This value is a string of size varying between 0 and 32. Asset tracking identifier is not needed for the physical entities (such as repeater ports within a repeater module) that are not considered as a field replaceable unit by the vendor. A zero-length string is returned for these entities.
	serial-number	-	Vendor-specific serial number string for the physical entity. This value is a string of size varying between 0 and 32. Serial number string is not needed for the physical entities (such as repeater ports within a repeater module) that are not considered as a field replaceable unit by the vendor. A zero-length string is returned for these entities.
	alias-name	-	Alias name for the physical entity. This value provides a non-volatile handle for the entity. This value is a string of size varying between 0 and 32.
	uris	-	Additional identification information (that is URI (Uniform Resource Indicator) about the physical entity.
Mode	Global Configuration mode		
Package	Workgroup, Enterprise and Metro		
Defaults	assetId	-	Zero-length string, on initial instantiation of the physical entity.

- | | |
|---------------|--|
| serial-number | <ul style="list-style-type: none"> - Zero-length string, on initial instantiation of the physical entity, if a serial number is unknown or non-existent.
Correct vendor-assigned serial number, on initial instantiation of the physical entity, if the serial number is available to the SNMP agent. |
| alias-name | <ul style="list-style-type: none"> - Zero-length string, on initial instantiation of the physical entity.
The SNMP agent may also set the value to a locally unique default value. |

Example `set entity physical index 3`



- If write access is implemented for an instance of asset ID and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.
- If write access is implemented for an instance of the serial number string and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.
- If the agents cannot provide non-volatile storage for the serial number string, then the agents are not required to implement write access for the the serial number string object.
- Implementations that can correctly identify the serial numbers of all installed physical entities are not required to provide write access to the serial number string object
- If write access is implemented for an instance of the alias name and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.

Related Command

- `show entity physical` - Displays the physical entities
-

ISS

4.77.2 show entity logical

This command displays the logical entities.

```
show entity logical [index <integer (1..2147483647)>]
```

Syntax **index** - Index of the logical entity. This value ranges between 1 and 2147483647.
Description

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show entity logical index 1
Logical Index: 1
Logical Description: Interface Masters Linux Router Ver 1.0
Logical Type: stdpnac
Logical Community: default
Logical Transport Address:
Logical Transport Domain:
Logical Context Engine Id: 80:00:08:1c:04:46:64
Logical Context Name: default
```

Related Commands

- **switch** - Creates virtual context

ISS

4.77.4 show entity lp-mapping

This command displays the mapping of logical and physical entities.

show entity lp-mapping

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show entity lp-mapping

```
Logical Index - 1 is mapped to Physical Index- 10
Logical Index - 1 is mapped to Physical Index- 11
Logical Index - 2 is mapped to Physical Index- 10
Logical Index - 2 is mapped to Physical Index- 11
Logical Index - 3 is mapped to Physical Index- 10
```

Related Commands

- **map switch** - Maps the port to the Context

ISS

4.77.6 show entity phy-containment

This command displays the containment relationship of physical components.

show entity phy-containment [index <integer (1..2147483647)>]

Syntax Description **index** - Index of the physical entity. This value ranges between 1 and 2147483647.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show entity phy-containment

Physical Index - 1 contains the physical component with Index - 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9

Physical Index - 9 contains the physical component with Index - 10 , 11 , 12

Related Commands • **interface - configuration and deletion** - Configures interface such as out of band management, port channel, tunnel and so on

4.78 Target Specific Commands

This section describes the CLI commands executable in all types for targets for configuring system features. These commands cannot be executed in Linux environment.

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

- reload
- monitor session - source
- monitor session - destination
- no monitor session
- negotiation
- speed
- duplex
- storm-control
- rate-limit-output
- show monitor - local / range / all
- show monitor records
- show monitor

ISS

4.78.1 reload

This command restarts the switch.

reload

Mode Privileged EXEC Mode

Example iss# reload

4.78.2 monitor session - source

This command configures a source port / remote VLAN for a mirroring session. The no form of the command removes the source port / remote VLAN configuration of the mirroring session.

```
monitor session <session-id (1-20)> { source { interface <interface-type>
<interface-id> [{ rx | tx | both }] | tunnel <tunnel-id> [{rx|tx|both}] | vlan
<vlan_range> [switch <context_name> ] [{rx|tx|both} ] |mac-acl <acl-id> |ip-acl
<acl-id>|remote vlan <vlan-id> [switch <context_name>]}}
```

```
no monitor session <session-id (1-20)> { source { interface <interface-type>
<interface-id> [{rx|tx|both}] | tunnel <tunnel-id> [{rx|tx|both}] | vlan
<vlan_range> [switch <context_name> ] [{rx|tx|both}] |mac-acl <acl-id>|ip-acl
<acl-id> |remote vlan <vlan-id> [switch <context_name>]}}
```

Syntax Description	session-id	-	Configures the session number that is used to identify a session.
	interface	-	<p>Configures the source interface whose traffic to be mirrored. The details to be provided are:</p> <ul style="list-style-type: none"> • <interface-type> - Sets the type of interface. The interface can be: <ol style="list-style-type: none"> 1. 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. 2. gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. 3. extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • <interface-id> - Sets the 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.
	rx	-	Mirrors received traffic
	tx	-	Mirrors transmitted traffic
	both	-	Specifies the traffic direction to monitor. If the traffic direction is not specified, both transmitted and received traffic is mirrored.

ISS

- tunnel** - Specifies the tunnel for which traffic is to be mirrored in the mirroring session. The value ranges between 0 and 128.
- vlan** - Specifies the VLAN for which traffic is to be mirrored in for the mirroring session.
- switch** - Context / switch name. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- mac-acl** - Specifies the ID of the MAC ACL (Access Control List) to be mirrored. This value ranges between 1 and 65535.
- ip-acl** - Specifies the ID of the IP ACL to be mirrored. This value ranges between 1 and 65535.
- remote vlan** - Specifies the remote VLAN used for achieving remote monitoring. This value ranges between 1 and 4094.

Mode Global Configuration Mode

Example `iss(config)# monitor session 1 source interface gigabitethernet 0/2`



A port that is a member of a port-channel cannot be used a mirror-to port.

Related Command

- **monitor session - destination** - Configures a destination port / remote VLAN for a mirroring session
- **show monitor** - Displays port-monitoring information
- **show monitor - local / range / all** - Displays the mirroring information present in the system

4.78.3 monitor session - destination

This command configures a destination port / remote VLAN for a mirroring session. The no form of the command removes the destination port / remote VLAN configuration of the mirroring session.

```
monitor session <session-id (1-20)> destination { interface <interface-type>
<interface-id> | tunnel <tunnel-id> | remote vlan <integer(1-4094)> [switch
<string(32) >]}
```

```
no monitor session <session-id (1-20)> destination { interface <interface-
type> <interface-id> | tunnel <tunnel-id> | remote vlan <integer(1-4094)>
[switch <string(32) >]}
```

Syntax Description	session-id	- Specifies the index of the mirroring session. This value ranges between 1 and 20.
	interface	- Specifies the destination port for the mirroring session. <ul style="list-style-type: none"> • interface-type - Interface type. This can be: GigabitEthernet or FastEthernet or Port Channel. • interface-id – Interface identifier. This is a combination of slot number and port number.
	tunnel	- Specifies the destination tunnel on which mirrored traffic is to be sent for the mirroring session. The value ranges between 0 and 128.
	remote vlan	- Specifies the remote VLAN on which mirrored traffic is to be sent for the mirroring session. This value ranges between 1 and 4094.
	switch	- Context / switch name.
Mode	Global Configuration Mode	

Example `iss(config)# monitor session 1 destination interface gigabitethernet 0/1`



A port that is a member of a port-channel cannot be a mirror-to port.

- Related Command**
- **monitor session - source** - Configures a source port / remote VLAN for a mirroring session
 - **show monitor** - Displays port-monitoring information
 - **show monitor - local /range/all** - Displays the mirroring information present in the system

ISS

4.78.4 no monitor session

This command is used to remove the mirroring configuration.

```
no monitor session { session-range | local | session-id (1-20) }
```

Syntax Description	session-range	- Specifies the list of session for which mirroring configuration should be removed
	local	- Removes all the local mirroring configuration sessions
	session-id	- Specifies the index of the mirroring session. This value ranges between 1 and 20.

Mode Global Configuration Mode

Example iss(config)# no monitor session local

Related Command

- **show monitor - local /range/all** - Displays the mirroring information present in the system

4.78.5 negotiation

This command enables auto-negotiation on the interface.

The no form of the command disables auto-negotiation on the interface.

The port in which auto-negotiation is enabled, negotiates with the other end for port properties like speed, duplexity and so one. The normal port uses the port property values configured by the administrator.

negotiation

no negotiation

Mode Interface Configuration Mode

Example `iss(config-if)# negotiation`

ISS

4.78.6 speed

This command sets the speed of the interface. The no form of the command sets the speed of the interface to its default value.

speed { 10 | 100 | 1000 | 10000 | auto | nonegotiate }

no speed

Syntax Description	10	- Port runs at 10Mbps
	100	- Port runs at 100Mbps
	1000	- Port runs at 1000Mbps
	10000	- Port runs at 10000Mbps
	auto	- Port automatically configures its speed based on the peer switch. The switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value.
	nonegotiate	- Disable negotiation on the ports. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Interface Configuration Mode

Defaults auto

Example iss(config-if)# speed 100



- The Gigabit Ethernet port speed can be configured to 10, 100, or 1000 Mbps
- This command cannot be executed to manually set values, if the port is automatically negotiating the link parameters with its peer. In that case, use the command no-negotiation to disable auto-negotiation feature.

Related Commands

- **no negotiation** - Disables auto-negotiation on the interface.
- **duplex** - Configures the duplex operation

4.78.7 duplex

This command configures the duplex operation.

The no form of the command configures the duplex operation to the default value.

```
duplex { full | half | auto }
```

```
no duplex
```

Syntax Description	full	- Port is in full-duplex mode, that is data simultaneously communicates in both directions.
	half	- Port is in half-duplex mode, that is data can communicate in both directions, but only in one direction at a time.
	auto	- Port is in auto mode. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
Mode	Interface Configuration Mode	
Defaults	full	
Example	<pre>iss(config-if)# duplex half</pre>	
	<ul style="list-style-type: none"> • Applicability of this command depends on the device to which the switch is attached. • This command cannot be executed to manually set values, if the port is automatically negotiating the link parameters with its peer. In that case, use the command <code>no negotiation</code> to disable auto-negotiation feature. 	
Related Commands	<ul style="list-style-type: none"> • <code>no negotiation</code> - Disables auto-negotiation on the interface • <code>speed</code> - Sets the speed of the interface 	

ISS

4.78.8 storm-control

This command sets the storm control rate for broadcast, multicast-broadcast, DLF_multicast-broadcast and all packets.

The no form of the command sets storm control rate for broadcast, multicast-broadcast, DLF-multicast-broadcast and all packets to the default value.

Storm control for a type of packets depicts the maximum traffic of that kind that can be sent out on that interface. This feature is supported only on physical interfaces.

```
storm-control { broadcast | multicast | dlf } level <rate-value>
```

```
no storm-control { broadcast | multicast | dlf } level
```

Syntax Description	broadcast	-	Configures the storm-control for broadcast packets
	multicast	-	Configures the storm-control for both multicast and broadcast packets
	dlf	-	Configures the storm-control for unicast, multicast and broadcast packets
	level	-	Configures storm-control suppression level as a total number of packets per second. Example: If 128K is set, then the suppression level is 128 kilobytes per second.

Mode Interface Configuration Mode

Defaults Broadcast, multicast, and DLF storm control are disabled.

Example `iss(config-if)# storm-control broadcast level 1000`

Related Command `show interfaces` - Displays the interface status and configuration

4.78.9 rate-limit-output

This command enables the rate limiting and burst size rate limiting by configuring the egress packet rate of an interface.

The no form of the command disables the rate limiting and burst size rate limiting on an egress port.

```
rate-limit output [<rate-value>] [<burst-value>]
```

```
no rate-limit output [rate-limit] [burst-limit]
```

Syntax Description	rate-value	-	Configures the maximum rate (in kbps) at which packets can be sent out through the interface.
	burst-value	-	Configures the burst size in kilobytes with which the rate is to be implemented. The value is the product of the rate and interval at which rate is to be measured.

Mode Interface Configuration Mode

Defaults rate-value = 0

burst-value = 0

Example iss(config-if)# rate-limit output 64 32

ISS

4.78.10 show monitor - local / range / all

This command displays the mirroring information present in the system.

```
show monitor [{ session <session-id (1-20)> | local | range <session-list> |
all }] [detail]
```

Syntax	session-id	- Displays the mirroring information for the specified index of the mirroring session. This value ranges between 1 and 20.
Description	local	- Displays the mirroring information in the Flash.
	range	- Displays the mirroring information for the specified list of mirroring session.
	all	- Displays the mirroring information of all the sessions.
	detail	- Displays the detailed information regarding the session.

Mode Privileged EXEC Mode

Example

```
iss# show monitor session 1
Session      : 1
-----
Source Ports
Rx           : None
Tx           : None
Both        : 1, 2, 3, 4
Destination Ports : 5, 6, 7, 8

iss# show monitor session 3
Session      : 3
-----
Source Ports
Rx           : None
Tx           : None
Both        : 12
Destination Ports : 11
Rspan Type   : Source
Rspan Vlan Id : 1

iss# show monitor local
Session      : 1
-----
```

```

Source Ports
  Rx           : None
  Tx           : None
  Both         : 1,2,3,4
Destination Ports : 5, 6, 7, 8

```

```

Source Vlans
  Rx           : None
  Tx           : None
  Both         : None
Destination Ports : 10

```

```

Session      : 3
-----

```

```

Source Ports
  Rx           : None
  Tx           : None
  Both         : 12
Destination Ports : 11
Rspan Type      : Source
Rspan Vlan Id   : 1

```

```

Session      : 4
-----

```

```

Source Ports
  Rx           : None
  Tx           : None
  Both         : 13
Destination Ports : 14
Rspan Type      : Destination
Rspan Vlan Id   : 1

```

```

Session      : 5
-----

```

```

Src Mac ACL    : 1
Src IP ACL     : None
Destination Ports : 15

```

```

Session      : 6
-----

```

```

Src Mac ACL    : None
Src IP ACL     : 1
Destination Ports : 16

```

```

iss# show monitor all

```

```

Session      : 1
-----

```

```

Source Ports
  Rx           : None
  Tx           : None
  Both         : 1,2,3,4
Destination Ports : 5, 6, 7, 8

```

```

Source Vlans
  Rx           : None
  Tx           : None

```

```

    Both          : None
Destination Ports : 10

Session         : 3
-----
Source Ports
  Rx            : None
  Tx            : None
  Both          : 12
Destination Ports : 11
Rspan Type      : Source
Rspan Vlan Id   : 1

Session        : 4
-----
Source Ports
  Rx            : None
  Tx            : None
  Both          : 13
Destination Ports : 14
Rspan Type      : Destination
Rspan Vlan Id   : 1

Session        : 5
-----
Src Mac ACL     : 1
Src IP ACL      : None
Destination Ports : 15

Session        : 6
-----
Src Mac ACL     : None
Src IP ACL      : 1
Destination Ports : 16

```

Related Command

- **monitor session - source** - Configures a source port / remote VLAN for a mirroring session
- **monitor session - destination** - Configures a destination port / remote VLAN for a mirroring session
- **no monitor session** - Removes the mirroring configuration

4.78.11 show monitor records

This command displays the available records.

show monitor records

Mode Privileged EXEC Mode

Example

```
iss# show monitor records
Mirroring Record Information
-----
Maximum   Source Records      : 100
Available Source Records     : 95
Maximum   Destination Records : 100
Available Destination Records : 94
```

ISS

4.78.12 show monitor

This command displays port-monitoring information.

show monitor [session (1-10)] [detail]

Syntax Description **session** - Session number. This value ranges between 1 and 10. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

detail - Detailed information regarding the session. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Privileged EXEC Mode

Example iss# show monitor

```
Port Monitoring is enabled
Monitor Port : Gi0/2
Port      Ingress-Monitoring      Egress-Monitoring
Gi0/1      Disabled                        Disabled
Gi0/2      Enabled                          Enabled
Gi0/3      Disabled                        Disabled
Gi0/4      Disabled                        Disabled
Gi0/5      Disabled                        Disabled
Gi0/6      Disabled                        Disabled
```

Related Command **monitor session - source** - Enables port-mirroring in the switch

4.79 BCM Specific Commands

This section describes the CLI commands executable only in BCM target for configuring system features.

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

- storm-control
- rate-limit-output

ISS

4.79.1 storm-control

This command sets the storm control rate for broadcast, multicast and DLF packets and the no form of the command sets storm control rate for broadcast, multicast and DLF packets to the default value.

```
storm-control { broadcast |multicast | dlf } level <rate-value>
```

```
no storm-control { broadcast |multicast | dlf } level
```

Syntax Description	broadcast	- Broadcast packets
	multicast	- Multicast packets
	dlf	- Unicast packets
	level	- Storm-control suppression level as a total number of bits per second.

Mode Interface Configuration Mode

Defaults Broadcast, multicast, and dlf storm control are disabled.

Example `iss(config-if)# storm-control broadcast level 1000`



- The rate must be specified in terms of packets per second
- Storm control is supported only on physical interfaces

Related Command `show interfaces` - Displays the interface status and configuration

4.79.2 rate-limit-output

This command enables the rate limiting and burst size rate limiting by configuring the egress packet rate of an interface and the no form of the command disables the rate limiting and burst size rate limiting on an egress port.

```
rate-limit output [<rate-value>] [<burst-value>]
```

```
no rate-limit output [rate-limit] [burst-limit]
```

Syntax	rate-value	-	Line rate in kbps
Description	burst-value	-	Burst size value in kbps
Mode	Interface Configuration Mode		
Defaults	rate-value	=	0
	burst-value	=	0
Example	iss(config-if)# rate-limit output 64 32		

ISS

4.80 CXE Specific Commands

This section describes the CLI commands executable only in CXE target for configuring system features.

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

- storm-control

4.80.1 storm-control

This command sets the storm control rate for broadcast, multicast and DLF packets and the no form of the command sets storm control rate for broadcast, multicast and DLF packets to the default value.

```
storm-control { broadcast |multicast | dlf } level <rate-value>
```

```
no storm-control { broadcast |multicast | dlf } level
```

Syntax Description	broadcast	- Broadcast packets
	multicast	- Multicast packets
	dlf	- Unicast packets
	level	- Storm-control suppression level as a total number of bits per second.

Mode Interface Configuration Mode

Defaults Broadcast, multicast, and dlf storm control are disabled.

Example `iss(config-if)# storm-control broadcast level 1000`



- The rate must be specified in terms of packets per second
- Storm control is supported only on physical interfaces

Related Command `show interfaces` - Displays the interface status and configuration

ISS

4.81 Marvell 6095 Specific Commands

This section describes the CLI commands executable only in Marvell 6095 target for configuring system features.

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

- storm-control
- rate-limit-output

4.81.1 storm-control

This command sets the storm control rate for broadcast, multicast and DLF packets and the no form of the command sets storm control rate for broadcast, multicast and DLF packets to the default value.

```
storm-control { bcast | mcast_bcast | dlf_mcast_bcast | all } level { 128K | 256K | 512K | 1M | 2M | 4M | 8M | 16M | 32M | 64M | 128M | 256M }
```

```
no storm-control
```

Syntax Description	bcast	- Configures the storm-control for broadcast packets
	mcast_bcast	- Configures the storm-control for both multicast and broadcast packets
	dlf_mcast_bcast	- Configures the storm-control for unicast, multicast and broadcast packets
	all	Configures the storm-control for all types of packets
	level	- Configures storm-control suppression level as a total number of packets per second. Example: If 128K is set, then the suppression level is 128 kilobytes per second.

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Broadcast, multicast, and DLF storm control are disabled.

Example `iss(config-if)# storm-control bcast level 256K`

Related Command `show interfaces` - Displays the interface status and configuration

ISS

4.81.2 rate-limit-output

This command enables the rate limiting and burst size rate limiting by configuring the egress packet rate of an interface and the no form of the command disables the rate limiting and burst size rate limiting on an egress port.

```
rate-limit output [<rate-value>] [<burst-value>]
```

```
no rate-limit output [rate-limit] [burst-limit]
```

Syntax Description	rate-value	-	Line rate in kbps
	burst-value	-	Burst size value in kbps

Mode Interface Configuration Mode

Defaults	rate-value	=	0
	burst-value	=	0

Example iss(config-if)# rate-limit output 64 32

4.82 xCAT Specific Commands

This section describes the CLI commands executable only in xCAT target for configuring system features.

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

- storm-control
- rate-limit-output

ISS

4.82.1 storm-control

This command sets the storm control rate for broadcast, multicast and DLF packets and the no form of the command sets storm control rate for broadcast, multicast and DLF packets to the default value.

```
storm-control { broadcast | multicast | dlf } level <rate-value>
```

```
no storm-control { broadcast | multicast | dlf } level
```

Syntax Description	broadcast	- Broadcast packets
	multicast	- Multicast packets
	dlf	- Unicast packets
	level	- Storm-control suppression level as a total number of bits per second.

Mode Interface Configuration Mode

Defaults Broadcast, multicast, and dlf storm control are disabled.

Example `iss(config-if)# storm-control broadcast level 1000`



- The rate must be specified in terms of packets per second
- Storm control is supported only on physical interfaces

Related Command `show interfaces` - Displays the interface status and configuration

4.82.2 rate-limit-output

This command enables the rate limiting and burst size rate limiting by configuring the egress packet rate of an interface and the no form of the command disables the rate limiting and burst size rate limiting on an egress port.

