



## Switch CLI Reference Guide for

**SSE-X3348S**  
**SSE-X3348SR**  
**SSE-X3348T**  
**SSE-X3348TR**

# Supermicro Intelligent Switch Command Line Interface User Guide

---

Supermicro Intelligent Switch

Release: 1.1i

Document: SM-CLI-Guide-1-2a3.Doc

Document status: Standard

Document release date: 1/10/2020

Copyright © 2020 Supermicro

All Rights Reserved.

This document is protected by copyright laws and international treaties. All information, copyrights and any other intellectual property rights contained in this document are the property of Supermicro. Except as expressly authorized in writing by Supermicro, the holder is granted no rights to use the information contained herein and this document shall not be published, copied, produced or reproduced, modified, translated, compiled, distributed, displayed or transmitted, in whole or part, in any form or media.

## Contents

1	Introduction.....	22
1.1	Purpose.....	22
1.2	Scope.....	22
1.3	Document Conventions.....	23
1.4	Key Conventions.....	23
1.4.1	Keyboard shortcuts.....	23
1.4.2	Others.....	23
2	Command Line Interface.....	24
2.1	CLI Command Modes.....	24
2.2	User EXEC Mode.....	26
2.3	Privileged EXEC Mode.....	26
2.4	Global Configuration Mode.....	26
2.5	Interface Configuration Mode.....	26
2.5.1	Physical Interface Mode.....	26
2.5.2	Port Channel Interface Mode.....	26
2.5.3	VLAN Interface Mode.....	26
2.6	Config-VLAN Mode.....	26
2.7	Line Configuration Mode.....	26
2.8	Slave Configuration.....	27
2.9	Config-CEE-Map Mode.....	27
2.10	Protocol Specific Modes.....	27
2.10.1	MSTP Configuration mode.....	27
2.10.2	DiffSrv ClassMap Configuration mode.....	27
2.10.3	DiffSrv Policy-Map Configuration Mode.....	27
2.10.4	DiffSrv Policy-Map Class Configuration Mode.....	28
2.10.5	DHCP Pool Configuration Mode.....	28
2.10.6	ACL Standard Access List Configuration Mode.....	28
2.10.7	ACL Extended Access List Configuration Mode.....	28
2.10.8	ACL MAC Configuration Mode.....	29
2.11	Command Privileges.....	29
3	System Features.....	30
3.1	ip address dhcp.....	38
3.2	ip address.....	39
3.3	ip gateway.....	40
3.4	login authentication.....	41
3.5	username.....	42
3.6	listuser.....	43
3.7	show users.....	44
3.8	show privilege.....	45
3.9	enable password.....	46
3.10	enable.....	47
3.11	disable.....	48
3.12	logout.....	49

3.13	lock .....	50
3.14	ip http port .....	51
3.15	set ip http .....	52
3.16	web session-timeout .....	53
3.17	show http server status.....	54
3.18	authorized-manager ip-source .....	55
3.19	show authorized-managers .....	56
3.20	debug nm .....	57
3.21	configure terminal.....	58
3.22	exit .....	59
3.23	end .....	60
3.24	show running-config.....	61
3.25	alias .....	63
3.26	help .....	64
3.27	show history.....	65
3.28	clear screen .....	66
3.29	exec-timeout .....	67
3.30	run script.....	68
3.31	show aliases .....	69
3.32	show line.....	70
3.33	line .....	71
3.34	cli pagination .....	72
3.35	firmware upgrade.....	73
3.36	ntp key .....	74
3.37	ntp broadcast.....	75
3.38	ntp server .....	76
3.39	ntp enable.....	77
3.40	ntp disable.....	78
3.41	tz offset .....	79
3.42	show ntp.....	80
3.43	clock set .....	81
3.44	show clock .....	82
3.45	rtc sync.....	83
3.46	write .....	84
3.47	set startup-config .....	85
3.48	copy .....	86
3.49	copy mtdoops.....	87
3.50	copy startup-config.....	88
3.51	copy-file.....	89
3.52	erase .....	90
3.53	list files.....	91
3.54	show file .....	92
3.55	show startup-config .....	93
3.56	show stored-config .....	94
3.57	interface .....	95

---

3.58	interface range .....	96
3.59	description .....	97
3.60	switchport .....	98
3.61	ip address .....	99
3.62	ip address dynamic .....	100
3.63	mtu frame size .....	101
3.64	system mtu frame size .....	102
3.65	flowcontrol.....	103
3.66	pfc .....	104
3.67	shutdown - physical/VLAN/port-channel Interface .....	105
3.68	negotiation .....	106
3.69	capabilities .....	107
3.70	speed .....	108
3.71	duplex .....	109
3.72	Energy Efficient Ethernet (SSE-X3348T/R only) .....	110
3.73	monitor session .....	112
3.74	hol blocking prevention .....	113
3.75	storm-control .....	114
3.76	rate-limit .....	115
3.77	snmp trap link-status.....	116
3.78	reset interface statistics .....	117
3.79	reset interface cpu statistics .....	118
3.80	single-blade-slot-num .....	119
3.81	split40g .....	120
3.82	show single-blade-slot-num.....	121
3.83	show split40g.....	122
	show ip interface .....	123
3.84	show interfaces .....	124
3.85	show interfaces - counters .....	127
3.86	show interfaces loopback.....	128
3.87	show interfaces cpu counters .....	129
3.88	show interface mtu.....	130
3.89	show conf.....	131
3.90	show port-monitoring .....	132
3.91	show flow-control.....	133
3.92	show transceiver .....	134
3.93	show transceiver diagnostics .....	135
3.94	show meminfo .....	136
3.95	device name .....	137
3.96	system location .....	138
3.97	system contact.....	139
3.98	set boot-up .....	140
3.99	reload .....	141
3.100	reset-to-factory-defaults.....	142
3.101	mac-address-table aging-time.....	143