```
rate-limit output [<rate-value>] [<burst-value>]
```

```
no rate-limit output [rate-limit] [burst-limit]
```

Syntax	rate-value	-	Line rate in kbps
Description	burst-value	-	Burst size value in kbps
Mode	Interface Configuration Mode		
Defaults	rate-value	=	0
	burst-value	=	0
Example	iss(config-if)# rate-limit output 64 32		

Chapter

5

VCM

VCM (Virtual Context Manager) enables protocols (such as STP, VLAN, IPv6, OSPFv3, IPv4 , and so on) to work with multiple instance of switches and routers. In addition, the Virtual context manager provides configurations to create/delete the virtual contexts in the system and also to add/remove the interfaces (physical ports or logical IP interfaces) to/from the virtual contexts.

Multiple Instance support is achieved by extending the functionality of the protocols, so that the protocol functionality is extended for all the virtual contexts. Configuration of the protocols that are instantiated is possible through SNMP/ CLI.

The protocol modules can be enabled or disabled per virtual switch / router in the system by means of MIB object configuration from the SNMP Manager/CLI Interface.



This module is specific to Multiple Instance.

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

- ip vrf
- ip vrf forwarding
- switch
- map switch
- set owner
- show ip vrf
- show switch
- show owner
- show switch map info

5.1 ip vrf

This command creates VRF instance. The no form of the command deletes the VRF instance.

```
ip vrf <vrf-name>
```

```
no ip vrf <vrf-name>
```

Syntax	vrf	-	Name of the VRF instance. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax.
Description			

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults VRF named as **default** is created.

Example `iss(config)# ip vrf vrf1`

- Related Commands**
- `ip redirects` – Enables sending ICMP
 - `ip unreachable` – Enables sending ICMP unreachable message
 - `ip mask-reply` – Enables sending ICMP Mask Reply messages
 - `ip echo-reply` – Enables sending ICMP Echo Reply messages
 - `maximum-paths` – Sets the maximum number of multipaths
 - `traffic-share` - Enables traffic sharing
 - `ip path mtu discover` – Enables path mtu discovery
 - `ip path mtu` – Sets the MTU for usage in PMTU Discovery
 - `ping- ip address` - Sends echo messages
 - `ip route` – Adds a static route
 - `ip routing` – Enables IP routing
 - `ip default-ttl` - Sets the Time-To-Live (TTL) value
 - `arp timeout` – Sets the ARP (Address Resolution Protocol) cache timeout
 - `arp - ip address` – Adds a static entry in the ARP cache
 - `ip arp max-retries` – Sets the maximum number of ARP request retries

- `ipv6 unicast-routing` - Enables unicast routing
- `ipv6 - static routes` - Configures static routes
- `ipv6 - neighbor` - Configures a static entry in the IPv6 neighbor cache table
- `ipv6 default - hop limit` - Defaults hop limit for IPv6 Datagrams
- `ping ipv6` - Sends IPv6 echo messages
- `debug ipv6` - Enables IPv6 Trace
- `tracert6` - Traces route to the destination
- `clear ipv6 neighbors` - Removes all the entries in the IPv6 neighbor table
- `clear ipv6 traffic` - Removes all the entries in the IPv6 traffic table
- `clear ipv6 route` - Removes all the entries in IPv6 route table
- `router rip` - Enters the router configuration mode
- `debug ip rip` - Sets the debug level for RIP module
- `router ospf` - Enables OSPF routing process
- `debug ip ospf` - Sets the OSPF debug level
- `export ospfv3` - Enables redistribution of OSPF area/External routes to the protocol
- `redistribute-policy - IPv6` - Adds the IPv6 permit/deny Redistribution Policy
- `default redistribute-policy - IPv6` - Sets the default behavior of the RRD6 Control Table
- `ipv6 router ospf` - Enables the OSPFv3 routing protocol
- `debug ipv6 ospf - pkt` - Sets the trace levels
- `show ip vrf` - Displays the virtual context table entries

ISS

5.2 ip vrf forwarding

This command maps the IPv4 / IPv6 interface to the context. The no form of the command unmaps the IPV4 / IPV6 interface from the context.

```
ip vrf forwarding <vrf-name>
```

```
no ip vrf forwarding <vrf-name>
```

Syntax	vrf	-	Name of the VRF instance. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax.
Description			

Mode	Interface Configuration Mode.
	. This command can be executed only in the VLAN Interface Configuration Mode.

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	Default VRF (default) is mapped to the interface vlan 1.
-----------------	---

Example	iss(config-if)# ip vrf forwarding vrf1
----------------	--

Related Commands	<ul style="list-style-type: none"> • ip route – Adds a static route • arp - ip address – Adds a static entry in the ARP cache • ipv6 - static routes - Configures static routes • ipv6 - neighbor - Configures a static entry in the IPv6 neighbor cache table • ping ipv6 - Sends IPv6 echo messages • show ip vrf - Displays the virtual context table entries
-------------------------	--

ISS

5.4 map switch

This command maps the port to the Context and the no form of the command unmaps the port from the Context.

map switch <name>

no map switch <name>

Mode Interface Configuration Mode

Package Metro

Example `iss(config-if)# map switch customer`

- Related Command**
- `set port mvrp / mmrp` - Enables / disables the MVRP / MMRP application on the port
 - `set port mvrp / mvrp periodictimer` - Enables / disables the periodic timer on the port
 - `set port mvrp - participant` - Sets the participant type on a port
 - `set port mvrp applicant` - Sets the MMRP applicant administrative control status of a port
 - `set port mvrp applicant` - Sets the MVRP applicant administrative control status of a port
 - `set port mvrp timer / set port mvrp timer` - Sets MRP timer on the port
 - `set vlan / mac notify failed-registration` - Enables / disables the trap for notifying VLAN / MAC failed-registrations
 - `clear mvrp / mvrp / mmrp statistics` - Resets MRP statistics values
 - `clear mvrp / mmrp configuration` - Clears MRP configurations and resets context or port related MVRP / MMRP objects to its default values
 - `set port mvrp registration` - Configures the registrar admin control in a port
 - `mrp vlan restricted` - Enables / disables the restricted VLAN registration on the port
 - `mrp mac-address restricted` - Enables / disables restricted MAC address registration on the port
 - `show switch` - Displays the virtual context table entries

- `show entLPmapping list` - Displays the mapping of logical and physical entities

ISS

5.5 set owner

This command sets the owner of the context.

set owner <owner-name>

Mode Virtual Context Configuration Mode

Package Metro

Example iss# set owner Interface Masters

Related Command **show owner** - Displays the owner of the given port.

5.6 show ip vrf

This command displays the VRF instances table entries.

show ip vrf [{**brief** | **detail** | **interfaces**}] [**<vrf-name>**]

Syntax Description	brief	-	Brief information of the virtual context table entries
	detail	-	Detailed information of the virtual context
	interfaces	-	Interfaces related information of the virtual context
	vrf	-	Name of the VRF instance. This value is a string of size 32.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Default vrf - default

Example

```

iss# sh ip vrf
Virtual Context Table
-----
VcId  VRF-Name          Interfaces
----  -
0     default          vlan1, vlan2
1     vr1              vlan3
  
```

```

iss# sh ip vrf vr1
Virtual Context Table
-----
VcId  VRF-Name          Interfaces
----  -
1     vr1              vlan3
  
```

```

iss# sh ip vrf interfaces
Interface map table
-----
IfName    VcNum  Vc-Name
-----
vlan1     0      default
vlan2     0      default
vlan3     1      vr1
  
```

- Related Commands**
- **ip vrf** - Creates VRF instance
 - **ip vrf forwarding** - Maps the IPV4 / IPV6 interface to the context

ISS

5.7 show switch

This command displays the virtual context table entries.

show switch [{**brief** | **detail** | **interfaces**}] [**name**]

Syntax Description	brief	- Brief information of the virtual context
	detail	- Detailed information of the virtual context
	interfaces	- Interfaces related information of the virtual context
	name	- Context/Switch Name

Mode Privileged EXEC Mode

Package Metro

Example iss# show switch interfaces

Interface map table

IfIndex	VcNum	Vc-Name	LocalPortId
Gi0/1	1	cust1	1
Gi0/2	1	cust1	2
Gi0/3	1	cust1	3
Gi0/4	1	cust1	4
Gi0/5	1	cust1	5
Gi0/6	1	cust1	6
Gi0/7	2	cust2	1
Gi0/8	2	cust2	2
Gi0/9	2	cust2	3
Gi0/10	2	cust2	4
Gi0/11	2	cust2	5
Gi0/12	2	cust2	6
Gi0/13	3	cust3	1
Gi0/14	3	cust3	2
Gi0/15	3	cust3	3
Gi0/16	3	cust3	4
Gi0/17	3	cust3	5
Gi0/18	3	cust3	6
Gi0/49	0	default	1

iss# show switch detail

```
Switch Name : default
Switch Context-Id : 0
Switch MAC-Address : 00:01:02:03:04:01
Next Free Local Port-Id : 2
Ports present in this context:
    Gi0/49 with LocalPort Id as 1
```

```
Switch Name : cust1
Switch Context-Id : 1
Switch MAC-Address : 00:01:02:03:04:02
Next Free Local Port-Id : 7
Ports present in this context:
    Gi0/1 with LocalPort Id as 1
    Gi0/2 with LocalPort Id as 2
    Gi0/3 with LocalPort Id as 3
    Gi0/4 with LocalPort Id as 4
    Gi0/5 with LocalPort Id as 5
    Gi0/6 with LocalPort Id as 6
```

```
Switch Name : cust2
Switch Context-Id : 2
Switch MAC-Address : 00:01:02:03:04:03
Next Free Local Port-Id : 7
Ports present in this context:
    Gi0/7 with LocalPort Id as 1
    Gi0/8 with LocalPort Id as 2
    Gi0/9 with LocalPort Id as 3
    Gi0/10 with LocalPort Id as 4
    Gi0/11 with LocalPort Id as 5
    Gi0/12 with LocalPort Id as 6
```

```
Switch Name : cust3
Switch Context-Id : 3
Switch MAC-Address : 00:01:02:03:04:04
Next Free Local Port-Id : 7
Ports present in this context:
    Gi0/13 with LocalPort Id as 1
    Gi0/14 with LocalPort Id as 2
    Gi0/15 with LocalPort Id as 3
    Gi0/16 with LocalPort Id as 4
    Gi0/17 with LocalPort Id as 5
    Gi0/18 with LocalPort Id as 6
```

- Related Commands**
- **switch** - Creates virtual context
 - **map switch**- Maps the port to the Context

ISS

5.8 show owner

This command displays the owner of the given port.

```
show owner < virtual context-id>
```

Syntax	<code>virtual context-</code>	-	Context ID. This can be any value in the range 1 and 4094.
Description	<code>id</code>		
Mode	Privileged EXEC Mode		
Package	Metro		
Example	<pre>iss# show owner 1</pre> <p>The owner of the port 1 is admin</p>		
Related Commands	<code>set owner</code> - Sets the owner of the context.		

5.9 show switch map info

This command displays the list of switch instances to which a physical or port channel interface is mapped.

```
show switch map info [<interface-type> <interface-id>]
```

Syntax	interface-type	- Interface type.
Description	interface-id	- Interface identifier.
Mode	Privileged EXEC Mode	

Package Metro

```
Example
iss# show switch map info
Port Context Mapping Info
=====
-----
Port           : Gi0/1
Primary Context : default
Secondary Contexts : VcName      SispPort
                   -----
                   cust1        -    sisp1
-----
Port           : Gi0/2
Primary Context : default
Secondary Contexts : VcName      SispPort
                   -----
                   cust1        -    sisp2
                   cust2        -    sisp3
-----
```

5.10 SISP

SISP (Switch Instance Shared Port) feature provides support for sharing a physical port or port channel to more than one context in a switch. The context in which physical port or port channel is mapped is called primary context and this physical port or port channel can be shared by a Sisp port in some other context called as secondary context of physical interface. This is achieved with a limitation that, all the ports should be in different VLAN and port mapped to one MST instance cannot mapped to same instance of other context through VLAN to instance mapping. For other protocol limitations, please refer SISP config user manual.

The list of commands for the configuration of SISP is as follows:

- shutdown switch-instance-shared-port
- switch-instance-shared-port
- map sisp
- show switch-instance-shared-port
- show switch-instance-shared-port vlan info

5.10.1 shutdown switch-instance-shared-port

This command shuts down SISP (Switch Instance Shared Port) feature in the switch. The no form of the command starts SISP feature in the switch.

shutdown switch-instance-shared-port

no shutdown switch-instance-shared-port

Mode Global Configuration Mode

Package Metro

Defaults shutdown

Example `iss(config)# shutdown switch-instance-shared-port`



- When SISP is shutdown in the switch, interfaces can be mapped to only one switch instance atmost.
- When SISP is started, interfaces can be mapped to more than one switch instance through appropriate SISP configurations.

Related Command `show switch-instance-shared-port` - Displays the SISP feature Start/Shutdown status as well as the per port SISP enable/disable status in the switch.

ISS

5.10.2 switch-instance-shared-port

This command enables/disables SISP on this interface.

```
switch-instance-shared-port { enable | disable }
```

Mode Interface Configuration Mode

Package Metro

Defaults disable

Example `iss(config-if)# switch-instance-shared-port enable`



When enabled, this interface can be mapped to more than one switch instance.

Related Command `show switch-instance-shared-port` - Displays the SISP feature Start/Shutdown status as well as the per port SISP enable/disable status in the switch.

5.10.3 map sisp

This command maps a physical interface to a secondary switch instance and assigns a logical-port number for this association. Any port specific configurations for this physical interface in the secondary context has to be done against this logical-port number. The no form of the command unmaps a physical port from a secondary switch instance. If the SISP ID (or) switch name is given. Otherwise, the physical port will be unmapped from all the secondary switch instances.

```
map sisp < interface-id (1-65535)> switch <name>
```

```
unmap sisp [{id <integer (1-65535)> | switch <name>}]
```

Syntax	interface-id	-	Interface identifier
Description	switch	-	Switch name to identify a switch

Mode Interface Configuration Mode

Package Metro

Example iss(config-if)# map sisp 40 switch test

Related Command **show switch map info** - Displays the list of switch instances to which a physical or port channel interface is mapped.

ISS

5.10.4 show switch-instance-shared-port

This command displays the SISP feature enable/disable status as well as the per port SISP enable/disable status in the switch.

```
show switch-instance-shared-port [interface <interface-type> <interface-id>]
```

Syntax **interface-type** - Interface type
Description

interface-id - Interface ID

Mode Privileged EXEC Mode

Package Metro

Example iss# show switch-instance-shared-port

```
SISP feature is globally started

Gi0/1      Enabled
Gi0/2      Enabled
```

Related Commands

- **shutdown switch-instance-shared-port** - Shuts down SISP (Switch Instance Shared Port) feature in the switch.
- **switch-instance-shared-port** - Enables/disables SISP feature on this interface.

5.10.5 show switch-instance-shared-port vlan info

This command displays context classification info of a packet through the port/port channel port. The VLAN in the incoming packet on the particular interface is compared against this Vlan membership information, to determine the switch instance in which the traffic has to be processed.

```
show switch-instance-shared-port vlan info [<interface-type> <interface-id>]
```

Syntax **interface-type** - Interface type
Description

interface-id - Interface ID

Mode Privileged EXEC Mode

Package Metro

Example iss# show switch-instance-shared-port vlan info

```
Port Vlan Context Mapping Information
```

Port	Vlan ID	Vc-Name
Gi0/1	1,2,3 4,5	default cust1
Gi0/2	1 4,5	default cust1

Related Commands

- **show vlan** - Displays VLAN global status variables.
- **show switch map infor** - Displays the list of switch instances to which a physical or port channel interface is mapped.

Chapter

6

RADIUS

RADIUS (Remote Authentication Dial-In User Service), widely used in network environments, is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for embedded network devices such as routers, modem servers, switches and so on. RADIUS is currently the de-facto standard for remote authentication. It is very prevalent in both new and legacy systems. It is used for several reasons:

- RADIUS facilitates centralized user administration(Authentication, Authorization and Accounting).
- RADIUS consistently provides some level of protection against an active attacker.

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

- radius-server host
- debug radius
- show radius server
- show radius statistics

6.1 radius-server host

This command configures the RADIUS client with the parameters (host, timeout, key, retransmit) and the no form of the command deletes RADIUS server configuration.

```
radius-server host {ipv4-address | ipv6-address | host-name} [auth-port
<integer(1-65535)>] [acct-port <integer(1-65535)>] [timeout <1-120>]
[retransmit <1-254>] [key <secret-key-string>] [primary]
```

```
no radius-server host {ipv4-address | ipv6-address | host-name} [primary]
```

Syntax	ipv4-address	-	IPv4 address of the RADIUS server host.
Description	ipv6-address	-	IPv6 address of the RADIUS server host.
	host-name	-	DNS (Domain Name System) name of the RADIUS server host. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
	auth-port	-	Specifies the UDP (User Datagram Protocol) destination port for authentication requests.
	acct-port	-	Specifies the UDP destination port for accounting requests.
	timeout		Configures the time period in seconds for which a client waits for a response from the server before re-transmitting the request.
	retransmit	-	Configures the maximum number of attempts the client undertakes to contact the server
	key	-	Configures the Per-server encryption key. Specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server. The Maximum length of the string is 46.
	primary	-	Sets the RADIUS server as the primary server. Only one server can be configured as the primary server. Any existing primary server will be replaced, when the command is executed with this option.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults timeout - 3 seconds

retransmit - 3 attempts

key - empty string

Example `iss(config)# radius-server host 10.0.0.1 key pass`

- Related Commands**
- **aaa authentication dot1x default** - Enables the dot1x local authentication or RADIUS server based remote authentication method for all ports
 - **show radius server** - Displays RADIUS server configuration
 - **show radius statistics** - Displays RADIUS statistics

ISS

6.2 debug radius

This command enables RADIUS debugging options. The no form of the command disables RADIUS debugging options. The radius debug traces capture error information and failure messages in the server. These are registered in a log file for future reference. Each trace has to be enabled individually.

debug radius {all | errors | events | packets | responses | timers}

no debug radius

Syntax	all	-	Generates traces for all the RADIUS server messages
Description	errors	-	Generates traces for error code messages. All the instances where an error is identified are captured by this trace. The error is registered in the log.
	events	-	Generates traces for events related messages. Events like authentication query from authenticator, response from server are registered in the log.
	packets	-	Generates traces for number of packets, kind of packets received and sent from server..
	responses	-	Generates traces for responses sent from the server to authenticator.
	timers	-	Generates traces for the different timers used in the session before the system is reboot.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Defaults Debugging is Disabled

Example iss# debug radius all

Related Command **show radius server** - Displays RADIUS server configuration

6.3 show radius server

This command displays RADIUS server configuration.

```
show radius server [{<ucast_addr> | <ip6_addr> | <string>}]
```

Syntax	ucast_addr	-	Unicast address of the RADIUS server host.
Description	ip6_addr	-	IPv6 address of the RADIUS server host.
	string	-	Name of the RADIUS server host. This value is a string of size 32.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# sh radius server
Primary Server          : 2005::33

Radius Server Host Information
-----
Index                   : 1
Server address          : 13.0.0.100
Shared secret           : Interface MastersRADIUS
Radius Server Status    : Enabled
Response Time           : 10
Maximum Retransmission  : 3
Authentication Port     : 1812
Accounting Port         : 1813
-----
Index                   : 2
Server address          : 2005::33
Shared secret           : Interface MastersRADIUS
Radius Server Status    : Enabled
Response Time           : 10
Maximum Retransmission  : 3
Authentication Port     : 1812
Accounting Port         : 1813
-----
```

Related Command **radius-server host** - Configures the RADIUS client with the parameters

ISS

6.4 show radius statistics

This command displays RADIUS Server Statistics for the data transfer between server and the client from the time of initiation.

show radius statistics

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show radius statistics

```
Radius Server Statistics
-----
Index                               : 1
Radius Server Address               : 10.0.0.1
UDP port number                     : 1812
Round trip time                     : 0
No of request packets              : 8
No of retransmitted packets        : 80
No of access-accept packets        : 0
No of access-reject packets        : 0
No of access-challenge packets     : 0
No of malformed access responses   : 0
No of bad authenticators           : 0
No of pending requests             : 97
No of time outs                    : 89
No of unknown types                : 0
-----
```

Related Command **radius-server host** - Configures the RADIUS client with the parameters

Chapter

7

TACACS

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for providing NAS (Network Access Security). NAS ensures secure access from remotely connected users. TACACS implements the TACACS Client and provides the AAA (Authentication, Authorization and Accounting) functionalities.

TACACS is used for several reasons:

- Facilitates centralized user administration.
- Uses TCP for transport to ensure reliable delivery.
- Supports inbound authentication, outbound authentication and change password request for the Authentication service.
- Provides some level of protection against an active attacker.