---

3.102	copy debug-logging .....	144
3.103	debug-logging .....	145
3.104	no startup-config .....	146
3.105	show system information .....	147
3.106	show version .....	148
3.107	show debug-logging .....	149
3.108	show debugging .....	150
3.109	show system acknowledgement .....	151
3.110	show system environment .....	152
3.111	show tech-support .....	153
4	Stacking .....	154
4.1	Stack .....	159
4.2	Show stack brief .....	160
4.3	Show stack details .....	161
4.4	Show stack counters .....	162
4.5	Show stack switchid .....	163
4.6	Show stack link status .....	164
5	Syslog .....	165
5.1	logging enable .....	167
5.2	logging disable .....	168
5.3	logging ip .....	169
5.4	logging buffered .....	170
5.5	logging console .....	171
5.6	logging facility .....	172
5.7	logging trap .....	173
5.8	logging file .....	174
5.9	cmdbuffs .....	175
5.10	service timestamps .....	176
5.11	clear log buffer .....	177
5.12	clear log file .....	178
5.13	show logging .....	179
5.14	show logging file .....	180
6	SSH .....	181
6.1	ip ssh .....	182
6.2	debug ssh .....	183
6.3	show ip ssh .....	184
7	SSL .....	185
7.1	ip http secure .....	186
7.2	ssl gen cert-req algo rsa sn .....	187
7.3	ssl server-cert .....	188
7.4	debug ssl .....	189
7.5	show ssl server-cert .....	190
7.6	show ip http secure server status .....	192
8	RMON .....	193
8.1	set rmon .....	194

---

8.2	rmon event.....	195
8.3	rmon alarm .....	196
8.4	rmon collection history.....	198
8.5	rmon collection stats.....	199
8.6	show rmon .....	200
9	STP.....	204
9.1	spanning-tree mode .....	206
9.2	spanning-tree .....	207
9.3	spanning-tree compatibility.....	208
9.4	spanning-tree timers .....	209
9.5	spanning-tree transmit hold-count.....	211
9.6	spanning-tree mst max-hops.....	212
9.7	spanning-tree priority .....	213
9.8	spanning-tree pathcost method.....	214
9.9	spanning-tree mst configuration.....	215
9.10	name.....	216
9.11	revision .....	217
9.12	instance .....	218
9.13	spanning-tree auto-edge.....	219
9.14	spanning-tree - Properties of an interface.....	220
9.15	spanning-tree restricted-role .....	222
9.16	spanning-tree restricted-tcn .....	223
9.17	spanning-tree mst- Properties of an interface for MSTP .....	224
9.18	spanning-tree mst hello-time .....	226
9.19	clear spanning-tree counters .....	227
9.20	spanning-tree pathcost dynamic .....	228
9.21	clear spanning-tree detected protocols .....	229
9.22	debug spanning-tree.....	230
9.23	show spanning-tree - Summary, Blockedports, Pathcost .....	232
9.24	show spanning-tree - Detail.....	236
9.25	show spanning-tree - Active .....	239
9.26	show spanning-tree interface .....	241
9.27	show spanning-tree root.....	245
9.28	show spanning-tree bridge.....	248
9.29	show spanning-tree mst - CIST or specified mst Instance .....	251
9.30	show spanning-tree mst configuration.....	253
9.31	show spanning-tree mst - Port Specific Configuration.....	255
10	PNAC.....	257
10.1	dot1x system-auth-control .....	258
10.2	aaa authentication dot1x default .....	259
10.3	dot1x local-database .....	260
10.4	set nas-id.....	262
10.5	dot1x default .....	263
10.6	dot1x max-req.....	264
10.7	dot1x max-start.....	265

10.8	dot1x reauthentication .....	266
10.9	dot1x timeout.....	267
10.10	dot1x port-control.....	269
10.11	dot1x access-control .....	270
10.12	dot1x control-direction .....	271
10.13	dot1x re-authenticate .....	272
10.14	shutdown dot1x.....	273
10.15	debug dot1x .....	274
10.16	show dot1x.....	275
11	RADIUS.....	280
11.1	radius-server host.....	281
11.2	debug radius.....	282
11.3	show radius server .....	283
11.4	show radius statistics .....	284
12	TACACS.....	285
12.1	tacacs-server host.....	286
12.2	tacacs use-server address .....	287
12.3	tacacs-server retransmit .....	288
12.4	aaa authentication tacacs .....	289
12.5	aaa authorization group tacacs.....	290
12.6	debug tacacs.....	291
12.7	show tacacs .....	292
13	Link Aggregation (LA).....	294
13.1	set port-channel.....	295
13.2	lacp system-priority .....	296
13.3	port-channel load-balance.....	297
13.4	lacp port-priority.....	299
13.5	channel-group .....	300
13.6	lacp wait-time .....	301
13.7	lacp allow-zero-partner-key.....	302
13.8	lacp timeout .....	303
13.9	show etherchannel .....	304
13.10	show interfaces .....	309
13.11	show lacp .....	312
13.12	debug la.....	314
14	IGMP Snooping .....	315
14.1	ip igmp snooping .....	317
14.2	ip igmp snooping proxy-reporting.....	318
14.3	snooping multicast-forwarding-mode.....	319
14.4	ip igmp snooping mrouter-time-out.....	320
14.5	ip igmp snooping port-purge-interval.....	321
14.6	ip igmp snooping report-suppression interval .....	322
14.7	ip igmp snooping retry-count .....	323
14.8	ip igmp snooping group-query-interval.....	324
14.9	ip igmp snooping report-forward.....	325