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

- tacacs-server host
- tacacs use-server address
- tacacs-server retransmit
- debug tacacs
- show tacacs

7.1 tacacs-server host

This command configures the TACACS server with the parameters (host, timeout, key). The no form of the command deletes server entry from the TACACS server table.

```
tacacs-server host {<ipv4-address> | <ipv6-address> | <host-name>} [single-connection] [port <tcp port (1-65535 )>] [timeout <time out in seconds(1-255)>] {key <secret key>}
```

```
no tacacs-server host { <ipv4-address> | <ipv6-address>}
```

Syntax Description	ipv4-address	-	IPv4 address of the host
	ipv6-address	-	IPv6 address of the host
	host-name	-	Name of the host This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
	single-connection	-	Allows multiple sessions to be established over a single TCP connection for AAA functionalities
	port	-	Configures the TCP port number in which the multiple sessions are established. The value ranges from 1 to 65535.
	timeout	-	Configures the time period (in seconds) till which a client waits for a response from the server before closing the TCP connection. The link between the server and the client gets disconnected, if the specified time is exceeded. The value ranges from 1 to 255 seconds.
	key	-	Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The value is string of maximum length 64.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults port - 40

timeout - 5 seconds

Example `iss(config)# tacacs-server host 12.0.0.100`
`TACACS+ server configured with default secret key !`

`iss(config)# tacacs-server host 2005::33`
`TACACS+ server configured with default secret key !`

**Related
Commands**

- **show tacacs** - Displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client.
- **tacacs use-server address** – Selects the server for the user from the list of configured servers.

7.2 tacacs use-server address

This command configures an active server from the list of servers available in the TACACS server table. The no form of the command disables the configured client active server.

```
tacacs use-server address { <ipv4-address> | <ipv6-address>}
```

```
no tacacs use-server
```

Syntax Description	ipv4-address	-	IPv4 address of the host
	ipv6-address	-	IPv6 address of the host

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# tacacs use-server address 10.0.0.100`



The specified ip address should be any one of the entries from the TACACS server table

- Related Commands**
- `sow tacacs` - Displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client.
 - `tacacs-server host` – Creates the TACACS server entry in a TACACS server table
 - `tacacs-server retransmit` - Configures the retransmit value which is the time interval(in seconds) till which the client waits for a response from active server.

7.3 tacacs-server retransmit

This command configures the retransmit value which is the time interval (in seconds) till which the client waits for a response from active server. The client searches for another server and gets connected with it, if a response is not received within the retransmit time. The no form of the command resets the retransmit value to its default value. The retransmit value ranges from 1 to 100 seconds

```
tacacs-server retransmit <retries>
```

```
no tacacs-server retransmit
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 2 seconds

Example iss(config)# tacacs-server retransmit 3

Related Commands

- **tacacs use-server address** – Selects an active server from the list of servers available in the TACACS server table.

ISS

7.4 debug tacacs

This command sets the debug trace level for TACACS client module. The no form of the command disables the debug trace level for TACACS client module.

```
debug tacacs { all | info | errors | dumptx | dumprx }
```

```
no debug tacacs
```

Syntax	all	-	Generates debug messages for all possible traces (Dumptx, Dumprx, Error, Info).
Description	info	-	Generates debug statements for server information messages such as TACACS session timed out, server unreachability, Session ID exceeded and so on.
	errors	-	Generates debug statements for error debug messages such as failure caused during packet transmission and reception.
	dumptx	-	Generates debug statements for handling traces. This trace is generated when there is an error condition in transmission of packets.
	dumprx	-	Generates debug statements for handling traces. This trace is generated when there is an error condition in reception of packets.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Defaults Debugging is Disabled

Example iss# debug tacacs all

7.5 show tacacs

This command displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client.

show tacacs

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example `iss# sh tacacs`

```

Server : 1
Server address          : 12.0.0.100
Address Type           : IPV4
    Single Connection   : no
    TCP port            : 49
    Timeout             : 5
    Secret Key          : Interface Masters
Server : 2
Server address          : 2005::33
Address Type           : IPV6
    Single Connection   : no
    TCP port            : 4949
    Timeout             : 5
    Secret Key          : Interface Masters
Authen. Starts sent    : 0
Authen. Continues sent : 0
Authen. Enables sent   : 0
Authen. Aborts sent    : 0
Authen. Pass rcvd.     : 0
Authen. Fails rcvd.    : 0
Authen. Get User rcvd. : 0
Authen. Get Pass rcvd. : 0
Authen. Get Data rcvd. : 0
Authen. Errors rcvd.   : 0
Authen. Follows rcvd.  : 0
Authen. Restart rcvd.  : 0
Authen. Sess. timeouts : 0
Author. Requests sent  : 0
Author. Pass Add rcvd. : 0
Author. Pass Repl rcvd : 0
Author. Fails rcvd.    : 0
Author. Errors rcvd.   : 0
Author Follows rcvd.   : 0
Author. Sess. timeouts : 0
Acct. start reqs. sent : 0
Acct. WD reqs. sent    : 0
Acct. Stop reqs. sent  : 0
Acct. Success rcvd.    : 0
  
```

ISS

```
Acct. Errors rcvd.      : 0
Acct. Follows rcvd.    : 0
Acct. Sess. timeouts   : 0
Malformed Pkts. rcvd.  : 0
Socket failures        : 0
Connection failures    : 0
```



It displays the information only for the servers configured in the TACACS server table.

**Related
Commands**

- **tacacs-server host** – Creates a TACACS server entry in a TACACS server
- **tacacs use-server address** – Configures an active server from the list of servers available in the TACACS server table.

Chapter

8

SSH

SSH (Secure Shell) is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

- The Transport Layer Protocol provides server authentication, confidentiality and integrity.
- The User Authentication Protocol authenticates the client-side user to the server. It runs over the transport layer protocol.
- The Connection Protocol multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with these protocols.

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

- ip ssh
- ssh
- debug ssh
- show ip ssh

8.1 ip ssh

This command enables SSH server on the device and configures the various parameters associated with SSH server. The no form of this command disables SSH server on the device and also re-sets the various parameters associated with SSH server. The standard port used by SSH is 22. SSH server allows remote and secure configuration of the switch. The SSH server provides protocol version exchange, data integrity, cipher and key exchange algorithms negotiation between two communicating entities, key exchange mechanism, encryption and server authentication. The auth takes values as bit mask. Setting a bit indicates that the corresponding MAC-list will be used for authentication

```
ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth ([hmac-md5] [hmac-sha1]) }
```

```
no ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth ([hmac-md5] [hmac-sha1]) }
```

Syntax	version compatibility	-	Configures the version of the SSH.
Description	compatibility		When set to true, it supports both SSH version-1 and version-2. When set to false, it supports only the SSH version-2.
	cipher	-	Configures the Cipher-List. This cipherlist takes values as bit mask. Setting a bit indicates that the corresponding cipher-list is used for encryption.
		•	des-cbc – This is a 1 bit cipherlist. It is based on a symmetric-key algorithm that uses a 56-bit key.
		•	3des-cbc – This is a 0 bit cipherlist. Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm.
	auth	-	Configures Public key authentication for incoming SSH sessions.

Mode Global configuration Mode

Package Workgroup, Enterprise and Metro

Defaults

version compatibility	-	false
cipher	-	3des-cbc
auth	-	hmac-sha1

Example

```
iss(config)#ip ssh version compatibility
iss(config)# ip ssh cipher des-cbc
```

Related Command

- **show ip ssh** - Displays SSH server information.
- **ip ssh**- Enables or disables the ssh subsystem.

8.2 ssh

This command either enables or disables the ssh subsystem. When set to enable, the switch is accessible through ssh from a remote locations. Setting ssh to disable, removes the ssh access to the switch.

```
ssh {enable | disable}
```

Syntax	enable	- Enables the ssh subsystem.
Description	disable	- Disables the ssh subsystem.

Mode Global configuration Mode

Package Workgroup, Enterprise and Metro

Package Workgroup, Enterprise and Metro

Defaults enable

Example iss# ssh enable

Related Command **ip ssh** - Enables SSH server on the device and configures the various parameters associated with SSH server

8.3 debug ssh

This command enables the trace levels for SSH. The no form of this command re-sets the SSH trace levels. Trace. System errors such as memory allocation failures are notified using LOG messages and TRACE messages. Interface errors and protocol errors are notified using TRACE messages. Setting all the bits will enable all the trace levels and resetting them will disable all the trace levels

```
debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer]
[server])
```

```
no debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer]
[server])
```

Syntax	all	-	Generates debug statements for all traces.
Description	shut	-	Generates debug statements for shutdown traces. This trace is generated on successful shutting down of SSH related module and memory.
	mgmt	-	Generates debug statements for management plane functionality traces.
	data	-	Generates debug statements for data path
	ctrl	-	Generates debug statements for Control Plane functionality traces
	dump	-	Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.
	resource	-	Generates debug statements for traces with respect to allocation and freeing of all resource except the buffers.
	buffer	-	Generates debug statements for traces with respect to allocation and freeing of buffer.
	server	-	Generates debug statements while creating/ opening/ closing SSH server sockets and any failures to wake up SSH server sockets. Also generates debug statements during enabling /disabling of SSH server.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Defaults Debugging is Disabled

Example iss# debug ssh all

Related Command show ip ssh - Displays SSH server information

8.4 show ip ssh

This command displays the SSH server information such as version, cipher algorithm, authentication and trace level.

show ip ssh

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ip ssh

```
Version           : 2
Cipher Algorithm  : 3DES-CBC
Authentication    : HMAC-SHA1
Trace Level       : None
```

Related Command

- **ip ssh** - Enables SSH server on the device and configures the various parameters associated with SSH server
- **debug ssh** - Enables the trace levels for SSH.

Chapter

9

SSL

SSL (Secure Sockets Layer), is a protocol developed for transmitting private documents through Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:

The SSL Protocol is designed to provide privacy between two communicating applications (a client and a server) and is designed to authenticate the server, and optionally the client. SSL requires a reliable transport protocol (for example, TCP) for data transmission and reception.

The advantage of the SSL Protocol is that it is application protocol independent. A higher level application protocol (for example, HTTP, FTP, TELNET and so on.) can layer on top of the SSL Protocol transparently. The SSL Protocol can negotiate an encryption algorithm and session key as well as authenticate a server before the application protocol transmits or receives its first byte of data. All of the application protocol data is transmitted encrypted, ensuring privacy.

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

- ip http secure
- ssl gen cert-req algo rsa sn
- ssl server-cert
- debug ssl
- show ssl server-cert
- show ip http secure server status

9.1 ip http secure

This command enables SSL server on the device and also configures ciphersuites and crypto keys. The no form of the command disables SSL server on the device and also disables ciphersuites and crypto key configuration.

```
ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha ] [dh-rsa-3des-sha] [rsa-exp1024-des-sha] | crypto key rsa [usage-keys (512|1024)] }
```

```
no ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha] [dh-rsa-3des-sha] [rsa-exp1024-des-sha]}
```

Syntax	server	-	Configures the server status to be enabled. When the server status is enabled it establishes the secure layer in the network
Description	ciphersuite	-	Configures the ciphersuite for providing the input. When an SSL connection is established, the client and server exchange information about which cipher suites they have in common. The options are: <ul style="list-style-type: none"> • RSA-NULL-MD5 – cipher suites using RSA key exchange. and offering no authentication combined with cipher suites using MD5 • RSA-NULL-SHA – cipher suites using RSA key exchange. and offering no authentication combined with cipher suites using SHA1 . • RSA-DES-SHA – cipher suites using RSA key exchange. and cipher suites using DES.combined with cipher suites using SHA1 • RSA-3DES-SHA – cipher suites using RSA key exchange. and cipher suites using triple DES.combined with cipher suites using SHA1 • DH-RSA-DES-SHA – cipher suites using DH , including anonymous DH with cipher suites using RSA key exchange. and cipher suites using DES.combined with cipher suites using SHA1 • DH-RSA-3DES-SHA – cipher suites using DH , including anonymous DH with cipher suites using RSA key exchange. and cipher suites using triple DES.combined with cipher suites using SHA1 • RSA-EXP-1024-DES-SHA – cipher suites using RSA key exchange with export encryption algorithms. Including 40 and 56 bits algorithms and cipher suites using DES.combined with cipher suites using SHA1

crypto key rsa - Configures the usage key (512 or 1024)

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults ciphersuite - rsa-null-md5

Example iss(config)# ip http secure ciphersuite rsa-null-sha

Related Commands

- **show ssl server-cert** - Displays SSL server certificate
- **show ip http secure server status** - Displays SSL status and configuration information

ISS

9.2 ssl gen cert-req algo rsa sn

This command creates a request to generate a certificate to the certificate authority. This command uses the RSA key pair and subject name for generating the request.

```
ssl gen cert-req algo rsa sn <SubjectName>
```

Syntax	SubjectName	-	Configures the name to uniquely identify the client by the certificate authority
Description			

Mode	Privileged EXEC Mode
-------------	----------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Example	iss# ssl gen cert-req algo rsa sn 10.6.4.248
----------------	--

Related Commands	<ul style="list-style-type: none"> • show ssl server-cert - Displays SSL server certificate • show ip http secure server status - Displays SSL status and configuration information
-------------------------	---

9.3 ssl server-cert

This command configures the server-certificate input in PEM format. It imports the public certificate of the ssl server. When the ssl server certificate installation is complete, ssl server sends this certificate for authentication of client

ssl server-cert

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example `iss# ssl server-cert`



The certificate request must have been created.

Related Commands

- `show ssl server-cert` - Displays SSL server certificate
- `show ip http secure server status` - Displays SSL status and configuration information

ISS

9.4 debug ssl

This command configures the debug trace messages levels for SSL. The no form of the command re-sets the given SSL debug level. System errors such as memory allocation failures are notified using LOG messages and TRACE messages. Interface errors and protocol errors are notified using TRACE messages

```
debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])
```

```
no debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])
```

Syntax Description	all	-	Generates debug statements for all traces.
	shut	-	Generates debug statements for shutdown traces. This trace is generated on successful shutting down of SSL related module and memory.
	mgmt	-	Generates debug statements for management plane functionality traces.
	data	-	Generates debug statements for datapath.
	ctrl	-	Generates debug statements for Control Plane functionality traces.
	dump	-	Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.
	resource	-	Generates debug statements for Traces with respect to allocation and freeing of all resource except the buffers.
	buffer	-	Generates debug statements for traces with respect to allocation and freeing of Buffer.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Defaults Disabled

Example iss# debug ssl all

Related Commands

- **show ssl server-cert** - Displays SSL server certificate
- **show ip http secure server status** - Displays SSL status and configuration information

9.5 show ssl server-cert

This command displays SSL server certificate information such as Certificate, Data, version, serial number, Signature algorithm.

show ssl server-cert

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ssl server-cert

```
Certificate:
Data:
  Version: 1 (0x0)
  Serial Number: 1 (0x1)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=in, ST=tn, L=ch, O=fsoft,OU=ps,
  CN=dheepaag/Email=products@Interface Masters.com
  Validity
    Not Before: Jan 12 07:40:35 2005 GMT
    Not After : Feb 11 07:40:35 2005 GMT
  Subject: CN=dee
  Subject Public Key Info:
    Public Key Algorithm:rsaEncryption
    RSA Public Key: (1024bit)
    Modulus (1024 bit):
      00:b1:cf:8f:04:39:c4:80:bc:f0:2b:40:e0:85:16:
      86:8f:cf:66:84:db:0d:fd:58:d5:fc:12:be:4d:d2:
      e2:ba:d6:d8:95:7c:9d:28:46:45:b3:8a:34:dd:41:
      c2:a3:46:ad:8f:c4:ae:17:37:22:91:c4:0a:8d:79:
      ce:10:34:2c:62:a5:6e:4c:a9:63:2e:93:46:a6:d2:
      1c:13:b7:38:02:fb:db:5f:13:46:8e:fb:df:7b:e7:
      c8:ba:00:ad:b2:96:cc:1c:4a:8b:2d:51:27:df:eb:
      9a:8f:6a:b2:8a:98:92:8e:6a:ed:ba:2e:04:38:3a:
      bf:40:f2:d1:37:6c:69:ed:d1
    Exponent:65537(0x10001)
  Signature Algorithm: md5WithRSAEncryption
  8c:d2:50:01:5c:08:d1:0f:ef:eb:70:56:8e:ea:85:72:32:53:
  13:0f:9c:7c:d6:d2:f6:2b:e4:6f:25:4e:86:08:5a:e2:c9:87:
  65:cf:98:6c:99:86:a5:55:66:23:b5:b0:f4:56:e6:35:5e:53:
  31:00:bc:9f:00:62:34:d1:15:c0:a4:7e:d9:27:c3:d2:d7:01:
  13:18:ee:de:f8:52:c8:90:1c:8b:57:15:50:56:8c:b6:7b:4d:
  77:e8:23:41:82:dc:9c:47:66:fb:9a:ba:7f:73:a1:d0:88:93:
  7b:c3:4b:c8:a5:ec:db:4a:36:19:02:c9:f7:e6:d1:c7:38:d3:
  13:f3
```



SSL server certificate must have been created.

Related Commands

- `ip http secure` - Enables SSL server on the device and also configures

ciphersuites and crypto keys

- **ssl gen cert-req algo rsa sn** - Creates a certificate request using RSA key pair and subjectName
- **ssl server-cert** - Configures the server cert, input in PEM format
- **show ip http secure server status** - Displays SSL status and configuration information

9.6 show ip http secure server status

This command displays SSL status and configuration information. Information such as HTTP secure server status, http secure server ciphersuite are displayed.

show ip http secure server status

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ip http secure server status

```
HTTP secure server status      : Enabled
HTTP secure server ciphersuite : RSA-DES-SHA:RSA-3DES-SHA:RSA-
EXP1024-DES-SHA:
```



This command will display output only if http secure server ciphersuite and crypto keys are configured.

**Related
Commands**

- **ip http secure** - Enables SSL server on the device and also configures ciphersuites and crypto keys
- **ssl gen cert-req algorsa sn** - Creates a certificate request using RSA key pair and subjectName
- **ssl server-cert** - Configures the server cert, input in PEM format
- **show ssl server-cert** - Displays SSL server certificate

Chapter

10

SNTP

The SNTP (Simple Network Time Protocol) is a simplified version or subnet of the NTP protocol. It is used to synchronize the time and date in ISS by contacting the SNTP Server. The administrator can choose whether to set the system clock manually or to enable SNTP. If SNTP is enabled, the SNTP implementation discovers the SNTP server and gets the time from the server. The SNTP implementation also has callouts to set the system time based on the time received from the SNTP server. It supports different time zones, where the user can set the required time zone.

The following are the list of SNTP commands:

- sntp
- set sntp client
- set sntp client version
- set sntp client addressing mode
- set sntp client port
- set sntp client clock-format
- set sntp client time zone
- set sntp client clock-summer-time
- set sntp client authentication-key
- set sntp unicast-server auto-discovery
- set sntp unicast-poll-interval
- set sntp unicast-max-poll-timeout
- set sntp unicast-max-poll-retry
- set sntp unicast-server

ISS

- set snmp broadcast-mode send-request
- set snmp broadcast-poll-timeout
- set snmp broadcast-delay-time
- set snmp multicast-mode send-request
- set snmp multicast-poll-timeout
- set snmp multicast-delay-time
- set snmp multicast-group-address
- set snmp anycast-poll-interval
- set snmp anycast-poll-timeout
- set snmp anycast-poll-retry-count
- set snmp anycast-server
- set snmp client clock-format
- show snmp status
- show snmp unicast-mode status
- show snmp broadcast-mode status
- show snmp multicast-mode status
- show snmp anycast-mode status
- debug snmp

10.1 sntp

This command enters to SNTP configuration mode which allows the user to execute all the commands that supports SNTP configuration mode.

sntp

Mode Global configuration mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# sntp`

Related Commands

- **set sntp client** - Sends the request to the host for time synchronization.
- **set sntp client version** - Sets the operating version of the client SNTP.
- **set sntp client addressing mode** - Sets the addressing mode of SNTP client.
- **set sntp client port**- Sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection.
- **set sntp client clock format** - Sets the system clock as either AM PM / HOURS format.
- **set sntp client time zone** - Sets the system time zone with respect to UTC.
- **sntp client clock-summer-time**- Enables the DST. (Daylight Saving Time).
- **set sntp client authentication key** - Sets the authentication key for the SNTP clients.
- **set sntp unicast-server auto-discovery** - Configures SNTP client status of auto-discovery
- **set sntp unicast-poll-interval**- Configures SNTP client poll interval.
- **set sntp unicast-max-poll-timeout**- Configures SNTP client maximum poll interval
- **set sntp unicast-max-poll-retry** - Configures SNTP client maximum retry poll count.
- **set sntp unicast-server**- Configures SNTP unicast server.
- **set sntp broadcast-mode send request** - Sets the status of sending the request for knowing the delay.
- **set sntp broadcast-poll-timeout**- Configures SNTP client poll interval in broadcast mode.
- **set sntp broadcast-delay-time**- Configures SNTP delay time in broadcast mode.

- **set sntp multicast-mode send-request** - Sets the status of sending the request for knowing the delay.
- **set sntp multicast-poll-timeout** - Configures SNTP client poll interval in multicast mode.
- **set sntp multicast-delay-time** - **set sntp multicast-delay-time** - Configures SNTP delay time in multicast mode.
- **set sntp multicast-group-address**- Configures SNTP multicast server address.
- **set sntp anycast-poll-interval**- Configures SNTP client poll interval in anycast mode.
- **set sntp anycast-poll-timeout** - Configures SNTP client poll timeout in anycast mode.
- **set sntp anycast-poll-retry-count** - Configures SNTP poll retries in anycast mode.
- **set sntp anycast-server**- Configures SNTP multicast or broadcast server address in anycast mode.

10.2 set sntp client

This command either enables or disables SNTP client module.