---

14.10	ip igmp snooping version .....	326
14.11	ip igmp snooping fast-leave.....	327
14.12	ip igmp snooping querier .....	328
14.13	ip igmp snooping query-interval.....	329
14.14	ip igmp snooping mrouter.....	330
14.15	ip igmp snooping send-query .....	331
14.16	ip igmp snooping clear counters.....	332
14.17	shutdown snooping.....	333
14.18	debug ip igmp snooping .....	334
14.19	show ip igmp snooping mrouter .....	335
14.20	show ip igmp snooping globals .....	336
14.21	show ip igmp snooping.....	339
14.22	show ip igmp snooping groups.....	341
14.23	show ip igmp snooping forwarding-database.....	344
14.24	show ip igmp snooping statistics .....	346
15	VLAN .....	350
15.1	vlan .....	352
15.2	protocol-vlan.....	353
15.3	map protocol.....	354
15.4	set gvrp .....	355
15.5	set port gvrp .....	356
15.6	set gmrp .....	357
15.7	set port gmrp.....	358
15.8	mac-vlan .....	359
15.9	mac-address-table static unicast .....	360
15.10	mac-address-table static multicast.....	362
15.11	mac-address-table aging-time.....	364
15.12	wildcard mac-address .....	365
15.13	ports .....	366
15.14	name.....	367
15.15	switchport pvid .....	368
15.16	switchport access vlan .....	369
15.17	Switchport trunk native vlan.....	370
15.18	switchport trunk allowed vlan .....	371
15.19	switchport acceptable-frame-type.....	372
15.20	switchport ingress-filter .....	373
15.21	port protocol-vlan .....	374
15.22	switchport map protocols-group.....	375
15.23	switchport priority default .....	376
15.24	switchport mode .....	377
15.25	switchport protected .....	378
15.26	set garp timer .....	379
15.27	vlan restricted .....	380
15.28	group restricted .....	381
15.29	vlan map-priority .....	382

---

15.30	shutdown garp.....	383
15.31	debug vlan.....	384
15.32	debug garp .....	385
15.33	show vlan.....	386
15.34	show vlan device info .....	389
15.35	show vlan device capabilities .....	392
15.36	show vlan traffic-classes.....	394
15.37	show garp timer .....	395
15.38	show vlan port config .....	397
15.39	show vlan protocols-group .....	399
15.40	show switchport protected.....	401
15.41	show protocol-vlan .....	402
15.42	show mac-vlan.....	403
15.43	show mac-address-table.....	404
15.44	show mac-address-table count.....	406
15.45	show mac-address-table static unicast.....	408
15.46	show mac-address-table static multicast.....	410
15.47	show mac-address-table dynamic unicast.....	412
15.48	show mac-address-table dynamic multicast .....	414
15.49	show mac-address-table aging-time .....	416
15.50	show wildcard.....	417
16	DHCP.....	418
16.1	DHCP Client.....	421
16.1.1	release .....	421
16.1.2	renew.....	423
16.1.3	debug ip dhcp client .....	424
16.1.4	show ip dhcp client stats .....	425
16.2	DHCP Relay .....	426
16.2.1	service dhcp-relay .....	426
16.2.2	ip dhcp server .....	427
16.2.3	ip dhcp relay information.....	428
16.2.4	ip dhcp relay circuit-id .....	429
16.2.5	ip dhcp relay remote-id .....	430
16.2.6	debug ip dhcp relay .....	431
16.2.7	show ip dhcp relay information .....	432
16.2.8	show dhcp server.....	433
16.3	DHCP Server .....	434
16.3.1	service dhcp-server .....	434
16.3.2	ip dhcp pool.....	435
16.3.3	ip dhcp next-server.....	437
16.3.4	ip dhcp bootfile .....	438
16.3.5	ip dhcp.....	439
16.3.6	ip dhcp option .....	440
16.3.7	network .....	442
16.3.8	excluded-address.....	443

---

16.3.9	domain-name.....	444
16.3.10	dns-server .....	445
16.3.11	netbios-name-server .....	446
16.3.12	netbios-node-type .....	447
16.3.13	default-router .....	448
16.3.14	option.....	449
16.3.15	lease.....	451
16.3.16	utilization threshold.....	452
16.3.17	host hardware-type .....	453
16.3.18	host hardware-type mac binding .....	454
16.3.19	interface ip binding.....	455
16.3.20	debug ip dhcp server .....	456
16.3.21	show ip dhcp server information.....	457
16.3.22	show ip dhcp server pools .....	458
16.3.23	show ip dhcp server binding.....	459
16.3.24	show ip dhcp server statistics .....	460
17	SNMPv3.....	461
17.1	snmp community index .....	463
17.2	snmp group .....	465
17.3	snmp access .....	466
17.4	snmp engineid.....	468
17.5	snmp view.....	469
17.6	snmp targetaddr .....	471
17.7	snmp targetparams .....	473
17.8	snmp user.....	475
17.9	snmp notify .....	476
17.10	snmp-server enable traps snmp authentication.....	477
17.11	snmp-server trap udp-port .....	478
17.12	enable snmpagent .....	479
17.13	disable snmpagent.....	480
17.14	enable snmpsubagent.....	481
17.15	disable snmpsubagent.....	482
17.16	show snmp agentx information.....	483
17.17	show snmp agentx statistics.....	484
17.18	show snmp .....	486
17.19	show snmp community.....	487
17.20	show snmp group.....	488
17.21	show snmp group access.....	490
17.22	show snmp engineID .....	492
17.23	show snmp viewtree .....	493
17.24	show snmp targetaddr.....	494
17.25	show snmp targetparam .....	495
17.26	show snmp user .....	496
17.27	show snmp notif.....	497
17.28	show snmp inform statistics .....	498