```
set sntp client {enabled | disabled}
```

Syntax Description **enabled** - Sends a request to the host for time synchronization.

disabled - Does not send any request to the host for time synchronization.

Mode SNTP configuration mode

Package Workgroup, Enterprise and Metro

Defaults Disabled.

Example `iss(config-sntp)# set sntp client enabled`

- Related Commands**
- `sntp` - Enters to SNTP configuration mode
 - `show sntp status` - Displays the status of SNTP client.

ISS

10.3 set sntp client version

This command sets the operating version of the SNTP for the client.

```
set sntp client version { v1 | v2 | v3 | v4 }
```

Syntax Description	v1	-	Sets the version of SNTP client as 1
	v2	-	Sets the version of SNTP client as 2
	v3	-	Sets the version of SNTP client as 3
	v4	-	Sets the version of SNTP client as 4

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults v4

Example `iss(config-sntp)# set sntp client version v3`

Related Command

- `sntp` - Enters to SNTP configuration mode.
- `show sntp status` - Displays the status of SNTP client.

10.4 set sntp client addressing mode

This command sets the addressing mode of SNTP client.

```
set sntp client addressing-mode { unicast | broadcast | multicast | anycast2
}
```

Syntax Description	unicast	-	Sets the addressing mode of SNTP client as unicast which operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.
	broadcast	-	Sets the addressing mode of SNTP client as broadcast which operates in a point-to-multipoint fashion. The SNTP server uses an IP local broadcast address instead of a multicast address. The broadcast address is scoped to a single subnet, while a multicast address has Internet wide scope.
	multicast		Sets the addressing mode of SNTP client as multicast which operates in point-to-multipoint fashion. The SNTP server uses a multicast group address to send unsolicited SNTP messages to clients. The client listens on this address and sends no requests for updates.
	anycast	-	Sets the addressing mode of SNTP client as anycast which operates in a multipoint-to-point fashion. The SNTP client sends a request to a designated IPv4 or IPv6 local broadcast address or multicast group address. One or more anycast servers reply with their individual unicast addresses
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		

² This functionality is not supported in this release.

ISS

Defaults unicast

Example `iss(config-sntp)# set sntp client addressing-mode unicast`



This command is executed only if SNTP client is enabled

Related Command

- `sntp` - Enters to SNTP configuration mode.
- `show sntp status` - Displays SNTP status.
- `show sntp unicast-mode status` - Displays the SNTP unicast mode status.
- `show sntp broadcast-mode status` - Displays the SNTP broadcast mode status.
- `show sntp multicast-mode status` - Displays the SNTP multicast mode status.
- `show sntp anycast-mode status` - Displays the SNTP anycast mode status.

10.5 set sntp client port

This command sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection. The value ranges between 1025 and 65535. The no form of this command deletes the listening port for SNTP client and sets the default value.

```
set sntp client port <portno(1025-65535)>
```

```
no sntp client port
```

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 123

Example `iss (config-sntp)# set sntp client port 1026`



This command is executed only if SNTP client is enabled

- Related commands**
- `sntp` - Enters to SNTP configuration mode.
 - `show sntp status` - Displays SNTP status.

ISS

10.6 set sntp client clock-format

This command sets the system clock as either AM PM format or HOURS format.

SNTP clock format configuration in the switch:

- Date – Hours, Minutes, Seconds, Date, Month and Year
- Month – Jan, Feb, Mar.....
- Year - yyyy

```
set sntp client clock-format {ampm | hours}
```

Syntax	am-pm	-	Sets the system clock in am/ pm format
Description	hours	-	Sets the system clock in 24 hours format
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	hours		
Example	iss (config-sntp)# set sntp client clock-format ampm		
Related Command	<ul style="list-style-type: none"> • sntp - Enters to SNTP configuration mode. • show sntp status - Displays SNTP status. • show sntp clock - Displays the current time. 		

10.7 set sntp client time zone

This command sets the system time zone with respect to UTC. The no form of command resets the system time zone to GMT.

```
set sntp client time-zone <+/- UTC TimeDiff in Hrs:UTC TimeDiff in Min> Eg:
+05:30
```

```
no sntp client time-zone
```

Syntax +/- - Sets the client time zone as after or before UTC. Plus indicates forward time zone and minus indicates backward time zone.

Description

UTCTimeDiff **in** - Sets the UTC time difference in hours

Hrs

UTC TimeDiff **in** - Sets the UTC time difference in minutes

Min

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Default + 0: 0

Example iss(config-sntp)# set sntp client time-zone +05:30



SNTP server must be enabled prior to the execution of this command.

Related Command

- **sntp** – Enters to SNTP configuration mode
- **show sntp status** – Displays SNTP status.

ISS

10.8 set sntp client clock-summer-time

This command enables the DST (Daylight Saving Time). DST is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. Many countries observe DST, although most have their own rules and regulations for when it begins and ends. The dates of DST may change from year to year. The no form of this command disables the Daylight Saving Time.

```
set sntp client clock-summer-time <week-day-month, hh:mm> <week-day-month, hh:mm>
Eg: set sntp client clock-summer-time First-Sun-Mar, 05:10
Second-Sun-Nov, 06:10
```

```
no sntp client clock summer-time
```

Syntax Description

week-day-month - Week – First, Second, Third, Fourth or Last week of month.
 Day – Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday.
 Month: January, February, March, April, May, June, July, August, September, October, November or December.

hh:mm - Time in hours and minutes

Mode SNTP Configuration Mode

Default Not set

Package Workgroup, Enterprise and Metro

Example

```
iss(config-sntp)# set sntp client clock-summer-time First-Sun-Jan, 12:12
Second-Sun-Mar, 12:12
```

- Related Commands**
- **sntp** – Enters to SNTP configuration mode
 - **show sntp status** - Displays SNTP status.

10.9 set sntp client authentication-key

This command sets the authentication parameters for the key. Some SNTP servers requires authentication to be done before exchanging any data. This authentication key is used to authenticate the client to the SNTP server to which it tries to connect. The no form of this command disables authentication.

```
set sntp client authentication-key <key-id> md5 <key>
```

```
no sntp client authentication
```

Syntax	<key-id>	-	Sets a key identifier (integer value) to provide authentication for the server. The value ranges between 1 and 65535.
Description	md5	-	Verifies data integrity. MD5 is intended for use with digital signature applications, which requires that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem.
	<key>	-	Sets the authentication code as a key value.
Mode	SNTP Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	Authentication key ID not set		
Example	<pre>iss(config-sntp)# set sntp client authentication-key 123 md5 Interface Masters</pre>		
Related Command	<ul style="list-style-type: none"> • sntp – Enters to SNTP configuration mode • show sntp status – Displays SNTP status. 		

ISS

10.10 set sntp unicast-server auto-discovery

This command discovers the entire available SNTP client.

```
set sntp unicast-server auto-discovery {enabled | disabled}
```

Syntax Description

enabled	- Automatically discovers the entire available SNTP client even if the necessary configuration is not done.
----------------	---

disabled	- Does not discover any SNTP client.
-----------------	--------------------------------------

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Disabled

Example

```
iss(config-sntp)# set sntp unicast-server auto-discovery
enabled
```



This command is executed only if the SNTP client addressing mode is set as unicast

Related Command

- **sntp** - Enters to SNTP configuration mode.
- **Show sntp unicast-mode status** - Displays the SNTP Unicast Mode status.

10.11 set sntp unicast-poll-interval

This command sets the SNTP client poll interval which is the maximum interval between successive messages in seconds. The value ranges between 16 and 16284 seconds.

```
set sntp unicast-poll-interval <value (16-16284) seconds>
```

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Default 64

Example `iss(config-sntp)# set sntp unicast-poll-interval 50`



This command is executed only if the SNTP client addressing mode is set as unicast

Related Command

- `sntp` - Enters to SNTP configuration mode
- `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

ISS

10.12 set sntp unicast-max-poll-timeout

This command configures SNTP client maximum poll interval timeout which is the maximum interval to wait for the poll to complete. The value ranges between 1 and 30 in seconds.

set sntp unicast-max-poll-timeout <value (1-30) seconds>

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Default 5

Example `iss(config-sntp)# set sntp unicast-max-poll-timeout 25`



This command is executed only if the SNTP client addressing mode is set as unicast

Related Command

- `sntp` - Enters to SNTP configuration mode.
- `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

10.13 set sntp unicast-max-poll-retry

This command configures SNTP client maximum retry poll count which is the maximum number of unanswered polls that cause a slave to identify the server as dead. The value ranges between 1 and 10 in times.

```
set sntp unicast-max-poll-retry <value (1-10) times>
```

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Default 3

Example `iss(config-sntp)# set sntp unicast-max-poll-retry 10`



This command is executed only if the SNTP client addressing mode is set as unicast

Related Command

- `sntp` - Enters to SNTP configuration mode
- `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

10.14 set sntp unicast-server

This command configures SNTP unicast server. The no form of this command deletes the sntp unicast server attributes and sets to default value.

```
set sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr>} [{primary | Secondary}] [version {3 | 4}] [port <integer(1025-36564)>]
```

```
no sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr>}
```

Syntax Description	ipv4 <ucast_addr>	-	Sets the address type of the unicast server as Internet Protocol Version 4.
	ipv6 <ip6_addr>	-	Sets the address type of the unicast server as Internet Protocol Version 6.
	Primary	-	Sets the unicast server type as primary server.
	secondary	-	Sets the unicast server type as secondary server.
	version 3	-	Sets the SNTP version as 3.
	version 4	-	Sets the SNTP version as 4.
	port <integer(1025-36564)>	-	Selects the port identifier numbers in the selected server. The port number ranges between 1025 and 36564.

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config-sntp)# set sntp unicast-server ipv4 12.0.0.100 Primary 3 1234`



This command is executed only if the SNTP client addressing mode is set as unicast

- Related Command**
- `sntp` - Enters to SNTP configuration mode
 - `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

10.15 set sntp broadcast-mode send-request

This command either enables or disables the sntp to send status request.

```
set sntp broadcast-mode send-request {enabled | disabled}
```

Syntax Description **enabled** - Sends the SNTP request packet to broadcast server to calculate the actual delay.

disabled - Does not send any SNTP request packet to broadcast server instead default value for the delay is taken.

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults disabled

Example `iss(config-sntp)# set sntp broadcast-mode send-request enabled`



This command is executed only if the SNTP client addressing mode is set as broadcast.

Related Command

- **sntp** – Enters to SNTP configuration mode
- **show sntp broadcast-mode status** – Displays the SNTP broadcast mode status.

ISS

10.16 set sntp broadcast-poll-timeout

This command configures SNTP client poll interval in broadcast mode which is the maximum interval to wait for a poll to complete. The value ranges between 1 and 30 seconds.

```
set sntp broadcast-poll-timeout [<value (1-30) seconds>]
```

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Default 5

Example `iss(config-sntp)# set sntp broadcast-poll-timeout 30`



This command is executed only if the SNTP client addressing mode is set as broadcast.

Related Command

- `sntp` – Enters to SNTP configuration mode
- `show sntp broadcast-mode status` – Displays the SNTP broadcast mode status

10.17 set sntp broadcast-delay-time

This command configures SNTP delay time in broadcast mode which is the time interval the SNTP client needs to wait for a response from the server. The value ranges between 1000 and 15000 in microseconds.

```
set sntp broadcast-delay-time [<value (1000-15000) microseconds>]
```

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Default 8000

Example `iss(config-sntp)# set sntp broadcast-delay-time 2000`



This command is executed only if the SNTP client addressing mode is set as broadcast.

Related Command

- `sntp` – Enters to SNTP configuration mode
- `show sntp broadcast-mode status` – Displays the SNTP broadcast mode status

10.18 set sntp multicast-mode send-request

This command sets the status of sending the request to the multicast server to calculate the delay time.

```
set sntp multicast-mode send-request {enabled | disabled}
```

Syntax Description **enabled** - Sends the SNTP request to the multicast server to calculate the actual delay time.

disabled - Does not send any SNTP request to the multicast server.

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Disabled

Example `iss(config-sntp)# set sntp multicast-mode send-request enabled`



This command is executed only if the SNTP client addressing mode is set as multicast.

- Related Command**
- `sntp` – Enters to SNTP configuration mode
 - `show sntp multicast-mode status` – Displays the SNTP multicast mode status

10.19 set sntp multicast-poll-timeout

This command configures SNTP client poll interval in multicast mode which is the maximum interval to wait for the poll to complete. The value ranges between 1 and 30 seconds.

```
set sntp multicast-poll-timeout [<value (1-30) seconds>]
```

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Default 5

Example `iss(config-sntp# set sntp multicast-poll-timeout 10`



If command is executed only if the SNTP client addressing mode is set as broadcast.

Related Command

- `sntp` – Enters to SNTP configuration mode.
- `show sntp multicast-mode status` – Displays the SNTP multicast mode status.

ISS

10.20 set sntp multicast-delay-time

This command configures SNTP delay time in which there is no response from the multicast server. The value ranges between 1000 and 15000 in microseconds.

```
set sntp multicast-delay-time [<value (1000-15000) microseconds>]
```

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Default 8000

Example `iss(config-sntp)# set sntp multicast-delay-time 2000`



This command is executed only if the SNTP client addressing mode is set as broadcast.

Related Command

- `sntp` – Enters to SNTP configuration mode
- `show sntp multicast-mode status` – Displays the SNTP multicast mode status

10.21 set sntp multicast-group-address

This command configures a group address for the SNTP so that all the SNTP client servers can be connected to this address.

```
set sntp multicast-group-address {ipv4 {<mcast_addr> | default} | ipv6
{<ipv6_addr> | default}}
```

Syntax	ipv4	- Sets the Internet Protocol Version as version 4
Description		<ul style="list-style-type: none"> • <mcast_addr> - Sets the multicast group address • Default – Sets the multicast default address as a default value
	ipv6	- Sets the Internet Protocol Version as version 6
		<ul style="list-style-type: none"> • < ipv6_addr > - Sets the ipv6 address • Default – Sets the multicast default address as a default value

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss(config-sntp)# set sntp multicast-group-address ipv4
224.1.1.10.



This command is executed only if the SNTP client addressing mode is set as multicast.

Related Command

- **sntp** – Enters to SNTP configuration mode.
- **show sntp multicast-mode status** – Displays the SNTP multicast mode status.

ISS

10.22 set sntp anycast-poll-interval

This command configures SNTP client poll interval which is the maximum interval between successive messages. The poll interval value ranges between 16 and 16284 in seconds.

```
set sntp anycast-poll-interval [<value (16-16284) seconds>]
```

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Default 64

Example `iss(config-sntp)# set sntp anycast-poll-interval 20`



If command is executed only if the SNTP client addressing mode is set as anycast.

Related Command

- `sntp` – Enters to SNTP configuration mode.
- `show sntp anycast-mode status` – Displays the SNTP anycast mode status.

10.23 set sntp anycast-poll-timeout

This command configures SNTP client poll timeout which is the maximum interval to wait for a poll to complete. The value ranges between 1 and 30 in seconds.

```
set sntp anycast-poll-timeout [<value (1-30) seconds>]
```

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Default 5

Example `iss(config-sntp)# set sntp anycast-poll-timeout 10`



This command is executed only if the SNTP client addressing mode is set as anycast.

Related Command

- `sntp` – Enters to SNTP configuration mode.
- `show sntp anycast-mode status` – Displays the SNTP anycast mode status.

ISS

10.24 set sntp anycast-poll-retry-count

This command configures SNTP poll retries count which is the maximum number of unanswered polls that cause a slave to identify the server as dead. The value ranges between 1 and 10 in seconds.

```
set sntp anycast-poll-retry-count [<value (1-10)>]
```

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Default 3

Example `iss(config-sntp)# set sntp anycast-poll-retry-count 5`



If command is executed only if the SNTP client addressing mode is set as anycast.

Related Command

- `sntp` – Enters to SNTP configuration mode.
- `show sntp anycast-mode status` – Displays the SNTP anycast mode status

10.25 set sntp anycast-server

This command configures SNTP multicast or broadcast server address in anycast mode.

```
set sntp anycast-server { broadcast | multicast {ipv4 [<ipv4_addr>] |ipv6
[<ipv6_addr>]} }
```

Syntax Description	broadcast	- Configures SNTP broadcast server address in anycast mode
	multicast	- Configures SNTP multicast server address in anycast mode. <ul style="list-style-type: none"> • ipv4 <ipv4_addr> - Sets the multicast server address in internet protocol v4 • ipv6 <ipv6_addr> - Sets the multicast server address in internet protocol v6

Mode SNTP Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config-sntp)# set sntp anycast-server ipv4 12.0.0.100`



This command is executed only if the SNTP client addressing mode is set as anycast.

- Related Command**
- **sntp** – Enters to SNTP configuration mode
 - **show sntp anycast-mode status** – Displays the SNTP anycast mode status

ISS

10.26 show sntp clock

This command displays the current time.

show sntp clock

Mode User EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show sntp clock

```
current time : Sat Jan 01 2000 00:07:04 (UTC + 0: 0 )
```

Related Command

- **set sntp client clock-format** - Sets the system clock as either AM PM format or HOURS format.

10.27 show sntp status

This command displays SNTP status.

show sntp status

Mode User EXEC Mode
Package Workgroup, Enterprise and Metro
Example iss# show sntp status

```
sntp client is enabled
current sntp client version is v4
current sntp client addressing mode is unicast
sntp client port is 123
sntp client clock format is 24 hours
sntp client authenticatin key id is 5
sntp client authentication algorithm is md5
sntp client auth Key is Interface Masters
sntp client time zone is + 05:30
sntp client dst start time is not set
sntp client dst end time is not set
```

Related Command

- **set sntp client** - Sends the request to the host for time synchronization.
- **set sntp client version** - Sets the operating version of the client SNTP.
- **set sntp client addressing mode** - Sets the addressing mode of SNTP client.
- **set sntp client port** - Sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection.
- **set sntp client clock-format** - Sets the system clock as either AM PM / HOURS format.
- **set sntp client authentication-key** - Sets the authentication key for the SNTP clients.
- **set sntp client time-zone** - Sets the system time zone with respect to UTC.
- **sntp client clock-summer-time** - Enables the Daylight Saving Time.
- **show sntp unicast-mode status** - Displays the SNTP Unicast Mode status.
- **show sntp broadcast-mode status** - Displays the SNTP broadcast mode status
- **show sntp multicast-mode status** - Displays the SNTP multicast mode status
- **show sntp anycast-mode status** - Displays the SNTP anycast mode status

ISS

10.28 show sntp unicast-mode status

This command displays the status of SNTP in unicast mode.

show sntp unicast-mode status

Mode User EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show sntp unicast-mode status

```
auto discovery of sntp/ntp servers is disabled
unicast poll interval value is 50
unicast max poll time out value is 25
unicast max retry time value is 10
unicast primary server address is 12.0.0.100
unicast primary server version is 3
unicast primary server port is 1234
```



This command is executed only if the addressing mode is set as unicast.

Related Command

- **set sntp client addressing mode** - Sets the addressing mode of SNTP client.
- **set sntp unicast-server auto-discovery** - Configures SNTP client status of auto-discovery of server.
- **set sntp unicast-poll-interval** - Configures SNTP client poll interval.
- **Set sntp unicast-max-poll-timeout** - Configures SNTP client maximum poll interval timeout.
- **set sntp unicast-max-poll-retry** - Configures SNTP client maximum retry poll count.
- **set sntp unicast-server** - Configures SNTP unicast server.
- **show sntp status** - Displays the status of SNTP client.

10.29 show sntp broadcast-mode status

This command displays the status of SNTP in broadcast mode.

show sntp broadcast-mode status

Mode User EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show sntp broadcast-mode status

```
send sntp request to server in broadcast mode is disabled
broadcast poll time out value is 5
broadcast delay time value is 8000
broadcast sntp server is 12.0.0.100
```



This command is executed only if the addressing mode is set as broadcast.

Related Command

- **set sntp client addressing mode** - Sets the addressing mode of SNTP client.
- **set sntp broadcast-mode send-request** - Sets the status of sending the request for knowing the delay.
- **set sntp broadcast-poll-timeout** - Configures SNTP client poll interval in broadcast mode.
- **set sntp broadcast-delay-time** - Configures SNTP delay time in broadcast mode.
- **Show sntp status**- Displays the status of SNTP client.

10.30 show sntp multicast-mode status

This command displays the status of SNTP in multicast mode.

show sntp multicast-mode status

Mode User EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show sntp multicast-mode status

```
send sntp request to server in multicast mode is disabled
multicast poll time out value is 5
multicast delay time value is 8000
multicast group address is 12.0.0.100
```



If command is executed only if the SNTP client addressing mode is set as multicast.

Related Command

- **set sntp client addressing mode** - Sets the addressing mode of SNTP client.
- **set sntp multicast-mode send-request** - Sets the status of sending the request for knowing the delay.
- **set sntp multicast-poll-timeout** - Configures SNTP client poll interval in multicast mode.
- **set sntp multicast-delay-time** - Configures SNTP delay time in multicast mode.
- **set sntp multicast-group-address** - Configures SNTP multicast server address.
- **show sntp status**- Displays the status of SNTP client.

10.31 show sntp anycast-mode status

This command displays the SNTP anycast mode status.

show sntp anycast-mode status

Mode User EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show sntp anycast-mode status

```
anycast poll interval value is 64
anycast max poll time out value is 5
anycast max retry time value is 3
anycast server type is broadcast
primary server address is 12.0.0.100
```



If command is executed only if the SNTP client addressing mode is set as anycast.

Related Command

- **set sntp client addressing mode** - Sets the addressing mode of SNTP client.
- **set sntp anycast-poll-interval** - Configures SNTP client poll interval in anycast mode.
- **set sntp anycast-poll-timeout** - Configures SNTP client poll timeout in anycast mode.
- **set sntp anycast-poll-retry-count** - Configures SNTP poll retries in anycast mode.
- **set sntp anycast-server**- Configures SNTP multicast or broadcast server address in anycast mode.
- **show sntp status**- Displays the status of SNTP client.

10.32 debug sntp

This command enables SNTP trace. The no form of the command disables the SNTP trace.

```
debug sntp {all | [init-shut] [mgmt] [data-path] [control] [pkt-dump]
[resource] [all-fail] [buff]}
```

```
no debug sntp {all | [init-shut] [mgmt] [data-path] [control] [pkt-dump]
[resource] [all-fail] [buff]}
```

Syntax Description	all	-	Generates debug statements for all kinds of traces
	init-shut	-	Generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of SNTP related entries
	mgmt	-	Generates debug statements for management traces. This trace is generated during failure in configuration of any of the SNTP features.
	data-path	-	Generates debug statements for data path traces. This trace is generated during failure in packet processing.
	control	-	Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of SNTP entries.
	pkt-dump	-	Generates debug statements for packet dump traces. This trace is currently not used in SNTP module.
	resource	-	Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.
	all-fail	-	Generates debug statements for all failure traces of the above mentioned traces.
	buff	-	Generates debug statements for SNTP buffer related traces. This trace is currently not used in SNTP module.

Mode User EXEC Mode

Package Workgroup, Enterprise and Metro

Defaults Debugging is Disabled

Example debug sntp all

Chapter

11

SNMPv3

SNMP (Simple Network Management Protocol) is the most widely-used network management protocol on TCP/IP-based networks. SNMPv3 is designed mainly to overcome the security shortcomings of SNMPv1/v2. USM (User based Security Model) and VACM (View based Access Control Model) are the main features added as part of the SNMPv3 specification. USM provides both encryption and authentication of the SNMP PDUs, while VACM specifies a mechanism for defining access policies for different users with different MIB trees. Also, SNMPv3 specifies a generic management framework, which is expandable for adding new Management Engines, Security Models, Access Control Models and so on. With SNMPv3, the SNMP communication is completely safe and secure.

SNMPv3 is a multi-lingual Agent supporting all three versions of SNMP (SNMPv1, SNMPv2c and SNMPv3) while conforming to the latest specifications. It is available as a portable source code product, which can be easily integrated to any platform (any OS and any Processor). MIB integration is made simple with the aid of a tool called Middle Level Code Generator (MIDGEN), which is available along with **Interface Masters SNMP**. MIDGEN generates the interface stubs required for every object in the MIB for the SET, GET and GETNEXT operations.

These stubs can be implemented by the respective modules supporting the MIB. **Interface Masters SNMP** is provided as source code available for licensing to OEMs and VARs who wish to incorporate the multi-lingual SNMP functionality into their products.

The list of CLI commands for the configuration of SNMPv3 is as follows:

- enable snmpsubagent
- disable snmpsubagent
- show snmp agentx information
- show snmp agentx statistics
- enable snmpagent
- disable snmpagent

ISS

- snmp community index
- snmp group
- snmp access
- snmp engineid
- snmp proxy name
- snmp mibproxy name
- snmp view
- snmp targetaddr
- snmp targetparams
- snmp user
- snmp notify
- snmp filterprofile
- snmp-server enable traps snmp authentication
- snmp-server trap udp-port
- snmp-server trap proxy-udp-port
- snmp agent port
- snmp tcp enable
- snmp trap tcp enable
- snmp-server tcp-port
- snmp-server trap tcp-port
- snmp-server enable traps
- show snmp
- show snmp community
- show snmp group
- show snmp group access
- show snmp engineID
- show snmp proxy
- show snmp mibproxy
- show snmp viewtree
- show snmp targetaddr
- show snmp targetparam
- show snmp user
- show snmp notif
- show snmp inform statistics
- show snmp-server traps

- show snmp-server proxy-udp-port
- show snmp tcp
- show snmp filter

11.1 enable snmpsubagent

This command configures the SNMP to act either as SNMP agent or Agentx-subagent.

```
enable snmpsubagent { master { ip4 <ipv4_address> | ip6 <ipv6_address> } [port <number>] }
```

Syntax Description	master	-	Registers all the MIB regions and agent capabilities after successful index allocation.
	ip4<ipv4_address>	-	Sets the IP Address type as version 4
	port<number>	-	Sets the master port number through which the Agentx PDUs are transmitted to the master agent.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults port - 705

Example iss(config)# enable snmpsubagent master ip4 10.0.0.5 port 897



This example is executable only if snmp agent is disabled.

Related Commands

- **disable snmpsubagent** - Disables agentx-subagent
- **disable snmpagent** - Disables SNMP agent.
- **enable snmpagent** - Enables SNMP agent.
- **show snmp agentx information** - Displays global information of SNMP Agentx communications.
- **show snmp agentx statistics** - Displays all the information regarding SNMP Agentx statistics.

11.2 disable snmpsubagent

This command disables agentx-subagent.

disable snmpsubagent

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# disable snmpsubagent`

Related Commands

- **enable snmpsubagent** - Enables either snmp agent or agentx-subagent capabilities.
- **show snmp agentx information** - Displays global information of SNMP Agentx communications.
- **show snmp agentx statistics**- Displays all the information regarding SNMP Agentx statistics.

ISS

11.3 enable snmpagent

This command enables SNMP agent which provides an interface between a SNMP manager and a switch. The agent processes SNMP packets received from the manager, frames the appropriate response packets and sends them to the manager.

enable snmpagent

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults SNMP agent is enabled.

Example `iss(config)# enable snmpagent`

Related Commands

- **enable snmpsubagent** - Enables either snmp agent or agentx-subagent capabilities.
- **Disable snmpagent** - Disables SNMP agent.

11.4 disable snmpagent

This command disables SNMP agent.

disable snmpagent

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# disable snmpagent`

Related Commands

- **enable snmosubagent** - Enables either snmp agent or agentx-subagent capabilities.
- **enable snmpagent** - Enables SNMP agent.
- **show snmp agentx statistics** - Displays all the information regarding SNMP Agentx statistics.

11.5 snmp community index

This command configures the SNMP community details. The no form of this command removes the SNMP community details.

```
snmp community index <CommunityIndex> name <CommunityName> security
<SecurityName> [context <Name >] [{volatile | nonvolatile}] [transporttag
<TransportTagIdentifier | none>] [contextengineid <ContextEngineID>]
```

```
no snmp community index <CommunityIndex>
```

Syntax	<CommunityIndex>	-	Creates a community index identifier which stores the index value of the row. This ID must be unique for every community name entry.
Description	name<CommunityName>	-	Creates a community name which stores the community string.
	security<SecurityName>	-	Stores the security model of the corresponding Snmp community name.
	Context <Name>	-	Indicates the name of the context in which the management information is accessed when using the community string specified by the corresponding instance of snmp community name
	volatile nonvolatile	-	Sets the storage type as either volatile or non volatile. Volatile – Sets the storage type as temporary and erases the configuration setting on restarting the system. • Non Volatile – Sets the storage type as permanent and saves the configuration to the system. The saved configuration can be viewed on restarting the system.
	<TransportTagIdentifier>	-	Specifies a set of transport endpoints from which a command responder application can accept management request.
	contextengineid<ContextEngineID>		Indicates the location of the context through which the management information is accessed when using the community string specified by the corresponding instance of snmp community name
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Community Index	-	NETMAN/PUBLIC

CommunityName	-	NETMAN/PUBLIC
Security Name	-	None
ContextName	-	Null
Context EngineID	-	80.00.08.1c.04.46.53
Transport Tag	-	Null
Storage type	-	Non Volatile
Row Status	-	Active

Example

```
iss(config)# snmp community index myv3com name myv3com security  
xyz context myinst nonvolatile transporttag myv3tag
```

**Related
Commands**

- **show snmp** - Displays the status information of SNMP communications
- **show snmp community** - Displays the configured SNMP community details

11.6 snmp group

This command configures SNMP group details. The no form of the command removes the SNMP group details.

```
snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 }
[ {volatile | nonvolatile} ]
```

```
no snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 }
```

Syntax	<GroupName>	-	Creates a name for an SNMP group
Description	user<UserName>	-	Sets an user for the configured group.
	security-model	-	Sets the security model for SNMP <ul style="list-style-type: none"> • V1 - Sets the SNMP version as Version 1. • V2c - Sets the SNMP version as Version 2. • V3 - Sets the SNMP version as Version 3.
	volatile nonvolatile		- Sets the required storage type for the group entry <ul style="list-style-type: none"> • Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system. • Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Security model		V3
	Security Name	-	none / initial / templateMD5 / templateSHA
	Group Name	-	iso/initial
	Storage Type	-	Non volatile
	Row status	-	Active

Example `iss(config)# snmp group myv3group user myv3user security-model v1
volatile`

**Related
Commands**

- `snmp access` - Configures the SNMP group access details
- `show snmp group` - Displays the configured SNMP groups
- `show snmp user` - Displays the configured SNMP users
- `show snmp group` - Displays the configured SNMP groups.

11.7 snmp access

This command configures the SNMP group access details. To configure an SNMP access along with the group, a group must have already been created using the snmp group command. The no form of the command removes the SNMP group access details.

```
snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}} [read <ReadView | none>] [write <WriteView | none>] [notify <NotifyView | none>] [{volatile | nonvolatile}] [context <string(32)> ]
```

```
no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}
```

Syntax Description	<GroupName>	-	Sets the name of the group for which access is to be provided.
	v1 v2c v3	-	<ul style="list-style-type: none"> • v1 – Sets the SNMP version as Version 1. • v2c – Sets the SNMP version as Version 2. • v3 – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
	auth	-	Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.
	noauth	-	Sets no-authentication
	priv	-	Sets both authentication and privacy
	read	-	Enables the user only to read the data.
	write	-	Enables the user to both read and write the data.
	notify	-	Enables the user to send the changes done to a destination through a tag.
	volatile nonvolatile	-	Sets the required storage type for the group entry <ul style="list-style-type: none"> • Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system. • Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

	context	-	Configures the name of the SNMP context. The maximum length of the string is 32.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Group Name	-	iso
	Read/Write/Notify view	-	iso
	Storage Type	-	volatile
	Row status		Active
	Group Name	-	initial
	Read/Write/Notify View	-	restricted
	Storage Type	-	non-volatile
	Group Name	-	Initial
	Read/Write/Notify View	-	iso
	Storage Type	-	non-volatile

Example `iss(config)# snmp access myv2group v2 read v2readview write v2writeview notify v2notifyview nonvolatile`

Related Commands

- **snmp group** - Configures SNMP group details
- **snmp view** - Configures the SNMP view
- **show snmp group** - Displays the configured SNMP groups
- **show snmp group access** - Displays the configured SNMP group access details
- **show snmp viewtree** - Displays the configured SNMP Tree views

ISS

11.8 snmp engineid

This command configures the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination. The no form of the command resets the engine ID to the default value.

- The Engine ID must be given as octets in hexadecimal separated by dots and the allowed length is 5 to 32 octets.
- SNMP engine ID is an administratively unique identifier.
- Changing the value of the SNMP engine ID has significant effects.
- All the user information will be updated automatically to reflect the change

```
snmp engineid <EngineIdentifier>
```

```
no snmp engineid
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 80.00.08.1c.04.46.53

Example iss(config)# snmp engineid 80.0.08.1c.04.5f.a9

- Related Commands**
- **show snmp engineID** - Displays the Engine Identifier
 - **show snmp user** - Displays the configured SNMP users

11.9 snmp proxy name

This command configures the proxy. The no form of the command removes the proxy.

```
snmp proxy name <ProxyName> ProxyType {Read | Write | inform | Trap}
ContextEngineID <EngineId> TargetParamsIn <TargetParam> TargetOut <TargetOut>
[ContextName <ProxyContextName>] [StorageType {volatile | nonvolatile}]
```

```
no snmp proxy name <ProxyName>
```

Syntax	<ProxyName>	-	Identifies an entry in the proxy table.
Description			<ul style="list-style-type: none"> · This will be the INDEX used for the Proxy Table.
	ProxyType	-	<p>Forwards the messages using the translation parameters defined by proxy entry. The list contains:. Options are:</p> <ul style="list-style-type: none"> • Read – Forwards the read messages to get the request from the manager. • Write – Forwards the write messages to set configurations. • Inform – Forwards the notification messages to the agent. • Trap – Forwards the SNMP trap messages to the agent
	ContextEngineID <EngineId>	-	Configures an context engine ID of the agent with whom the manager communicates through the proxy.
	TargetParamsIn <TargetParam>	-	Configures the SNMP version that the manager sends as request to the proxy.
	TargetOut <TargetOut>	-	<p>Configures the SNMP version that the proxy uses to communicate with multiple agent .</p> <ul style="list-style-type: none"> · This object is only used when selection of a single target is required (that is, when forwarding an incoming read or write request).

ISS

ContextName - Configures a unique context name for an SNMP sub agent. This name is used to identify the corresponding sub agent when more than one sub agent exists.
<ProxyContextName>

Storage Type - Sets the required storage type for the group entry

- Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.
- Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Storage Type - Nonvolatile

Example

```
iss(config)# snmp proxy name proxy1 ProxyType write
ContextEngineID 80.00.08.1c.04.46.53 TargetParamsIn param2
TargetOut target2 ContextName pxycxtxtname StorageType
nonvolatile
```

Related Commands

- **show snmp group** - Displays the configured SNMP groups
- **show snmp proxy** – Displays proxy details.

11.10 snmp mibproxy name

This command configures the proxy. The no form of the command removes the proxy.

```
snmp mibproxy name <ProxyName> ProxyType {Read | Write | inform | Trap} mibid
<MibId> TargetParamsIn <TargetParam> TargetOut <TargetOut> [StorageType
{volatile | nonvolatile}]
```

```
no snmp mibproxy name <ProxyMibName>
```

Syntax	<ProxyName>	-	Identifies an entry in the proxy table
Description	ProxyType	-	<ul style="list-style-type: none"> . This will be the INDEX used for the Proxy Table. - Forwards the messages using the translation parameters defined by proxy entry. The list contains:. Options are: <ul style="list-style-type: none"> • Read – Forwards the read messages to get the request from the manager. • • Write – Forwards the write messages to set configurations. • • Inform – Forwards the notification messages to the agent. • • Trap – Forwards the SNMP trap messages to the agent
	Mibid <MibId>	-	Configures an context MIB ID of the agent with whom the manager communicates through the proxy.
	TargetParamsIn<TargetParam>	-	Configures the SNMP version that the manager sends as request to the proxy.
	TargetOut<TargetOut>	-	<ul style="list-style-type: none"> - Configures the SNMP version that the proxy uses to communicate with multiple agent . . This object is only used when selection of a single target is required (that is, when forwarding an incoming read or write request).
	Storage Type	-	<ul style="list-style-type: none"> - Storage type. Options are: <ul style="list-style-type: none"> • volatile • nonvolatile
Mode	Global Configuration Mode		

ISS

Package Workgroup, Enterprise and Metro

Example

```
iss(config)# snmp mibproxy name mibproxy1 ProxyType read mibid 1
TargetParamsIn param1 TargetOut target1 StorageType nonvolatile
```

Related Commands

- `show snmp group` - Displays the configured SNMP groups
- `show snmp mibproxy` - Displays proxy details.

11.11 snmp view

This command configures the SNMP view. To configure an SNMP view (read/write/notify), a group must have already been created using the `snmp group` command and SNMP group access must be configured using the `snmp access` command. The `no` form of the command removes the SNMP view.

```
snmp view <ViewName> <OIDTree> [mask <OIDMask>] {included | excluded}
[volatile | nonvolatile]
```

```
no snmp view <ViewName> <OIDTree>
```

Syntax	<ViewName>	-	Specifies the view name for which the view details are to be configured.
Description	<OIDTree>	-	Specifies the sub tree value for the particular view.
	mask <OIDMask>	-	Specifies a mask value for the particular view.
	included	-	Allows access to the subtree
	excluded		Denies access to the subtree
	volatile		Sets the storage type as temporary. Erases the configuration setting on restarting the system.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	View Name	-	iso/restricted
	OIDTree	-	1
	OIDMask	-	1
	View type	-	included
	Storage type	-	non-volatile
	Row status		Active

ISS

Example `iss(config)# snmp view v2readview 1.3.6.1 mask 1.1.1.1 included nonvolatile`

Related Commands

- `snmp access` - Configures the SNMP group access details
- `show snmp viewtree` - Displays the configured SNMP Tree views
- `show snmp group access` - Displays the configured SNMP group access details

11.12 snmp targetaddr

This command configures the SNMP target address. The no form of the command removes the configured SNMP target address.

```
snmp targetaddr <TargetAddressName> param <ParamName> {<IPAddress> |
<IP6Address>} [timeout <Seconds(1-1500)>] [retries <RetryCount(1-3)>] [taglist
<TagIdentifier | none>] [{volatile | nonvolatile}] [port <integer (1-65535)>]
```

```
no snmp targetaddr <TargetAddressName>
```

Syntax	<TargetAddressName>	-	Configures a unique identifier of the Target.
Description	param<ParamName>	-	Configures the parameters when generating messages to be sent to transport address.
	IPAddress	-	Configures a IP target address to which the generated SNMP notifications are sent.
	IP6Address	-	Configures a IP6 target address to which the generated SNMP notifications are sent.
	timeout<Seconds(1-1500)>	-	Sets the time in which the SNMP agent waits for a response from the SNMP Manager before retransmitting the Inform Request Message. The value ranges between 1 and 1500 seconds.
	retries<RetryCount(1-3)>	-	Sets the maximum number of times the agent can retransmit the Inform Request Message. The value ranges between 1 and 3.
	taglist	-	Sets the tag identifier that selects the target address for the SNMP.
	volatile		Sets the storage type as temporary. Erases the configuration setting on restarting the system
	nonvolatile		Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.

ISS

port <integer (1-65535)> - Configures a port number through which the generated SNMP notifications are sent to the target address. The value ranges between 1 and 65535.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults ParamName - Internet

IPAddress - 10.0.0.10

taglist - snmp

volatile | nonvolatile - volatile

port - 162

Example

```
iss(config)# snmp targetaddr issmgr param issd 10.0.0.10 taglist mytag nonvolatile
```



Target param must have been configured.