---

17.29	show snmp-server traps .....	499
17.30	debug ip snmp.....	500
18	IP.....	501
18.1	show ip information.....	502
18.2	ping .....	503
18.3	ip route.....	504
18.4	ip routing.....	506
18.6	ip default-ttl .....	507
18.7	arp timeout.....	508
18.8	arp – ip address .....	509
18.9	ip arp max-retries.....	510
18.10	show ip traffic.....	511
18.11	show ip route .....	512
18.12	show ip arp.....	514
19	IGMP.....	516
19.1	set ip igmp .....	517
19.2	set ip igmp .....	518
19.3	ip igmp immediate-leave .....	519
19.4	ip igmp version .....	520
19.5	ip igmp query-interval .....	521
19.6	ip igmp query-max-response-time.....	522
19.7	ip igmp robustness.....	523
19.8	ip igmp last-member-query-interval.....	524
19.9	ip igmp static-group.....	525
19.10	no ip igmp interface.....	526
19.11	debug ip igmp .....	527
19.12	show ip igmp global-config.....	528
19.13	show ip igmp interface .....	529
19.14	show ip igmp groups.....	531
19.15	show ip igmp sources .....	532
19.16	show ip igmp statistics.....	533
20	RRD .....	535
20.1	as-num .....	536
20.2	router-id .....	537
20.3	export ospf .....	538
20.4	redistribute-policy.....	539
20.5	default redistribute-policy.....	541
20.6	show ip protocols.....	542
20.7	show redistribute-policy .....	544
20.8	show redistribute information.....	545
21	DVMRP .....	546
21.1	set ip dvmrp .....	547
21.2	ip dvmrp prune-life-time .....	548
21.3	set ip dvmrp - interface.....	549
21.4	debug ip dvmrp.....	550

---

21.5	show ip dvmrp .....	552
22	PIM .....	554
22.1	set ip pim .....	556
22.2	set ip pim threshold.....	557
22.3	set ip pim spt-switchperiod.....	558
22.4	set ip pim rp-threshold.....	559
22.5	set ip pim rp-switchperiod .....	560
22.6	set ip pim regstop-ratelimit-period .....	561
22.7	set ip pim pmbr .....	562
22.8	ip pim component .....	563
22.9	set ip pim static-rp .....	564
22.10	set mode.....	565
22.11	rp-candidate rp-address.....	566
22.12	rp-candidate holdtime .....	567
22.13	rp-static rp-address .....	568
22.14	ip pim query-interval .....	569
22.15	ip pim message-interval.....	570
22.16	ip pim bsr-candidate .....	571
22.17	ip pim componentId.....	572
22.18	ip pim hello-holdtime .....	573
22.19	ip pim dr-priority .....	574
22.20	ip pim override-interval .....	575
22.21	ip pim lan-delay .....	576
22.22	set ip pim lan-prune-delay .....	577
22.23	no ip pim interface.....	578
22.24	debug ip pim .....	579
22.25	show ip pim interface .....	581
22.26	show ip pim neighbor .....	584
22.27	show ip pim rp-candidate .....	586
22.28	show ip pim rp-set .....	587
22.29	show ip pim bsr.....	588
22.30	show ip pim rp-static .....	589
22.31	show ip pim component.....	590
22.32	show ip pim thresholds .....	591
22.33	show ip pim mroute .....	592
23	PIMv6 .....	594
23.1	set ipv6 pim .....	596
23.2	set ip pim threshold.....	597
23.3	set ip pim spt-switchperiod.....	598
23.4	set ip pim rp-threshold.....	599
23.5	set ip pim rp-switchperiod .....	600
23.6	set ip pim regstop-ratelimit-period .....	601
23.7	set ip pim pmbr .....	602
23.8	set ip pim static-rp .....	603
23.9	ip pim component .....	604

---

23.10	ipv6 pim rp-candidate rp-address .....	605
23.11	ipv6 pim rp-static rp-address .....	606
23.12	ipv6 pim query-interval .....	607
23.13	ipv6 pim message-interval.....	608
23.14	ipv6 pim bsr-candidate .....	609
23.15	ipv6 pim componentId.....	610
23.16	ipv6 pim hello-holdtime .....	611
23.17	ipv6 pim dr-priority .....	612
23.18	ipv6 pim override-interval .....	613
23.19	ipv6 pim lan-delay .....	614
23.20	set ipv6 pim lan-prune-delay .....	615
23.21	no ipv6 pim interface .....	616
23.22	debug ipv6 pim .....	617
23.23	show ipv6 pim interface .....	619
23.24	show ipv6 pim neighbor .....	621
23.25	show ipv6 pim rp-candidate .....	623
23.26	show ipv6 pim rp-set .....	624
23.27	show ipv6 pim bsr.....	625
23.28	show ipv6 pim rp-static .....	626
23.29	show ipv6 pim component.....	627
23.30	show ipv6 pim thresholds .....	628
23.31	show ipv6 pim mroute .....	629
24	VRRP .....	631
24.1	router vrrp .....	632
24.2	interface vlan .....	633
24.3	vrrp - ip address .....	634
24.4	vrrp - priority .....	635
24.5	vrrp - preempt .....	636
24.6	vrrp - text-authentication .....	637
24.7	vrrp - interval .....	638
24.8	show vrrp .....	639
24.9	show vrrp interface .....	641
24.10	debug vrrp.....	644
25	RIP .....	645
25.1	router rip .....	647
25.2	ip rip security .....	648
25.3	ip rip retransmission .....	649
25.4	network .....	650
25.5	neighbor .....	651
25.6	passive-interface vlan .....	652
25.7	output-delay .....	653
25.8	redistribute .....	654
25.9	default-metric.....	655
25.10	route-tag.....	656
25.11	auto-summary .....	657