Related Commands

- **snmp targetparams** - Configures the SNMP target parameters
- **show snmp targetaddr** - Displays the configured SNMP target Addresses
- **show snmp targetparam** - Displays the configured SNMP Target Address Params

11.13 snmp targetparams

This command configures the SNMP target parameters. The no form of the command removes the SNMP target parameters.

```
snmp targetparams <ParamName> user <UserName> security-model {v1 | v2c | v3
{auth | noauth | priv}} message-processing {v1 | v2c | v3} [{volatile |
nonvolatile}] [filterprofile-name <profile-name> ] [filter-storage-type
{volatile | nonvolatile}]
```

```
no snmp targetparams <ParamName>
```

Syntax	<ParamName>	-	Sets a unique identifier of the parameter.
Description	User <UserName>	-	Sets an user for which the target parameter is to be done.
	security-model	-	Sets the security model <ul style="list-style-type: none"> • v1 – Sets the SNMP version as Version 1. • v2c – Sets the SNMP version as Version 2. • v3 – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
	auth	-	Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication
	noauth	-	Sets no-authentication
	priv	-	Specifies both authentication and privacy
	message-processing	-	Sets the message processing model <ul style="list-style-type: none"> • v1 – Sets the SNMP version as Version 1. • v2c – Sets the SNMP version as Version 2. • v3 – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
	volatile		Sets the storage type as temporary. Erases the configuration setting on restarting the system

ISS

nonvolatile Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.

filterprofile-name Configures the profile name
 <profilename>

filter-storage-type Sets the required storage type for the filter profile

- Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.
- Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Target ParamName - internet

User/Security Name - None

Security Model - v2c

Security Level - NoauthNoPriv

Message Processing Model - v2c

Storage Type - Non-volatile

Row status Active

Filter profile name None

ParamName - test1

User/Security Name - None

Security Model - v1

Security Level	-	NoauthNoPriv
Message Processing Model	-	v1
Storage Type	-	Non-volatile
Row status		Active
Filter profile name		None

Example `iss(config)# snmp targetparams param1 user user1 security-model v3 noauth message-processing v3`



User information must have been configured prior to the configuration of SNMP target parameters

Related Commands

- `snmp user` - Configures the SNMP user details
- `snmp targetaddr` - Configures the SNMP target address
- `show snmp targetparam` - Displays the configured SNMP Target Address Params
- `show snmp user` - Displays the configured SNMP users.
- `show snmp notif` - Displays the configured SNMP Notifications

11.14 snmp user

This command configures the SNMP user details. The no form of the command removes the SNMP user details.

```
snmp user <UserName> [auth {md5 | sha} <passwd> [priv DES <passwd>]]
[volatile | nonvolatile] [EngineId <EngineID>]
```

```
no snmp user <UserName> [EnginId <EngineID>]
```

Syntax	<UserName>	-	Configures an user name which is the User-based Security Model dependent security ID.
Description	auth	-	Sets an authentication Algorithm . Options are: <ul style="list-style-type: none"> • md5 - Sets the Message Digest 5 based authentication. • sha - Sets the Security Hash Algorithm based authentication.
	<Passwd>	-	Sets the password for the user name.
	priv DES<passwd>	-	Sets a secret authentication key used for messages sent on behalf of this user
	volatile	-	Sets the storage type as temporary. Erases the configuration setting on restarting the system
	nonvolatile		Sets the storage type as permanent. Saves the configuration to the system. You can view the saved configuration on restarting the system
	EngineId <EngineID>		Sets the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults UserName - Initial

Authentication Protocol	-	None
Privacy Protocol	-	None
Storage type	-	Non-volatile
Storage type	-	Non-volatile

Example `iss(config)# snmp user user1`



SNMP passwords are localized using the local SNMP engine ID

Related Commands

- `show snmp engineID` - Displays the Engine Identifier
- `show snmp user` - Displays the configured SNMP users
- `snmp targetparams` - Configures the SNMP target parameters
- `show snmp group` - Displays the configured SNMP groups

11.15 snmp notify

This command configures the SNMP notification details. The no form of this command removes the SNMP notification details.

```
snmp notify <NotifyName> tag <TagName> type {Trap | Inform} [{volatile | nonvolatile}]
```

```
no snmp notify <NotifyName>
```

Syntax	<NotifyName>	-	Configures an unique identifier associated with the entry.
Description	tag<TagName>	-	Sets a notification tag, which selects the entries in the Target Address Table.
	type	-	Sets the notification type. The list contains: <ul style="list-style-type: none"> • Trap – Allows routers to send traps to SNMP managers. Trap is a one-way message from a network element such as a router, switch or server; to the network management system. • Inform – Allows routers / switches to send inform requests to SNMP managers
	volatile	-	Sets the storage type as temporary. Erases the configuration setting on restarting the system.
	nonvolatile	-	Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults	Notify Name	-	iss/iss1
	Notify Tag	-	iss/iss1
	Storage type	-	volatile

Example iss(config)# snmp notify notel tag tag1 type Inform

Related Commands

- `show snmp notif` - Displays the configured SNMP Notifications
- `show snmp targetaddr` - Displays the configured SNMP target Addresses

ISS

11.16 snmp filterprofile

This command creates Notify filter Table. The no form of the command removes the filter entry from the table.

```
snmp filterprofile <profile-name> <OIDTree> [mask <OIDMask>] {included |
excluded} [{volatile | nonvolatile}]
```

```
no snmp filterprofile <profilename> <OIDTree>
```

Syntax	profile-name	-	Name of the filter profile.
Description	OIDTree	-	Object Identifier
	mask <OIDMask>	-	Defines a family of subtrees, in combination with the object identifier.
	included excluded		Type of filter. This indicates whether the OID and mask should be included in or excluded from the filter profile.
	volatile nonvolatile		Storage type. <ul style="list-style-type: none"> • volatile - Temporary storage. Details are lost once restarted. • nonvolatile - Permanent storage. Details are present even after restart.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss(config)# snmp filterprofile filter1 1.5 mask 1.1 included nonvolatile

- Related Commands**
- **show snmp filter** - Displays the configured SNMP filters
 - **snmp targetparams** - Configures the SNMP target parameters

11.17 snmp-server enable traps snmp authentication

This command enables generation of authentication traps for SNMPv1 and SNMPv2c. The no form of the command disables generation of authentication traps for SNMPv1 and SNMPv2c.

snmp-server enable traps snmp authentication

no snmp-server enable traps snmp authentication

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Disabled

Example `iss(config)# snmp-server enable traps snmp authentication`

ISS

11.18 snmp-server trap udp-port

This command configures the udp port over which agent sends the trap. The no form of the command configures the snmp agent to sent trap on default udp port.

```
snmp-server trap udp-port <port>
```

```
no snmp-server trap udp-port
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss(config)# snmp-server trap udp-port 1234

Related Commands `show snmp notif` - Displays the configured SNMP Notification types.

11.19 snmp-server trap proxy-udp-port

This command configures the udp port over which agent sends the trap. The no form of the command configures the snmp agent to sent trap on default udp port.

```
snmp-server trap proxy-udp-port <port>
```

```
no snmp-server trap proxy-udp-port
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 162

Example iss(config)# snmp-server trap proxy-udp-port 162

Related Commands `show snmp-server proxy-udp-port` - Displays the proxy udp port.

ISS

11.20 snmp agent port

This command configures the agent port on which agent listens.

snmp agent port <port>

Syntax	port	-	Port number. This value ranges between 1 and 65535.
Description			
Mode			Global Configuration Mode
Package			Workgroup, Enterprise and Metro
Defaults			161
Example			<code>iss(config)# snmp agent port 100</code>
Related Commands			<code>show snmp</code> - Displays the status information of SNMP communications

11.21 snmp tcp enable

This command enables sending snmp messages over tcp. The no form of the command disables sending snmp messages over tcp.

snmp tcp enable

no snmp tcp enable

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Disabled

Example `iss(config)# snmp tcp enable`

Related Commands `show snmp tcp` - Displays the configuration for snmp over tcp.

ISS

11.22 snmp trap tcp enable

This command enables sending snmp trap messages over tcp. The no form of the command disables sending snmp trap messages over tcp.

```
snmp trap tcp enable
```

```
no snmp trap tcp enable
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Disabled

Example `iss(config)# snmp trap tcp enable`

Related Commands `show snmp tcp` - Displays the configuration for snmp over tcp.

11.23 snmp-server tcp-port

This command configures the tcp port over which agent sends the snmp message. The no form of the command configures the snmp agent to sent snmp message on default tcp port.

```
snmp-server tcp-port <port>
```

```
no snmp-server tcp-port
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 161

Example `iss(config)# snmp-server tcp-port 161`

Related Commands `show snmp tcp` - Displays the configuration for snmp over tcp.

ISS

11.24 snmp-server trap tcp-port

This command configures the tcp port over which agent sends the trap. The no form of the command configures the snmp agent to sent trap on default tcp port.

```
snmp-server trap tcp-port <port>
```

```
no snmp-server trap tcp-port
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 162

Example iss(config)# snmp-server trap tcp-port 162

Related Commands `show snmp tcp` - Displays the configuration for snmp over tcp.

11.25 snmp-server enable traps

This command enables generation of a particular trap. The no form of the command disables generation of a particular trap.

```
snmp-server enable traps {[firewall-limit] [linkup] [linkdown] [sip-states]
[sip-cfg-change] [coldstart] [poe-power] [dhcp-pool-limit] [dsx1-line]}
```

```
no snmp-server enable traps {[firewall-limit] [linkup] [linkdown] [sip-states]
[sip-cfg-change] [coldstart] [poe-power] [dhcp-pool-limit] [dsx1-line]}
```

Syntax	firewall-limit	-	Generates a trap for all the firewall attack summary
Description	linkup	-	Generates a trap whenever there is a linkup
	linkdown	-	Generates a trap whenever there is a linkdown
	sip-states	-	Generates a trap for all the SIP states .
	sip-cfg-change	-	Generates a trap for all the SIP configuration
	coldstart	-	Generates a trap for all the Coldstart
	poe-power	-	Generates a trap whenever there is Power on Ethernet
	dhcp-pool-limit	-	Generates a trap for all the DHCP server pool limit trap
	dsx1-line	-	Generates a trap for all the DSX1 line trap

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss(config)# snmp-server enable traps firewall-limit

Related Commands **show snmp-server traps** - Displays the set of traps that are currently enabled.

ISS

11.26 show snmp agentx information

This command displays global information of SNMP Agentx communications.

show snmp agentx information

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp agentx information

```
Agentx Subagent is enabled
TransportDomain :TCP
Master IP Address :10.0.0.2
Master PortNo :705
```

Related Commands

- **enable snmpsubagent** - Enables either snmp agent or agentx-subagent capabilities.
- **disable snmpsubagent** - Disables agentx-subagent.
- **disable snmpagent** - Disables agentx-subagent.

11.27 show snmp agentx statistics

This command displays all the information regarding SNMP Agentx statistics.

show snmp agentx statistics

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp agentx statistics

```
Tx Statistics
  Transmitted Packets           :860
  Open PDU                      :1
  Index Allocate PDU           :0
  Index DeAllocate PDU        :0
  Register PDU                 :2
  Add Agent Capabilities PDU   :0
  Notify PDU                   :0
  Ping PDU                     :20
  Remove Agent Capabilities PDU :0
  UnRegister PDU              :0
  Close PDU                    :0
  Response PDU                 :837

Rx Statistics
  Rx Packets                    :859
  Get PDU                      :1
  GetNext PDU                   :836
  GetBulk PDU                   :0
  TestSet PDU                   :0
  Commit PDU                    :0
  Cleanup PDU                   :0
  Undo PDU                      :0
  Dropped Packets              :0
  Parse Drop Errors            :1
  Open Fail Errors             :0
  Close PDU                    :0
  Response PDU                 :21
```

- Related Commands**
- **enable snmpsubagent** - Enables either snmp agent or agentx-subagent capabilities.
 - **disable snmpsubagent** - Disables agentx-subagent.
 - **disable snmpagent** - Disables agentx-subagent

ISS

11.28 show snmp

This command displays the status information of SNMP communications.

show snmp

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example `iss# show snmp`

```
0 SNMP Packets Input
  0 Bad SNMP Version errors
  0 Unknown community name
  0 Get request PDUs
  0 Get Next PDUs
  0 Set request PDUs

0 SNMP Packets Output
  0 Too big errors
  0 No such name errors
  0 Bad value errors
  0 General errors
  0 Trap PDUs

0 SNMP Rollback failures

SNMP Manager-role output packets
  0 Drops

SNMP Informs:
  0 Inform Requests generated
  0 Inform Responses received
  0 Inform messages Dropped
  0 Inform Requests awaiting Acknowledgement

SNMP Trap Listen Port is 162

snmp agent port : 170
```

Related Command

- **snmp community index** – Configures the SNMP community details

11.29 show snmp community

This command displays the configured SNMP community details.

show snmp community

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp community

```
Community Index: NETMAN
Community Name: NETMAN
Security Name: none
Context Name:
Transport Tag:
Storage Type: volatile
Row Status: active
-----
```

```
Community Index: PUBLIC
Community Name: PUBLIC
Security Name: none
Context Name:
Transport Tag:
Storage Type: volatile
Row Status: active
```

Related Command **snmp community index** - Configures the SNMP community details

ISS

11.30 show snmp group

This command displays the configured SNMP groups.

show snmp group

Mode Privileged EXEC Mode
Package Workgroup, Enterprise and Metro
Example iss# show snmp group

```
Security Model: v1
Security Name: none
Group Name: iso
Storage Type: volatile
Row Status: active
-----
Security Model: v2c
Security Name: none
Group Name: iso
Storage Type: volatile
Row Status: active
-----
Security Model: v3
Security Name: initial
Group Name: initial
Storage Type: nonVolatile
Row Status: active
-----
Security Model: v3
Security Name: templateMD5
Group Name: initial
Storage Type: nonVolatile
Row Status: active
-----
Security Model: v3
Security Name: templateSHA
Group Name: initial
Storage Type: nonVolatile
Row Status: active
```

Related Commands

- **snmp group** - Configures the SNMP group details
- **snmp access** - Configures the SNMP group access details
- **snmp user** - Configures the SNMP user details
- **snmp proxy name** - Configures the proxy.
- **snmp mibproxy name** - Configures the mibproxy.

11.31 show snmp group access

This command displays the configured SNMP group access details.

show snmp group access

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp group access

```
Group Name: iso
Read View: iso
Write View: iso
Notify View: iso
Storage Type: volatile
Row Status: active
-----
```

```
Group Name: iso
Read View: iso
Write View: iso
Notify View: iso
Storage Type: volatile
Row Status: active
-----
```

```
Group Name: initial
Read View: restricted
Write View: restricted
Notify View: restricted
Storage Type: nonVolatile
Row Status: active
-----
```

```
Group Name: initial
Read View: iso
Write View: iso
Notify View: iso
Storage Type: nonVolatile
Row Status: active
```

- Related Commands**
- **snmp access** - Configures the SNMP group access details
 - **snmp view** - Configures the SNMP view

ISS

11.32 show snmp engineID

This command displays the Engine Identifier.

show snmp engineID

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp engineID

EngineId: 80.00.08.1c.04.46.53

Related Command

- **snmp engineid** - Configures the engine identifier
- **snmp user** - Configures the SNMP user details

11.33 show snmp proxy

This command displays proxy details.

show snmp proxy

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp proxy

```
Proxy Name           : PROXY1
Proxy ContextEngineID : 80.00.08.1c.04.46.54
Proxy ContextName    :
Proxy TargetParamIn  : param1
Proxy SingleTargetOut : Tgt1
Proxy MultipleTargetOut :
Proxy Type           : Read
Storage Type        : Non-volatile
Row Status          : Active
```

```
-----
Proxy Name           : PROXY2
Proxy ContextEngineID : 80.00.08.1c.04.46.54
Proxy ContextName    :
Proxy TargetParamIn  : param1
Proxy SingleTargetOut : Tgt1
Proxy MultipleTargetOut :
Proxy Type           : Write
Storage Type        : Non-volatile
Row Status          : Active
-----
```

Related Command **snmp proxy name** - Configures the proxy.

ISS

11.34 show snmp mibproxy

This command displays proxy details.

show snmp mibproxy

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp mibproxy

```
Prop Proxy Name           : proxy1
Prop MibID                 : 2
Prop Proxy TargetParamIn  : param1
Prop Proxy SingleTargetOut : target1
Prop Proxy MultipleTargetOut :
Prop Proxy Type           : Read
Prop Storage Type         : Non-volatile
Prop Row Status           : Active
-----
```

Related Command `snmp mibproxy name` - Configures the proxy.

11.35 show snmp viewtree

This command displays the configured SNMP Tree views.

show snmp viewtree

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp viewtree

```
View Name: iso
Subtree OID: 1
Subtree Mask:
View Type: included
Storage Type: nonVolatile
Row Status: active
-----
```

```
View Name: restricted
Subtree OID: 1
Subtree Mask:
View Type: included
Storage Type: nonVolatile
Row Status: active
-----
```

Related Command

- **snmp access** - Configures the SNMP group access details
- **snmp view** - Configures the SNMP view

ISS

11.36 show snmp targetaddr

This command displays the configured SNMP target Addresses.

show snmp targetaddr

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example `iss# sh snmp targetaddr`

```
Target Address Name : ht231
IP Address          : 12.0.0.100
Port                : 150
Tag List            : tg231
Parameters          : pa231
Storage Type       : Non-volatile
Row Status          : Active
```

- Related Commands**
- `snmp targetaddr` - Configures the SNMP target address
 - `snmp targetparams` - Configures the SNMP target parameters
 - `snmp notify` - Configures the SNMP notification details

11.37 show snmp targetparam

This command displays the configured SNMP Target Address Params.

show snmp targetparam

Mode Privileged EXEC Mode
Package Workgroup, Enterprise and Metro
Example iss# sh snmp targetparam

```
Target Parameter Name      : internet
Message Processing Model   : v2c
Security Model             : v2c
Security Name              : none
Security Level             : No Authentitcation, No Privacy
Storage Type              : Non-volatile
Row Status                 : Active
Filter Profile Name       : None
Row Status                 : Active
-----
Target Parameter Name      : pa231
Message Processing Model   : v3
Security Model             : v3
Security Name              : u231
Security Level             : No Authentitcation, No Privacy
Storage Type              : Volatile
Row Status                 : Active
Filter Profile Name       : filter1
Row Status                 : Active
-----
Target Parameter Name      : test1
Message Processing Model   : v2c
Security Model             : v1
Security Name              : none
Security Level             : No Authentitcation, No Privacy
Storage Type              : Non-volatile
Row Status                 : Active
Filter Profile Name       : None
Row Status                 : Active
-----
```

Related Commands

- **snmp targetaddr** - Configures the SNMP target address
- **snmp targetparams** - Configures the SNMP target parameters
- **snmp user** - Configures the SNMP user details

ISS

11.38 show snmp user

This command displays the configured SNMP users.

show snmp user

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp user

```
Engine ID: 80.00.08.1c.04.46.53
User: initial
Authentication Protocol: none
Privacy Protocol: none
Storage Type: nonVolatile
Row Status: active
-----
```

```
Engine ID: 80.00.08.1c.04.46.53
User: templateMD5
Authentication Protocol: MD5
Privacy Protocol: none
Storage Type: nonVolatile
Row Status: active
-----
```

```
Engine ID: 80.00.08.1c.04.46.53
User: templateSHA
Authentication Protocol: SHA
Privacy Protocol: DES_CBC
Storage Type: nonVolatile
Row Status: active
-----
```

Related Commands

- **snmp group** - Configures the SNMP group details
- **snmp user** - Configures the SNMP user details
- **show snmp community** - Displays the configured SNMP community details
- **snmp engineid** - Configures the engine identifier
- **snmp targetparams** - Configures the SNMP target parameters

11.39 show snmp notif

This command displays the configured SNMP Notification types.

show snmp notif

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp notif

```
Notify Name: iss
Notify Tag: iss
Notify Type: trap
Storage Type: volatile
Row Status: active
-----
```

```
Notify Name: iss1
Notify Tag: iss1
Notify Type: trap
Storage Type: volatile
Row Status: active
```

**Related
Commands**

- **snmp notify** - Configures the SNMP notification details
- **snmp targetparams** - Configures the SNMP target parameters
- **snmp-server trap udp-port**- Configures the udp port over which agent sends the trap

ISS

11.40 show snmp inform statistics

This command displays the inform message statistics.

show snmp inform statistics

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp inform statistics

```
Target Address Name : issmanager
IP Address          : 10.0.0.10
Inform messages sent : 20
Acknowledgement awaited for : 2 Inform messages
Inform messages dropped : 0
Acknowledgement failed for : 0 Inform messages
Informs retransmitted: 0
Inform responses received: 18
```



SNMP Manager must have been configured and Inform type notifications must have been generated.

11.41 show snmp-server traps

This command displays the set of traps that are currently enabled.

show snmp-server traps

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp-server traps

```
Currently enabled traps:
-----
linkup,linkdown,
```

Related Command **snmp-server enable traps** - Enables generation of a particular trap.

ISS

11.42 show snmp-server proxy-udp-port

This command displays the proxy udp port.

```
show snmp-server proxy-udp-port
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show snmp-server proxy-udp-port  
snmp-server proxy-udp-port : 162
```

Related Command `snmp-server trap proxy-udp-port` - Configures the udp port over which agent sends the trap.

11.43 show snmp tcp

This command displays the configuration for snmp over tcp.

show snmp tcp

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show snmp tcp
snmp over tcp disabled
snmp trap over tcp disabled
snmp listen tcp port 161
Snmp listen tcp trap port 162
```

Related Command

- **snmp tcp enable** – Enables sending snmp messages over tcp.
- **snmp trap tcp enable** - Enables sending snmp trap messages over tcp.
- **snmp-server tcp-ports** – Configures the tcp port over which agent sends the snmp message.
- **snmp-server trap tcp-ports** - Configures the tcp port over which agent sends the trap.

ISS

11.44 show snmp filter

This command displays the configured SNMP filters.

show snmp filter

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show snmp filter

```
Filter Name   : filter1
Subtree OID   : 1.5
Subtree Mask  : 1.1
Filter Type   : Included
Storage Type  : Non-volatile
Row Status    : Active
-----
```

Related Command

- **snmp filterprofile** - Creates Notify filter Table

Chapter

12

Syslog

Syslog is a protocol used for capturing log information for devices on a network. The syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is simply designed to transport the event messages.

One of the fundamental tenets of the syslog protocol and process is its simplicity. The transmission of syslog messages may be started on a device without a receiver being configured, or even actually physically present. This simplicity has greatly aided the acceptance and deployment of syslog.

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

- logging
- logging synchronous
- mailserver
- sender mail-id
- cmdbuffs
- clear logs
- syslog mail
- syslog local storage
- syslog filename-one
- syslog filename-two
- syslog filename-three
- syslog relay - port

ISS

- syslog profile
- logging-file
- logging server
- syslog relay
- syslog relay transport type
- show logging
- show email alerts
- show syslog role
- show syslog mail
- show syslog localstorage
- show logging-file
- show logging-server
- show mail-server
- show syslog relay-port
- show syslog profile
- show syslog relay transport type
- show syslog file-name
- show syslog information

12.1 logging

This command enables syslog server and configures the syslog related parameters. The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server. The no form of the command disables syslog server and resets the configured parameters. The existing syslog buffers will not be cleared and none of the configured options will be changed, when the syslog feature is disabled.

```
logging { buffered [<size (1-200)>] | console | facility {local0 | local1 |
local2 | local3 | local4 | local5 | local6 | local7|}| severity [{ <level (0-
7)> | alerts | critical | debugging | emergencies | errors | informational |
notification | warnings }] | on }
```

```
no logging { buffered | console | facility | severity | on }
```

Syntax	buffered	- Limits Syslog messages displayed from an internal buffer. This size ranges between 1 and 200 entries.
Description		<ul style="list-style-type: none"> • The size feature is optional only in the code using the industrial standard command, otherwise this feature is mandatory.
	console	- Limits messages logged to the console.
	facility	- The facility that is indicated in the message. Can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7.
	severity	<ul style="list-style-type: none"> - Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are: <ul style="list-style-type: none"> • 0 emergencies - System is unusable. • 1 alerts - Immediate action needed. • 2 critical - Critical conditions. • 3 errors - Error conditions. • 4 warnings - Warning conditions. • 5 notification - Normal but significant conditions. • 6 informational - Informational messages. • 7 debugging – Debugging messages.
	alerts	- Immediate action needed
	critical	- Critical conditions
	debugging	- Debugging messages
	emergencies	- System is unusable
	errors	- Error conditions

ISS

- informational** - Information messages
- notification** - Normal but significant messages
- warnings** - Warning conditions
- on** - Syslog enabled

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

- Defaults**
- console - enabled
 - severity - informational, when no option is selected while debugging, at system start-up.
 - buffered - 50
 - facility - local0

Example `iss(config)# logging 12.0.0.2`



- The log file is stored in ASCII text format. The Privileged EXEC command is used to display its contents
- The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or Syslog server
- The existing syslog buffers will not be cleared and none of the configured options will be changed, when the Syslog feature is disabled

Related Command `show logging` - Displays Logging status and configuration information

-

12.2 logging synchronous

This command enables synchronous logging of messages.

This command is a complete standardized implementation of the existing command. It operates similar to that of the command logging.

```
logging synchronous {severity [{<short (0-7)> | alerts | critical | debugging
| emergencies | errors | informational | notification | warnings|all}] | limit
<number-of-buffers (size (1-200)) }
```

Syntax	severity	<ul style="list-style-type: none"> - Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are: <ul style="list-style-type: none"> • 0 emergencies - System is unusable. • 1 alerts - Immediate action needed. • 2 critical - Critical conditions. • 3 errors - Error conditions. • 4 warnings - Warning conditions. • 5 notification - Normal but significant conditions. • 6 informational - Informational messages. • 7 debugging – Debugging messages. • all - All messages are printed asynchronously regardless of the severity level.
Description	limit	<ul style="list-style-type: none"> - Number of buffers to be queued for the terminal after which new messages are dropped. This value ranges between 1 and 200 entries.
Mode	Line Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Defaults	severity	<ul style="list-style-type: none"> - informational, when no option is selected while configuration. debugging, at system start-up.
	limit	<ul style="list-style-type: none"> - 50
Example	<pre>iss(config-line)# logging synchronous severity 4</pre>	



- The log file is stored in ASCII text format. The Privileged EXEC command is used to display its contents.
- The logging process controls the distribution of logging messages to the various

ISS

destinations, such as the logging buffer, logging file, or Syslog server.

- The existing syslog buffers will not be cleared and none of the configured options will be changed, when the Syslog feature is disabled.

**Related
Command**

show logging - Displays Logging status and configuration information

12.3 mailserver

This command sets the mail server IP address to be used for sending email alert messages and the no form of the command re-sets the mail server IP address used for sending email alert messages.

```
mail-server <short (0-191)> {ipv4 <uicast_addr> | ipv6 <ip6_addr>} <string(50)>
```

```
no mail-server <short (0-191)> {ipv4 <uicast_addr> | ipv6 <ip6_addr>}
```

Syntax	<short (0-191)>	-	Sets the priority for that particular mail-server configuration. The value ranges between 0 and 191.
Description	ipv4<uicast_addr>	-	Configures the ipv4 destination address for the syslog mail server
	ipv6<ip6_addr>	-	Configures the ipv6 destination address for the syslog mail server.
	<string(50)>	-	Specifies the receiver mail id in which the email alert messages are received and logged.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config)# mail-server 190 ipv4 23.78.67.89 support@Interface  
Masters.com
```

Related Commands

- **logging** - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- **show email alerts** - Displays email alerts related configuration

ISS

12.4 sender mail-id

This command sets the sender mail id from which the email alert messages are sent. The no form of the command deletes the configured sender mail id.

```
sender mail-id <mail-id (100)>
```

```
no sender mail-id
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults syslog@InterfaceMasters.com

Example `iss(config)# sender mail-id plabinik@InterfaceMasters.com`



This command can be executed only if the mail server is configured.

- Related Commands**
- **mailserver** - Sets the mail server IP address to be used for sending email alert messages
 - **logging** - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
 - **show logging** - Displays Logging status and configuration information
 - **show email alerts** - Displays email alerts related configuration
 - **receiever mail-id** - Sets the receiver mail id

12.5 cmdbuffs

This command configures the number of syslog buffers for a particular user.

```
cmdbuffs <user name> <no.of buffers (1-200)>
```

Syntax	<user name>	-	User Name
Description	<no.of buffers (1-200)>	-	Number of log buffers to be allocated in the system
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	50		
Example	iss(config)#cmdbuffs Interface Masters 50		
Related Commands	<ul style="list-style-type: none">• logging - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter• show logging - Displays Logging status and configuration information• clear logs - Clears the logs buffered in the system.• username - Creates a user and sets the enable password for that user with the privilege level.		

ISS

12.6 clear logs

This command clears the system syslog buffers.

clear logs

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# clear logs`

- Related Commands**
- **cmdbuffs** - Configures the number of Syslog buffers for a particular user
 - **logging** - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
 - **show logging** - Displays Logging status and configuration information

12.7 syslog mail

This command enables the syslog mail storage in the system. By enabling syslog mail storage,, ISS sends the syslog messages as mail messages to the mail-server configured in the system. The no form of command disables the mail option in syslog.

syslog mail

no syslog mail

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# syslog mail`

Related

- Commands**
- **show syslog mail** - Displays the mail option in syslog.
 - **mail server table** - Adds an entry to mail-server table.
 - **show syslog information** - Displays the status of consolidated syslog log information.

12.8 syslog local storage

This command enables the syslog file storage to log the status in the local storage path. The no form of command disables the syslog local storage.

syslog localstorage

no syslog localstorage

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss (config)# syslog localstorage

- Related Commands**
- **show syslog local storage** - Displays the syslog local storage.
 - **syslog filename-one** - Configures the file name to store the syslog messages.
 - **syslog filename-two** - Configures the file name to store the syslog messages.
 - **syslog filename-three** - Configures the file name to store the syslog messages
 - **logging-file** - Adds an entry in to file table
 - **show syslog file-name** - Displays all the syslog local storage file names.
 - **show syslog information** - Displays the status of consolidated syslog log information.

12.9 syslog filename-one

This command configures a first file to store the syslog messages locally. The maximum size of the file name is 32.

```
syslog filename-one <string(32)>
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss (config)# syslog filename-one iss1`



This command is executed only if syslog local storage is enabled.

Related Commands

- **syslog local storage** - Enables the syslog local storage
- **logging-file** - Adds an entry in to file table
- **show syslog local storage** - Displays the syslog local storage.
- **show logging-file** - Displays the Syslog file table
- **show syslog file-name** - Displays all the syslog local storage file names.

ISS

12.10 syslog filename-two

This command configures a second file name to store the syslog messages locally. The maximum size of the file name is 32.

```
syslog filename-two <string(32)>
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# syslog filename-two iss2`



This command is executed only if syslog local storage is enabled.

Related Commands

- **syslog local storage** - Enables the syslog local storage
- **show syslog file-name** - Displays the Syslog local storage file name
- **logging-file** - Adds an entry in to file table
- **show syslog local storage** - Displays the syslog local storage.
- **show logging-file** - Displays the Syslog file table

12.11 syslog filename-three

This command configures a third file name to store the syslog messages locally. The maximum size of the file name is 32.

```
syslog filename-three <string(32)>
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# syslog filename-three iss3`



This command is executed only if syslog local storage is enabled.

Related Commands

- `syslog local storage` - Enables the syslog local storage
- `show syslog file-name` - Displays the Syslog local storage file name
- `logging-file` - Adds an entry in to file table
- `show syslog local storage` - Displays the syslog local storage.
- `show logging-file` - Displays the Syslog file table

ISS

12.12 syslog relay - port

This command sets the syslog port through which the relay receives the syslog messages irrespective of the transport type. The port number ranges between 0 and 65535. The no form of command sets the syslog port to default port.

```
syslog relay-port <integer(0-65535)>
```

```
no syslog relay-port
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss(config)# syslog relay-port 500

Default 514



This command is executed only if syslog relay is enabled.

Related Commands

- **syslog relay** - Changes the syslog role from device to relay
- **syslog relay transport type** - Sets the syslog relay transport type either as udp or tcp
- **show syslog relay - port** - Displays the syslog relay port
- **show syslog relay transport type** - Displays the Syslog relay transport type

12.13 syslog profile

This command sets the profile for reliable syslog. The no form of command sets the profile to default (raw) for Reliable Syslog.

```
syslog profile {raw | cooked3}
```

```
no syslog profile
```

Syntax Description	raw	-	Sets the syslog profile as raw which is the profile with minimum number of beep.
	cooked	-	Sets the syslog profile as cooked. This feature is not supported. It may be implemented in the future.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Default	Raw		
Example	iss(config)# syslog profile raw		
Related Commands	• show syslog profile - Displays the Syslog profile.		

³ This feature is not supported .It may be implemented in the future.

12.15 logging server

This command configures a server table to log an entry in it. The no form of command deletes an entry from the server table.

```
logging-server <short(0-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr>} [ port
<integer(0-65535)>] [{udp | tcp | beep}]
```

```
no logging-server <short(0-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr>}
```

Syntax Description	<short(0-191)>	-	Sets the priority for the syslog messages. 0-lowest priority, 191-highest priority.
	ipv4 <ucast_addr>	-	Sets the server address type as internet protocol version 4.
	ipv6 <ip6_addr>		Sets the server address type as internet protocol version 6.
	port	-	Sets the port number through which it sends the syslog message.
	udp	-	Sets the forward transport type as udp.,
	tcp	-	Sets the forward transport type as tcp,
	beep	-	Sets the forward transport type as beep.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Example	iss (config)# logging-server 134 ipv4 12.0.0.3		
Related Commands	<ul style="list-style-type: none"> • show logging server - Displays the Syslog logging server table 		

ISS

12.16 syslog relay

This command changes the syslog role from device to relay. The no form of command changes the syslog role from relay to device.

syslog relay

no syslog relay

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# syslog relay`

- Related Commands**
- **show syslog relay-port** - Displays the syslog relay port
 - **show syslog role** - Displays the syslog role.
 - **syslog relay transport type** - Sets the syslog relay transport type either as udp or tcp
 - **syslog relay - port** - Sets the syslog port through which it receives the syslog messages
 - **show syslog relay transport type** - Displays the Syslog relay transport type
 - **show syslog information** - Displays the status of consolidated syslog log information.

12.17 syslog relay transport type

This command sets the Syslog relay transport type either as `udp` or `tcp`.

```
syslog relay transport type {udp | tcp}
```

Syntax `udp` - Sets the relay transport type as `udp`

Description `tcp` - Sets the relay transport type as `tcp`

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# syslog relay transport type udp`



This command is executed only if `syslog relay` is enabled.

Related Commands

- `syslog relay` - changes the syslog role from device to relay
- `show syslog role` - Displays the syslog role.
- `syslog relay - port` - Sets the syslog port through which it receives the syslog messages
- `show syslog relay transport type` - Displays the Syslog relay transport type
- `show syslog relay - port` - Displays the Syslog relay port.

ISS

12.18 show logging

This command displays all the logging status and configuration information.

show logging

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show logging

System Log Information

```
-----
Syslog logging   : enabled(Number of messages 0)
Console logging  : enabled(Number of messages 0)
TimeStamp option : enabled
Severity logging : Debugging
Log server IP    : 10.0.0.1
Facility         : Default (local0)
Buffered size    : 100
```

LogBuffer(0 Entries, 0 bytes)

**Related
Commands**

- **logging** - Enables Syslog Server and configures Syslog Server IP address, log-level and other Syslog related parameter
- **sender mail-id** - Sets the sender mail id from which the email alert messages are sent.
- **cmdbuffs** - Configures the number of syslog buffers for a particular user.
- **clear logs** - Clears the logs buffered in the system..

12.19 show email alerts

This command displays configurations related to email alerts.

show email alerts

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show email alerts

```
Sender email-id : syslog@Interface Masters.com  
Receiver email-id : admin@Interface Masters.com  
Mail server IP : 12.0.0.3
```



This command is executed only if mail server is configured.

- Related Commands**
- **mail-server** - Sets the mail server IP address to be used for sending email alert messages
 - **sender mail-id** - Sets the sender mail id from which the email alert messages are sent.

ISS

12.20 show syslog role

This command displays the syslog role.

show syslog role

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show syslog role

Related Commands

[Syslog Role](#) : [Relay](#)

- **syslog relay** - Changes the syslog role from device to relay
- **syslog relay transport type** - Sets the syslog relay transport type either as udp or tcp

12.21 show syslog mail

This command displays status of the mail option in syslog.

```
show syslog mail
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show syslog mail

```
Syslog Mail Option : Enabled
```

Related Commands

- `syslog mail` – Enables the mail option in syslog

ISS

12.22 show syslog localstorage

This command displays the syslog local storage.

show syslog localstorage

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show syslog localstorage

```
Syslog Localstorage : Enabled
```

**Related
Commands**

- **syslog local storage** - Enables the syslog local storage
- **syslog filename-one** - Configures the first file to store the syslog messages locally
- **syslog filename-two** - Configures the second file name to store the syslog messages locally
- **syslog filename-three** - Configures the third file name to store the syslog messages locally
- **shpw syslog file-name** - Displays all the syslog local storage file names.

12.23 show logging-file

This command displays the priority and file name of all the three files configured in the syslog file table.

show logging-file

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show logging-file

```
Syslog File Table Information
```

```
-----  
Priority   File-Name  
-----  
134       iss1  
  
134       iss2  
  
134       iss3
```

**Related
Commands**

- **syslog** - Configures the first file to store the syslog messages locally
- **syslog filename-two** - Configures the second file name to store the syslog messages locally
- **syslog filename-three** - Configures the third file name to store the syslog messages locally
- **logging-file** - Adds an entry in to file table

ISS

12.24 show logging-server

This command displays the information about the syslog logging server table.

show logging-server

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show logging-server

Syslog Forward Table Information

Priority	Address-Type	IpAddress	Port	Trans-Type
129	ipv4	12.0.0.2	514	udp
134	ipv4	12.0.0.1	514	udp

Related Commands

- **logging server** - Adds an entry in to logging-server table

12.25 show mail-server

This command displays the information about the syslog mail server table.

show mail-server

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show mail-server

Syslog Mail Table Information

```
-----  
Priority  Address-Type  IPAddress  Receiver Mail-Id  
-----  
134      ipv4           12.0.0.100 root@localhost
```

Related Commands

- **mail server table** - Adds an entry to mail-server table

ISS

12.26 show syslog relay-port

This command displays the Syslog relay port.

```
show syslog relay-port
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show syslog relay-port
Syslog Port : 251

Related Commands

- **syslog relay - port** - Sets the syslog port through which it receives the syslog messages
- **syslog relay** - Changes the syslog role from device to relay
- **syslog relay transport type** - Sets the syslog relay transport type either as udp or tcp

12.27 show syslog profile

This command displays the syslog profile.

show syslog profile

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show syslog profile
Syslog Profile : raw

Related Commands

- **syslog profile** - Sets the profile for reliable syslog

ISS

12.28 show syslog relay transport type

This command displays the Syslog relay transport type.

```
show syslog relay transport type
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show syslog relay transport type

```
Syslog Relay Transport type udp
```

- Related Commands**
- **syslog relay transport type** - Sets the Syslog relay transport type either as udp or tcp
 - **syslog relay -port** - Sets the syslog port through which it receives the syslog messages
 - **syslog relay -** Changes the syslog role from device to relay

12.29 show syslog file-name

This command displays all the syslog local storage file names.

show syslog file-name

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show syslog file-name

```
Syslog File Name
-----
Syslog File-One :iss1
Syslog File-Two :iss2
Syslog File-Three :iss3
```

- Related Commands**
- **syslog local storage** - Enables the syslog local storage
 - **show syslog local storage** - Displays the syslog local storage.
 - **syslog filename-one** - Configures the file name to store the syslog messages.
 - **syslog filename-two** - Configures the file name to store the syslog messages.
 - **syslog filename-three** - Configures the file name to store the syslog messages

ISS

12.30 show syslog information

This command displays the status of consolidated syslog log information.

show syslog information

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show syslog information

```
System Log Information
-----
Syslog Localstorage      : Enabled
Syslog Mail Option      : Enabled
Syslog Port              : 251
Syslog Role              : Relay
```

- Related Commands**
- **syslog local storage** - Enables the syslog local storage
 - **syslog mail** – Enables the mail option in syslog
 - **syslog relay** – Changes the syslog role from device to relay

Chapter

13

TCP

Transmission Control Protocol (TCP) is a portable implementation of the industry standard TCP based on RFC 793. The software consists of the core TCP protocol, a library that provides a Socket Layer Interface (SLI) to support both Telnet Server and FTP server. TCP interacts with the Network Layer protocols (IPv4/IPv6) and uses their services for end-to-end communication.

The list of TCP commands is as follows:

- show tcp statistics
- show tcp connections
- show tcp listeners
- show tcp retransmission details

ISS

13.1 show tcp statistics

This command displays the tcp statistics. The information such as Max connections, Active opens, Passive opens, attempts fail are displayed.

show tcp statistics

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show tcp statistics

```
Max Connections : 500
Active Opens : 0
Passive Opens : 0
Attempts Fail : 0
Estab Resets : 0
Current Estab : 0
Input Segments : 0
Output Segments : 0
Retransmitted Segments : 0
Input Errors : 0
TCP Segments with RST flag Set: 0
HC Input Segments : 0
HC Output Segments : 0
```

13.2 show tcp connections

This command displays the tcp connections for the switch. The information such as Local IP Address type, Local IP, Local Port, Remote Port are displayed.

show tcp connections

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show tcp connections

```
TCP Connections
=====
```

```
Local IP Address Type : IPv4
Local IP               : 127.0.0.1
Local Port             : 35040
Remote IP Address Type : IPv4
Remote IP              : 127.0.0.1
Remote Port           : 631
TCP State              : FinWait1
```

```
Local IP Address Type : IPv4
Local IP               : 127.0.0.1
Local Port             : 35041
Remote IP Address Type : IPv4
Remote IP              : 127.0.0.1
Remote Port           : 631
TCP State              : FinWait1
```

```
Local IP Address Type : IPv4
Local IP               : 127.0.0.1
Local Port             : 35042
Remote IP Address Type : IPv4
Remote IP              : 127.0.0.1
Remote Port           : 631
TCP State              : FinWait1
```

```
Local IP Address Type : IPv4
Local IP               : 172.30.4.110
Local Port             : 22
Remote IP Address Type : IPv4
Remote IP              : 10.203.113.47
Remote Port           : 4886
TCP State              : Closed
```

```
Local IP Address Type : IPv4
Local IP               : 172.30.4.110
Local Port             : 22
```

Remote IP Address Type : IPv4
Remote IP : 10.203.113.113
Remote Port : 4391
TCP State : Closed

Local IP Address Type : IPv4
Local IP : 172.30.4.110
Local Port : 32911
Remote IP Address Type : IPv4
Remote IP : 172.31.112.88
Remote Port : 2003
TCP State : Closed

13.3 show tcp listeners

This command displays the tcp listeners in the network. Information such as Local IP Address Type, Local IP and Local Port are displayed for each listener.

show tcp listeners

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show tcp listeners
TCP Listeners
=====
Local IP Address Type : 0
Local IP               : 0.0.0.0
Local Port             : 22

Local IP Address Type : 0
Local IP               : 0.0.0.0
Local Port             : 23

Address Type [0 - IPv4 and IPv6] [1 - IPv4] [2 - IPv6]
```

ISS

13.4 show tcp retransmission details

This command displays the tcp retransmission details.

show tcp retransmission details

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# sh tcp retransmission details

```
RTO Algorithm Used : VAN JACOBSON  
Min Retransmission Timeout : 0 msec  
Max Retransmission Timeout : 0 msec
```

Chapter

14

UDP

Interface Masters UDP (User Datagram Protocol) is a portable implementation of the industry standard UDP. **Interface Masters UDP** is used in packet-switched computer communication networks and in interconnected systems of such networks. The software consists of the core UDP protocol and a library that provides a Socket Layer Interface (similar to BSD sockets) for applications like SNMP. **Interface Masters UDP** supports a number of standard features in addition to the core protocol.

The following are the list of UDP commands:

- show udp statistics
- show udp connections


```
UDP with no Checksum      : 0
No. ICMP error packets   : 0
UDP with wrong Checksum  : 0
UDP In Broadcast Mode    : 0
```

```
iss# show udp statistics vrf vr1
```

```
Global UDP Statistics
```

```
=====
```

```
InDatagrams              : 0
OutDatagrams             : 0
HC InDatagrams           : 0
HC OutDatagrams          : 0
UDP No Ports             : 4
UDP In Errors            : 0
UDP with no Checksum     : 0
No. ICMP error packets   : 0
UDP with wrong Checksum  : 0
UDP In Broadcast Mode    : 0
```

```
Virtual Context - UDP Statistics
```

```
=====
```

```
VRF Name: vr1
```

```
-----
```

```
InDatagrams              : 0
OutDatagrams             : 0
HC InDatagrams           : 0
HC OutDatagrams          : 0
UDP No Ports             : 0
UDP In Errors            : 0
UDP with no Checksum     : 0
No. ICMP error packets   : 0
UDP with wrong Checksum  : 0
UDP In Broadcast Mode    : 0
```

14.2 show udp connections

This command displays the udp configurations such as Local IP Address Type, Local IP, Local Port, Remote IP Address Type, Remote IP and Remote Port for various connections.

show udp connections [vrf <vrf-name>]

Syntax **vrf** - Name of the VRF instance. This value is a string of size 32. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Description

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Default vrf - default

Example iss# show udp connections

```

Global UDP Connections
=====

Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 161
Remote IP Address Type : 0
Remote IP             : 0.0.0.0
Remote Port           : 0

Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 6125
Remote IP Address Type : 0
Remote IP             : 0.0.0.0
Remote Port           : 0

Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 49152
Remote IP Address Type : 0
Remote IP             : 0.0.0.0
Remote Port           : 0

iss# show udp connections vrf vr1

Global UDP Connections
=====

Local IP Address Type : 0
  
```

```
Local IP           : 0.0.0.0
Local Port         : 161
Remote IP Address Type : 0
Remote IP          : 0.0.0.0
Remote Port        : 0
```

```
Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 6125
Remote IP Address Type : 0
Remote IP             : 0.0.0.0
Remote Port           : 0
```

```
Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 49152
Remote IP Address Type : 0
Remote IP             : 0.0.0.0
Remote Port           : 0
```

Virtual Context - UDP Connections

=====

VRF Name: vr1

```
Local IP Address Type : IPv4
Local IP              : 0.0.0.0
Local Port            : 0
Remote IP Address Type : IPv4
Remote IP             : 0.0.0.0
Remote Port           : 0
```

Related Commands `show udp statistics` - Displays the udp statistics

Chapter

15

PoE

Power over Ethernet technology is a system that transmits electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. The advantage of this technology is that the installers need to run only a single Ethernet cable that carries both power and data to each device. IP telephones, wireless LAN access points, webcams, Ethernet hubs, computers, and other appliances use this technology. Access Points and network devices can be easily located, decreasing installation costs in many cases.