---

25.12	ip rip default route originate .....	658
25.13	ip rip summary-address .....	659
25.14	ip rip default route install.....	660
25.15	ip rip send version.....	661
25.16	ip rip receive version .....	662
25.17	ip rip authentication mode .....	663
25.18	timers basic .....	664
25.19	ip split-horizon.....	665
25.20	debug ip rip.....	666
25.21	show ip rip .....	667
26	OSPF.....	669
26.1	router ospf.....	672
26.2	router-id .....	673
26.3	area - Stability interval .....	674
26.4	area - translation-role.....	675
26.5	compatible rfc1583 .....	676
26.6	abr-type.....	677
26.7	neighbor .....	678
26.8	area-default cost.....	679
26.9	area- nssa .....	681
26.10	area-stub.....	683
26.11	default-information originate always.....	684
26.12	area - virtual-link .....	686
26.13	ASBR Router.....	688
26.14	area - range .....	689
26.15	summary-address .....	691
26.16	redistribute .....	693
26.17	redist-config.....	694
26.18	network .....	696
26.19	set nssa asbr-default-route translator .....	697
26.20	passive-interface vlan .....	698
26.21	passive-interface default.....	699
26.22	ip ospf demand-circuit .....	700
26.23	ip ospf retransmit-interval .....	701
26.24	ip ospf transmit-delay .....	702
26.25	ip ospf priority .....	703
26.26	ip ospf hello-interval.....	704
26.27	ip ospf dead-interval .....	705
26.28	ip ospf cost.....	706
26.29	ip ospf network .....	707
26.30	ip ospf authentication-key .....	708
26.31	ip ospf authentication.....	709
26.32	ip ospf message-digest-key.....	711
26.33	debug ip ospf .....	712
26.34	show ip ospf interface.....	714

---

26.35	show ip ospf neighbor.....	716
26.36	show ip ospf request-list.....	717
26.37	show ip ospf retransmission-list.....	718
26.38	show ip ospf virtual-links.....	719
26.39	show ip ospf border-routers.....	720
26.40	show ip ospf - summary address.....	721
26.41	show ip ospf info.....	722
26.42	show ip ospf route.....	723
26.43	show ip ospf - database summary.....	724
26.44	show ip ospf - database.....	727
27	BGP.....	729
27.1	router bgp.....	732
27.2	ip bgp dampening.....	735
27.3	ip bgp overlap-policy.....	737
27.4	ip bgp synchronization.....	738
27.5	clear ip bgp - Flap-Statistics.....	739
27.6	bgp router-id.....	740
27.7	bgp default local-preference.....	741
27.8	neighbor - remote-as.....	742
27.9	neighbor - ebgp-multihop.....	743
27.10	neighbor - next-hop-self.....	744
27.11	neighbor - interval.....	745
27.12	neighbor - timers.....	746
27.13	neighbor - shutdown.....	747
27.14	neighbor - send-community.....	748
27.15	bgp nonbgproute-advt.....	749
27.16	redistribute.....	750
27.17	bgp always-compare-med.....	751
27.18	default-metric.....	752
27.19	bgp med.....	753
27.20	bgp local-preference.....	755
27.21	bgp update-filter.....	757
27.22	aggregate-address index.....	759
27.23	bgp cluster-id.....	760
27.24	bgp client-to-client reflection.....	761
27.25	neighbor - route-reflector-client.....	762
27.26	bgp comm-route.....	763
27.27	bgp comm-peer.....	764
27.28	bgp comm-filter.....	765
27.29	bgp comm-policy.....	766
27.30	bgp ecomm-route.....	767
27.31	bgp ecomm-peer.....	769
27.32	bgp ecomm-filter.....	770
27.33	bgp ecomm-policy.....	771
27.34	bgp confederation identifier.....	772



27.35	bgp confederation peers.....	773
27.36	bgp bestpath med confed .....	774
27.37	neighbor - password.....	775
27.38	clear ip bgp .....	776
27.39	shutdown ip bgp.....	777
27.40	debug ip bgp .....	778
27.41	show bgp-version.....	779
27.42	show ip bgp.....	780
27.43	show ip bgp community - routes .....	782
27.44	show ip bgp extcommunity - routes .....	784
27.45	show ip bgp summary.....	786
27.46	show ip bgp filters .....	787
27.47	show ip bgp aggregate .....	788
27.48	show ip bgp med.....	789
27.49	show ip bgp dampening.....	790
27.50	show ip bgp local-pref .....	791
27.51	show ip bgp timers.....	792
27.52	show ip bgp info .....	793
27.53	show ip bgp rfl info .....	795
27.54	show ip bgp confed info .....	796
27.55	show ip bgp community .....	797
27.56	show ip bgp extcommunity.....	799
27.57	show ip bgp dampened-paths .....	801
27.58	show ip bgp flap-statistics .....	802
28	IPv6.....	803
28.1	ipv6 enable.....	805
28.2	ipv6 unicast-routing.....	806
28.3	ipv6 - address.....	807
28.4	ipv6 - link local address.....	808
28.5	ipv6 - static routes.....	809
28.6	ipv6 - neighbor.....	810
28.7	ipv6 nd suppress-ra.....	811
28.8	ipv6 nd managed-config flag .....	812
28.9	ipv6 nd other-config flag .....	813
28.10	ipv6 hop-limit .....	814
28.11	ipv6 nd ra-lifetime .....	815
28.12	ipv6 nd dad attempts.....	816
28.13	ipv6 nd reachable-time .....	817
28.14	ipv6 nd retrans-time.....	818
28.15	ipv6 nd ra-interval .....	819
28.16	ipv6 nd prefix.....	820
28.17	ping ipv6.....	822
28.18	debug ipv6 .....	823
28.19	traceroute .....	824
28.20	clear ipv6 neighbors.....	825