Power over Ethernet is standardized in IEEE 802.3af. This technology offers new options to system designers by providing economical and flexible deployment of networked devices.

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

- set poe
- power inline mac-address
- power inline
- power inline priority
- show power detail
- show power inline
- show poe mac-address-list

ISS

15.1 set poe

This command enables/disables Power Over Ethernet module in the switch.

`set poe {enable | disable}`

Syntax	<code>enable</code>	- Enables the Power Over Ethernet module in the switch. which initializes the data structures and gets the power supply status.
Description	<code>disable</code>	- Disables the Power Over Ethernet module and releases all the resources allocated to the POE module to the system and the power is shut off on all POE enabled ports.
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Defaults	<code>disable</code>	
Example	<code>iss(config)# set poe enable</code>	
Related Command	<code>show power detail</code> - Displays Power Over Ethernet power supply status	

15.2 power inline mac-address

This command adds included a MAC address of the powered device for which power is to be applied. The no form of the command deletes MAC Address of the Powered Device from which power is to be removed.

```
power inline mac-address <mac address>
```

```
no power inline mac-address <mac address>
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# power inline mac-address 00:11:22:33:44:55`



- Power Over Ethernet must be enabled in the device.

**Related
Commands**

- `show power inline` - Displays power status for all or the specified Power Over Ethernet interface
- `show poe mac-address-list` - Displays Power Over Ethernet configured MAC list
-

ISS

15.3 power inline

This command enables/disables Power Over Ethernet on the specified port.

```
power inline {auto [ max <milli-watts (1-3600)> ] | never | static [ max <milli-watts (1-3600)> ]}
```

Syntax	auto	- Enables Power Over Ethernet on a port. Automatically allocates power to the PoE port after device detection, if enough power is available.
Description		The maximum wattage feature limits the power allocated on the port. This value ranges between 1 and 3600 milli-watts. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
	never	- Disables Power Over Ethernet on a port and disables power to the port.
	static [max <milli-watts (1-3600)	- Enables powered-device detection. Pre-allocates power for a port before discovering the powered device, thus guaranteeing the availability of power upon device detection. The maximum wattage feature limits the power allocated on the port. This value ranges between 1 and 3600 milli-watts. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults never

Example `iss(config-if)# power inline auto`



- Power Over Ethernet must be enabled in the device.

Related Command `show power inline` - Displays power status for all or the specified Power Over Ethernet interface

15.4 power inline priority

This command sets the priority of the Power Over Ethernet on the specified port.

```
power inline priority { critical | high | low }
```

Syntax Description	critical	- Sets the Power Over Ethernet port priority to critical
	high	- Sets the Power Over Ethernet port priority to high
	low	- Sets the Power Over Ethernet port priority to low

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults low

Example `iss(config-if)# power inline priority high`



- Power Over Ethernet must be enabled in the device.
- POE module is dependent on hardware APIs that are not available currently.
- The power inline command has to be enabled prior to the execution of this command.

Related Command `show power inline` - Displays power status for all or the specified Power Over Ethernet interface

ISS

15.5 show power detail

This command displays the Power Over Ethernet power supply status information such as PoE Global admin state, PSE operational status and Maximum power supply.

show power detail

Mode User/Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show power detail

```
PSE Status
-----
PoE Global Admin State : Enabled
PSE Oper Status       : Off
Max Power Supply      : 2
Total Power in (watts) : 0
Total Power Consumed  : 0
```

Related Command **set poe** - Enables/disables Power Over Ethernet module in the switch

15.6 show power inline

This command displays the power status for all or the specified Power Over Ethernet interface.

```
show power inline [{<interface-type> <interface-id>}]
```

Syntax Description	<interface-type>	<ul style="list-style-type: none"> - Displays the specified type of interface. The interface can be: <ul style="list-style-type: none"> • 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. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	<ul style="list-style-type: none"> - Displays the 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.

Mode User/Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show power inline

```
PoE Port Info
-----
```

```
Port-Index PoeAdminState DetectionStatus powerClass priority
-----
```

ISS

```
1          up          Disabled      class 0    high
2          down        Disabled      class 0    low
3          down        Disabled      class 0    low
```

```
iss# show power inline fastethernet 0/1
```

```
PoE Port Info
```

```
-----
```

```
Port Number      : 1
PoeAdminStatus   : Up
PoeDetectionState : Disabled
class            : 0
Priority          : high
```

**Related
Commands**

- **power inline mac-address** - Adds MAC Address of the Powered Device for which power is to be applied
- **power inline** - Enables/disables Power Over Ethernet on a port
- **power inline priority** - Sets the Power Over Ethernet port priority (critical | high | low)

15.7 show poe mac-address-list

This command displays the Power Over Ethernet configured MAC list information such as port, power consumed and detection state are displayed.

```
show poe mac-address-list
```

Mode User / Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show poe mac-address-list

```
PD Mac Entries
```

```
-----  
PD mac-address      Port    powerConsumed  DetectionState  
-----  
00:11:11:11:11:11   0      Unknown        Unknown  
00:11:22:33:44:55   0      Unknown        Unknown
```

Related Command **power inline mac-address** - Adds MAC Address of the Powered Device for which power is to be applied

Chapter

16

L2 DHCP Snooping

The DHCP snooping feature filters the untrusted DHCP messages and builds a DHCP snooping binding database. It acts as a firewall between untrusted hosts and DHCP servers. These untrusted messages are sent from devices outside a network and are usually sources of traffic attacks. DHCP snooping binding database maintains a table which contains MAC address, IP address, lease time, binding type, VLAN number and interface information of the local untrusted interfaces of the switch.

The list of CLI commands used to configure the L2 DHCP snooping are

- ip dhcp snooping - Global Command
- ip dhcp snooping verify mac-address
- ip dhcp snooping - VLAN Interface Command
- ip dhcp snooping trust
- show ip dhcp snooping globals
- show ip dhcp snooping vlan
- debug ip dhcp snooping

ISS

16.1 ip dhcp snooping - Global Command

This command globally enables the layer 2 DHCP snooping in the switch or enables the snooping in the specific VLAN. The DHCP snooping module will start the protocol operation when the snooping is enabled globally..

The no form of the command globally disables layer 2 DHCP snooping in the switch or disables DHCP snooping in the specific VLAN. The DHCP snooping module will stop the protocol operation when the snooping is globally disabled.

```
ip dhcp snooping [ vlan < vlan-id (1-4094)>]
```

```
no ip dhcp snooping [vlan <integer(1-4094)>]
```

Syntax description	vlan n	- Configures the L2 DHCP snooping feature for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
---------------------------	---------------	---

Mode Global Configuration mode

Package Workgroup, Enterprise and Metro

Defaults DHCP snooping is globally disabled in the switch and on all VLAN's.

Example

```
iss(config)# ip dhcp snooping
iss(config)# ip dhcp snooping vlan 2
```



The example used above and the ip dhcp snooping command used in the config-vlan mode serve the same purpose,

Related Commands

- **show ip dhcp snooping globals** - Displays the global configuration of dhcp snooping
- **show ip dhcp snooping vlan** - Displays the configuration and statistics of the specified VLAN

16.2 ip dhcp snooping verify mac-address

This command globally enables DHCP MAC verification in the switch.

The no form of the command globally disables DHCP MAC verification in the switch.

If the MAC verification status is enabled, DHCP snooping module will verify whether the source Mac address and client hardware Mac address are same. If they are same, packet will be processed further, else, it is dropped.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults DHCP MAC address verification is enabled.

Example `iss(config)# ip dhcp snooping verify mac-address`

Related Commands

- **show ip dhcp snooping globals** - Displays the global configuration of dhcp snooping

ISS

16.3 ip dhcp snooping - VLAN Interface Command

This command enables layer 2 DHCP snooping in the VLAN.

The no form of the command disables layer 2 DHCP snooping in the VLAN.

DHCP snooping feature filters the untrusted DHCP messages to provide security for DHCP servers.

ip dhcp snooping

no ip dhcp snooping

Mode Config-VLAN mode

Package Workgroup, Enterprise and Metro

Defaults L2 DHCP snooping is disabled on VLANs

Example `iss(config-vlan)# ip dhcp snooping`

Related Commands

- **show ip dhcp snooping vlan** - displays the configuration and statistics of the specified VLAN
- **ip dhcp snooping - Global command** - This command enables layer 2 dhcp snooping on a particular VLAN.

16.4 ip dhcp snooping trust

This command configures the port as a trusted port.

The no form of the command configures the port as an untrusted port.

The packets coming from the trusted port is considered as trusted packets and are not filtered by the DHCP snooping feature.

```
ip dhcp snooping trust
```

```
no ip dhcp snooping trust
```

Mode Interface Configuration mode

Package Workgroup, Enterprise and Metro

Defaults Ports are considered as trusted

Example `iss(config-if)# ip dhcp snooping trust`

16.5 show ip dhcp snooping globals

This command displays the global configuration of DHCP snooping. The global status of layer 2 DHCP snooping and MAC verification are displayed.

show ip dhcp snooping globals [**switch <Context Name>**]

Syntax description **switch** - Displays the global configuration of DHCP snooping 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 MI feature.

Mode Privileged EXEC mode

Package Workgroup, Enterprise and Metro

Example iss# show ip dhcp snooping globals

```
DHCP Snooping Global information
-----
```

```
Layer 2 DHCP Snooping is globally disabled
MAC Address verification is enabled
```

- Related Commands**
- **ip dhcp snooping - Global command** - Globally enables the layer 2 DHCP snooping in the switch and allocates the resources for the DHCP snooping module.
 - **ip dhcp snooping verify mac-address** - Globally enables DHCP MAC verification in the switch.

16.6 show ip dhcp snooping vlan

This command displays the DHCP snooping configuration and statistics of all VLANs in which the DHCP snooping feature is enabled.

```
show ip dhcp snooping [vlan <vlan-id (1-4094)>] [switch <context name>]
```

Syntax description	vlan	<ul style="list-style-type: none"> - Displays the DHCP snooping configuration and statistics for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
	switch	<ul style="list-style-type: none"> - Displays the DHCP snooping configuration and statistics 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 MI feature.

Mode Privileged EXEC mode

Package Workgroup, Enterprise and Metro

Example iss# show ip dhcp snooping vlan 3

```
DHCP Snooping Vlan information
-----
VLAN                               : 3
Snooping status                     : Enabled
Number of Incoming Discovers        : 0
Number of Incoming Requests         : 0
Number of Incoming Releases         : 0
Number of Incoming Declines         : 0
Number of Incoming Informs          : 0
Number of Transmitted Offers        : 0
Number of Transmitted Acks          : 0
Number of Transmitted Naks          : 0
Total Number Of Discards            : 0
Number of MAC Discards              : 0
Number of Server Discards           : 0
Number of Option Discards           : 0
```

Related Commands

- **ip dhcp snooping - VLAN interface command** - Enables layer 2 DHCP snooping in the VLAN.

16.7 debug ip dhcp snooping

This command enables the tracing of the DHCP snooping module as per the configured debug level. The trace statements are generated for the configured trace levels.

The no form of the command disables the tracing of the DHCP module. The trace statements are not generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

```
debug ip dhcp snooping {[entry][exit][debug][fail] | all}
```

```
no debug ip dhcp snooping
```

Syntax description	entry	<ul style="list-style-type: none"> - Generates debug statements for function entry traces. - The names of the functions entered are displayed in the log.
	exit	Generates debug statements for function exit traces. The names of the functions exited are displayed in the log.
	debug	Generates debug statements for debug traces. This is used for debugging the packet flow of DHCP snooping functionality.
	fail	Generates debug statements for 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.
	all	- Generates debug statements for all types of traces.

Mode Privileged EXEC mode

Package Workgroup, Enterprise and Metro

Example iss# debug ip dhcp snooping entry

Chapter

17

IPDB

IP source guard is used to restrict the IP traffic on Layer 2 interfaces by filtering traffic based on the IP binding database.

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

- ip binding
- ip source binding
- ip verify source
- show ip binding
- show ip source binding
- show ip binding counters
- show ip verify source
- debug ip binding database

17.1 ip binding

This command configures the static binding information for the hosts connected to the switch.

The no form of the command deletes the binding information for the specified host.

```
ip binding <mac-address> vlan <vlan-id (1-4094)> <ip address> interface
<interface-type> <interface-id> gateway <ip address>
```

```
no ip binding <mac-address> vlan <vlan-id (1-4094)>
```

Syntax	<mac-address>	-	Configures the unicast MAC address of the host for which the binding information should be configured.
Description	<vlan-id (1-4094)>	-	Configures the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
	<ip address>	-	Configures IP address of the host for which the binding information should be configured.
	<interface-type>	-	Configures the type of interface to which the host is connected. The interface can be: <ul style="list-style-type: none"> • 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. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	-	Configures the interface identifier to which the host is connected. 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 internal-lan and port-channel.

For example: 0/1 represents that the slot number is 0 and port number is 1.

Only internal-lan or port-channel ID is provided, for interface types internal-lan and port-channel. For example: 1 represents internal-lan and port-channel ID.

gateway address> **<ip** - Configures the IP address of the gateways to which the host has access.

Mode Global Configuration mode

Package Workgroup, Enterprise and Metro

Example iss(config)# ip binding 00:01:02:03:04:05 vlan 3 30.0.0.4
interface gigabitethernet 0/2 gateway 30.0.0.1

Related Commands

- **show ip binding** - Displays the IP binding database.
- **show ip binding counters** - Displays the global or VLAN statistics information.

17.2 ip source binding

This command adds a static IP source binding entry. The no form of the command deletes the static IP source binding entry.

```
ip source binding <mac-address> vlan <vlan-id (1-4094)> <ip-address> interface
<interface-type> <interface-id> [gateway <gateway-ip>]
```

```
no ip source binding <mac-address> vlan <vlan-id (1-4094)> <ip-address>
interface <interface-type> <interface-id>
```

Syntax	<mac-address>	-	Configures the unicast MAC address of the host for which the binding information should be configured.
Description	<vlan-id (1-4094)>	-	Configures the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
	<ip-address>	-	Configures IP address of the host for which the binding information should be configured.
	<interface-type>	-	Configures the type of interface to which the host is connected. The interface can be: <ul style="list-style-type: none"> • 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. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	-	Configures the interface identifier to which the host is connected. 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 internal-lan and port-channel.

For example: 0/1 represents that the slot number is 0 and port number is 1.

Only internal-lan or port-channel ID is provided, for interface types internal-lan and port-channel. For example: 1 represents internal-lan and port-channel ID.

gateway <gateway-ip> - Configures the gateway IP address of the gateways to which the host has access.

Mode Global Configuration mode

Package Workgroup, Enterprise and Metro

Example
iss(config)# ip source binding 00:01:02:03:04:05 vlan 3
30.0.0.4 interface gigabitethernet 0/2 gateway 30.0.0.1

Related Commands

- **show ip source binding** - Displays the source IP binding database.

ISS

17.3 ip verify source

This command enables the IP source guard status for the specified interface. The no form of the command disables the IP source guard on an interface.

The port-security option is mandatory for this command. Else it will throw the error message “Interface Masters IP source guard feature does not support source IP filter type” .

```
ip verify source [ port-security ]
```

```
no ip verify source [ port-security ]
```

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Disable

Example iss(config-if)# ip verify source port-security

Related Commands

- **show ip verify source** - Displays the IP source guard interface status.

17.4 show ip binding

This command displays the IP binding database.

```
show ip binding [vlan <vlan-id (1-4094)>] {[ static | dhcp | ppp ]} [switch
<switch_name>]
```

Syntax Description	vlan <vlan-id (1-4094)> - Displays the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094. static - Displays the static ip binding configuration. dhcp - Displays the dynamic IP binding updates through DHCP snooping. ppp - Displays the dynamic IP binding updates through Pppoe intermediate agent. switch <switch_name> - Displays the database of the specified switch.
---------------------------	---

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ip binding vlan 2 static

```

Host Binding Information
-----
VLAN  HostMac           HostIP  Port  GatewayIP  Type
-----
2     00:10:12:13:13:15  12.0.0.1  Gi0/1  12.0.0.0  static
```

Related Commands

- **ip binding** – Configures the static binding information for the hosts connected to the switch.

17.5 show ip source binding

This command displays the source IP binding database.

```
show ip source binding [<ip-address>] [<mac-address>] [{ dhcp-snooping |
static }] [ interface <interface-type> <interface-id> ] [ vlan <vlan-id (1-
4094)> ] [switch <switch_name>]
```

Syntax Description	<ip-address>	-	Displays the IP address of the host for which the binding information should be configured.
	<mac-address>	-	Displays the unicast MAC address of the host for which the binding information should be configured.
	dhcp-snooping	-	Displays the dynamic IP binding updation through DHCP snooping.
	static	-	Displays the static ip binding configuration.
	<interface-type>	-	<p>Displays the type of interface to which the host is connected. The interface can be:</p> <ul style="list-style-type: none"> • 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. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	-	<p>Displays the interface identifier to which the host is connected. 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 internal-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 internal-lan or port-channel ID is provided, for interface types internal-lan and port-channel. For</p>

example: 1 represents internal-lan and port-channel ID.

vlan <vlan-id (1-4094)> - Displays the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.

switch <switch_name> - Displays the status of the ip source binding of the specified switch.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ip source binding

```

Host Binding Information
-----
VLAN      HostMac      HostIP      Port      GatewayIP      Type
-----
```

Related Commands

- **ip source binding** - Adds a static IP source binding entry

17.6 show ip binding counters

This command displays the global or VLAN statistics information.

```
show ip binding counters [{"vlan <short (1-4094)>"} | global | [ switch
<switch-name>"] ]]
```

Syntax	<code>vlan <short (1-</code>	-	Displays the VLAN ID to which the host belongs.
Description	<code>4094)></code>		This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
	<code>global</code>	-	Displays the static information of all binding types (static, dhcp, ppp)
	<code>switch <switch-name</code>	-	Displays the static information of the specified VLAN.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ip binding counters vlan 2

```
Global Binding count Information
```

```
-----
Number of Bindings           : 1
Number of Static Bindings    : 1
Number of DHCP Bindings     : 0
Number of PPP Bindings      : 0
```

Related Commands

- **ip binding** - Configures the static binding information for the hosts connected to the switch.

17.7 show ip verify source

This command displays the IP source guard interface status.

```
show ip verify source [ interface <interface-type> <interface-id> ]
```

Syntax	<interface-type>	Displays the type of interface to which the host is connected. The interface can be:
Description		<ul style="list-style-type: none"> • 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. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.

<interface-id>	Configures the interface identifier to which the host is connected. 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 internal-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only internal-lan or port-channel ID is provided, for interface types internal-lan and port-channel. For example: 1 represents internal-lan and port-channel ID.
-----------------------------	--

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show ip verify source
Interface          IP Source guard Status
-----
Gi0/1              Disable
Gi0/2              Disable
```

ISS

Gi0/3	Disable
Gi0/4	Disable
Gi0/5	Disable
Gi0/6	Disable
Gi0/7	Disable
Gi0/8	Disable
Gi0/9	Disable
Gi0/10	Disable
Gi0/11	Disable
Gi0/12	Disable
Gi0/13	Disable
Gi0/14	Disable
Gi0/15	Disable
Gi0/16	Disable
Gi0/17	Disable
Gi0/18	Disable
Gi0/19	Disable
Gi0/20	Disable
Gi0/21	Disable
Gi0/22	Disable
Gi0/23	Disable
Gi0/24	Disable

**Related
Commands**

- **ip verify source** - Enables the IP source guard status for the specified interface

17.8 debug ip binding database

This command specifies the debug levels for IP Binding Database module. The no form of this command disables IPDB module debugging.

```
debug ip binding database {[entry][exit][debug][fail] | all}
```

```
no debug ip binding database [{ [entry][exit][debug][fail] | all }]
```

Syntax Description	entry	- Generates debug statements for all function entry traces.
	exit	- Generates debug statements for all function exit traces.
	debug	- Generates debug statements for all debug traces.
	fail	- Generates debug statements for all the failure traces.
	all	- Generates debug statements for all the above mentioned traces.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss# debug ip binding database entry	

Feature not supported - This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.