---

28.21	clear ipv6 traffic.....	826
28.22	clear ipv6 route .....	827
28.23	show ipv6 interface.....	828
28.24	show ipv6 route .....	830
28.25	show ipv6 route summary.....	831
28.26	show ipv6 neighbors .....	832
28.27	show ipv6 traffic .....	833
29	RRD6 .....	835
29.1	export ospfv3 .....	836
29.2	redistribute-policy.....	837
29.3	default redistribute-policy.....	839
29.4	throt.....	840
29.5	show redistribute-policy ipv6 .....	841
29.6	show redistribute information ipv6.....	842
30	RIPv6 .....	843
30.1	ipv6 router rip .....	844
30.2	ipv6 split-horizon.....	845
30.3	ipv6 rip enable .....	846
30.4	ipv6 poison reverse.....	847
30.5	ipv6 rip default-information originate .....	848
30.6	ipv6 rip metric-offset .....	849
30.7	redistribute .....	850
30.8	distribute prefix.....	851
30.9	debug ipv6 rip.....	852
30.10	show ipv6 rip database .....	853
30.11	show ipv6 rip stats .....	854
30.12	show ipv6 rip filter .....	855
31	OSPFv3 .....	856
31.1	ipv6 router ospf.....	859
31.2	router-id .....	860
31.3	area - stub/nssa.....	861
31.4	area - stability-interval.....	862
31.5	area - translation-role.....	863
31.6	timers spf .....	864
31.7	abr-type .....	865
31.8	area - default-metric value .....	866
31.9	area - default-metric type.....	867
31.10	area - virtual-link .....	868
31.11	ASBR Router .....	870
31.12	area - range .....	871
31.13	area - external summary address .....	873
31.14	redistribute .....	875
31.15	passive-interface .....	876
31.16	host - metric/area-id.....	877
31.17	no area.....	878

---

31.18	nssaAsbrDfRtTrans .....	880
31.19	redist-config.....	881
31.20	as-external lsdb-limit .....	882
31.21	exit-overflow-interval .....	883
31.22	demand-extensions .....	884
31.23	reference-bandwidth .....	885
31.24	ipv6 ospf area.....	886
31.25	ipv6 ospf demand-circuit .....	887
31.26	ipv6 ospf retransmit-interval .....	888
31.27	ipv6 ospf transmit-delay .....	889
31.28	ipv6 ospf priority .....	890
31.29	ipv6 ospf hello-interval.....	891
31.30	ipv6 ospf dead-interval .....	892
31.31	ipv6 ospf poll-interval .....	893
31.32	ipv6 ospf metric .....	894
31.33	ipv6 ospf network .....	895
31.34	ipv6 ospf neighbor .....	896
31.35	ipv6 ospf passive-interface .....	897
31.36	ipv6 ospf neighbor probing.....	898
31.37	ipv6 ospf neighbor-probe retransmit-limit .....	899
31.38	ipv6 ospf neighbor-probe interval .....	900
31.39	debug ipv6 ospf .....	901
31.40	show ipv6 ospf interface.....	903
31.41	show ipv6 ospf neighbor.....	905
31.42	show ipv6 ospf - request/retrans-list.....	906
31.43	show ipv6 ospf virtual-links .....	907
31.44	show ipv6 ospf border-routers .....	908
31.45	show ipv6 ospf - area-range / summary-prefix.....	909
31.46	show ipv6 ospf - General Information.....	911
31.47	show ipv6 ospf - LSA Database .....	913
31.48	show ipv6 ospf route.....	915
31.49	show ipv6 ospf areas.....	916
31.50	show ipv6 ospf host .....	917
31.51	show ipv6 ospf redist-config .....	918
32	DiffServ (Differentiated Services).....	919
32.1	set qos .....	921
32.2	class-map .....	922
32.3	policy-map .....	923
32.4	match .....	924
32.5	class .....	925
32.6	set cos .....	926
32.7	police .....	927
32.8	cosq scheduling algorithm .....	929
32.9	traffic class.....	930
32.10	show policy-map.....	931

---

32.11	show class-map.....	933
32.12	show cosq algorithm.....	934
32.13	show cosq weights-bw.....	935
33	ACL (Access Control Lists).....	936
33.1	ip access-list.....	938
33.2	mac access-list extended.....	940
33.3	permit - standard mode.....	941
33.4	deny - standard mode.....	942
33.5	redirect - standard mode.....	943
33.6	permit- ip/ospf/pim/protocol type.....	944
33.7	deny - ip/ospf/pim/protocol type.....	946
33.8	redirect - ip/ospf/pim/protocol type.....	948
33.9	permit tcp.....	950
33.10	deny tcp.....	952
33.11	redirect tcp.....	954
33.12	permit udp.....	956
33.13	deny udp.....	958
33.14	redirect udp.....	960
33.15	permit icmp.....	962
33.16	deny icmp.....	965
33.17	redirect icmp.....	967
33.18	ip access-group.....	970
33.19	mac access-group.....	971
33.20	permit.....	972
33.21	deny.....	974
33.22	redirect.....	976
33.23	show access-lists.....	978
34	Loop protection.....	980
34.1	loop-protect.....	981
34.2	loop-protect - interface.....	982
34.3	loop-protect disable-period.....	983
34.4	loop-protect receive-action.....	984
34.5	loop-protect transmit-interval.....	985
34.6	show loop-protect.....	986
35	Link Status Tracking.....	987
35.1	link-status-tracking.....	988
35.2	link-status-tracking group.....	989
35.3	link-status-tracking group - interface.....	990
35.4	show link-status-tracking.....	991
36	Data Center Bridging.....	993
36.1	group.....	994
36.2	group-bandwidth.....	995
36.3	pfc priority.....	996
36.4	pri2pg.....	998
36.5	pfc group.....	1000

36.6	pfc priority .....	1002
36.7	cee .....	1004
36.8	dcbx cee .....	1005
37	LLDP .....	1006
37.1	set lldp .....	1008
37.2	lldp chassis-id-subtype .....	1009
37.3	lldp holdtime-multiplier .....	1011
37.4	lldp notification interval .....	1012
37.5	lldp reinitialization-delay .....	1013
37.6	lldp transmit-interval .....	1014
37.7	lldp tx-delay .....	1015
37.8	clear lldp counters .....	1016
37.9	clear lldp table .....	1017
37.10	lldp notification .....	1018
37.11	lldp port-id-subtype .....	1019
37.12	lldp tlv-select basic-tlv .....	1020
37.13	lldp tlv-select dcbx-cee-pfc .....	1021
37.14	lldp tlv-select dcbx-cee-pg .....	1022
37.15	lldp tlv-select dot1tlv .....	1023
37.16	lldp tlv-select dot3tlv .....	1024
37.17	lldp transmit   receive .....	1025
37.18	debug lldp .....	1026
37.19	show lldp .....	1028
37.20	show lldp dcbx .....	1029
37.21	show lldp errors .....	1030
37.22	show lldp interface .....	1031
37.23	show lldp local .....	1032
37.24	show lldp neighbors .....	1033
37.25	show lldp statistics .....	1034
37.26	show lldp traffic .....	1035

# 1 Introduction

## 1.1 Purpose

The **SSE-3348S/R, and SSE-X3348T/R standalone switches** are 1U rackmount Ethernet switches – also part the Supermicro Intelligent Switch product line, and are standalone units.

All of these switches are managed Layer2/Layer 3 switches that share a common switching and protocol support code base, and provide wire speed switching on each of their 1 Gig and 10 Gig Ethernet ports.

**SMIS** provides the basic switching functionality and also offers advanced features such as link aggregation, GVRP/GMRP, IGMP Snooping, layer 3 unicast and multicast routing for both IPv4 and IPv6.

This guide details the Command Line Interface (CLI) configurations for the features supported in **SMIS**. For specific details about any of the Blade switches or the standalone switches, please refer to their corresponding user guides.

## 1.2 Scope

The scope of this document is limited to the following **Super Micro Intelligent Switch** products:

- **SSE-3348S**
- **SSE-3348SR**
- **SSE-X3348T**
- **SSE-X3348TR**

Other switch products may be added to these product lines from time to time. It is anticipated that all will use this base of CLI commands unless otherwise noted.

## 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.

## 1.4 Key Conventions

### 1.4.1 Keyboard shortcuts

Keys	Action
Up Arrow / Down Arrow	Displays the previously executed command
Ctrl + A	Moves the cursor to the previous command line
Ctrl + C	Exits from the SMIS 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

### 1.4.2 Others

Keys	Action
?	Helps to list the available commands
Q	Exits the output display if display is more than one page and returns to the SMIS prompt
show history	Displays the command history list

## 2 Command Line Interface

This section describes the configuration of **SMIS** 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 **SMIS** CLI supports a simple login authentication mechanism. The authentication is based on a user name and password provided by the user during login.

When **SMIS** is started, the user name and password must be given at the login prompt to access the CLI shell. The default password for the user ID 'ADMIN' is unique for each switch that are shipped after 1<sup>st</sup> January, 2020 and the password can be found on the label stuck on the switch. For the older switches that were shipped before 1<sup>st</sup> January, 2020, the default password for user ID 'ADMIN' is 'ADMIN'.

### Supermicro Intelligent Switch Solution

```
smis Login: ADMIN  
Password: *****
```

```
smis>
```

The "user-exec" mode is now available to the user. CLI Command Modes provide a detailed description of the various modes available.

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 **SMIS** 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. Appropriate error messages will be displayed if the dependencies are not satisfied

### 2.1 CLI Command Modes



Command Mode	Access Method	Prompt	Exit method
User EXEC	This is the initial mode to start a session.	<b>smis&gt;</b>	The logout method is used.
Privileged EXEC	The User EXEC mode command <b>enable</b> , is used to enter the Privileged EXEC mode.	<b>SMIS#</b>	To return from the Privileged EXEC mode to User EXEC mode the <b>disable</b> command is used.
Global Configuration	The Privileged EXEC mode command <b>configure terminal</b> , is used to enter the Global Configuration mode	<b>SMIS (config) #</b>	To exit to the Global Configuration mode the <b>exit</b> command is used and to exit to the Privileged EXEC mode the <b>end</b> command is used.
Interface configuration	The Global Configuration mode command <b>interface &lt;interfacetype&gt;&lt;interfaceid&gt;</b> is used to enter the Interface configuration mode	<b>SMIS (config-if) #</b>	To exit to the Global Configuration mode the <b>exit</b> command is used and to exit to the Privileged EXEC mode the <b>end</b> command is used.
Config-VLAN	The global configuration mode command <b>vlan vlan-id</b> , is used to enter the Config-VLAN mode.	<b>SMIS (config-vlan) #</b>	To exit to the Global Configuration mode the <b>exit</b> command is used and to exit to the privileged EXEC mode the <b>end</b> command is used.
Line Configuration	The global configuration mode command <b>line</b> is used to enter the Line Configuration mode.	<b>SMIS (config-line) #</b>	To exit to the Global Configuration mode the <b>exit</b> command is used and to exit to the privileged EXEC mode the <b>end</b> command is used.
Slave Configuration	This is the initial mode to start SMIS in slave session.	<b>smis-boot&gt;</b>	The <b>reload</b> command is used to restart the switch.
Config-CEE-Map	The global configuration mode command <b>cee-map Cee-map-id</b> , is used to enter the Config-CEE-Map mode.	<b>smis (config-cee-map) #</b>	To exit to the Global Configuration mode the <b>exit</b> command is used and to exit to the privileged EXEC mode the <b>end</b> command is used.

## 2.2 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.

## 2.3 Privileged EXEC Mode

Since many of the privileged commands set operating parameters, privileged access is password protected in order 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.

## 2.4 Global Configuration Mode

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

## 2.5 Interface Configuration Mode

### 2.5.1 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.

### 2.5.2 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.

### 2.5.3 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.

## 2.6 Config-VLAN Mode

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

## 2.7 Line Configuration Mode

Line configuration commands modify the operations of a terminal line.

## 2.8 Slave Configuration

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

## 2.9 Config-CEE-Map Mode

The `cee-map` global configuration command creates a CEE-Map to declare a set of DCBX (CEE standard) settings, including:

- the mappings of priority and Priority Groups (PGs),
- bandwidth allocation for each PG, and
- PFC setting for each priority and PG.

The Global configuration mode command `cee-map <cee-map-number(1-4)>` is used to create/enter the CEE-Map Configuration mode and the prompt seen at this mode is `SMIS(config-cee-map)#`.

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

## 2.10 Protocol Specific Modes

### 2.10.1 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 `smis (config-mst)#`.

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

### 2.10.2 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 `SMIS (config-cmap) #`.

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

### 2.10.3 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 `smis (config-pmap) #`.

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

## 2.10.4 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 `smis (config-pmap-c) #`.

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

## 2.10.5 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 `SMIS (dhcp-config) #`.

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

## 2.10.6 ACL Standard Access List Configuration Mode

Standard accesses 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 `SMIS (config-std-nacl) #`.

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

## 2.10.7 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 `SMIS (config-ext-nacl) #`.

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

## 2.10.8 ACL MAC Configuration Mode

The MAC access-list global configuration command creates Layer 2 MAC ACLs, and returns the MACAccess 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 **SMIS (config-extmacl) #**.

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

## 2.11 Command Privileges

CLI commands are associated with a privilege. Similarly user accounts are also associated with a privilege level. Users can execute commands with privilege level same or lower than their privilege level.

Though switch supports privilege level 1 to 15, by default all the CLI commands are associated with either level 1 or 15. All the show commands and similar display commands are associated with privilege level 1. And all the configuration change commands are associated with level 15.

## 3 System Features

SMIS 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 might have special hardware requirements and others might have special design considerations. The related command links provide overview descriptions of the features and includes specific information to consider when using these features.

### Management IP Commands

Command	Description
<a href="#">ip address dhcp</a>	This command configures the mode by which the default interface acquires its IP address.
<a href="#">ip address</a>	This command configures the IP address and subnet mask for the default interface.
<a href="#">ip gateway</a>	This command configures the gateway IP address for the default management interface.

### Management Access Commands

Command	Description
<a href="#">login authentication</a>	This command sets the authentication method for user logins and the no form of the command sets the authentication method for user logins to default values.
<a href="#">username</a>	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.
<a href="#">listuser</a>	This command lists all valid users, along with their permissible mode.
<a href="#">show users</a>	This command displays information about terminal lines.
<a href="#">show privilege</a>	This command shows current user privilege level.
<a href="#">enable password</a>	This command modifies enable password

	parameters and the no form of the command disables enable password parameters.
<a href="#">enable</a>	This command turns on privileged commands.
<a href="#">disable</a>	This command turns off privileged commands.
<a href="#">logout</a>	This command exits from Privileged EXEC/ User EXEC mode to ISS Login Prompt in case of console session.
<a href="#">lock</a>	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.
<a href="#">ip http port</a>	This command sets the HTTP port and the no form of the command resets the HTTP port.
<a href="#">set ip http</a>	This command enables/disables HTTP.
<a href="#">web session-timeout</a>	This command configures the idle timeout value for web management sessions.
<a href="#">show http server status</a>	This command displays the http server status.
<a href="#">authorized-manager ip-source</a>	This command configures an IP authorized manager and the no form of the command removes manager from authorized managers list.
<a href="#">show authorized-managers</a>	This command displays the configured authorized managers.
<a href="#">debug nm</a>	This command enables the display of debug messages for web interface module.

### CLI Helping Commands

Command	Description
<a href="#">configure terminal</a>	This command enters the configuration mode.
<a href="#">exit</a>	This command exits the current configuration mode to the next highest configuration mode in the CLI.
<a href="#">end</a>	This command exits from Configuration mode.

<a href="#">show running-config</a>	This command displays the current operating configuration in the system. This command is common for both Single Instance and Multiple Instance.
<a href="#">alias</a>	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.
<a href="#">help</a>	This command displays help for a particular command.
<a href="#">show history</a>	This command displays command list history.
<a href="#">clear screen</a>	This command clears the screen.
<a href="#">exec-timeout</a>	This command sets EXEC timeout (in seconds) for line disconnection and the no form of the command clears EXEC timeout for line disconnection.
<a href="#">run script</a>	This command runs CLI commands from the specified script file.
<a href="#">show aliases</a>	This command displays the aliases.
<a href="#">show line</a>	This command displays TTY line information.
<a href="#">line</a>	This command configures a console/virtual terminal line.
<a href="#">cli pagination</a>	This command helps to enable and disable the paginated display.

### Firmware Upgrade Command

Command	Description
<a href="#">firmware upgrade</a>	

### Time management Commands

Command	Description
<a href="#">ntp key</a>	This command configures a trusted key.
<a href="#">ntp server</a>	This command configures the SNTP server IP



	address.
<a href="#">ntp broadcast</a>	This command enables the SNTP broadcast client. This is used to enable SNTP client to accept SNTP traffic from any broadcast server.
<a href="#">ntp enable</a>	This command enables SNTP.
<a href="#">ntp disable</a>	This command disables SNTP.
<a href="#">tz offset</a>	This command configures the time zone offset with respect to coordinated universal time (UTC).
<a href="#">show ntp</a>	This command displays SNTP configurations.
<a href="#">clock set</a>	This command manages the system clock.
<a href="#">show clock</a>	This command displays the system date and time.

### Configuration File Management Commands

Command	Description
<a href="#">write</a>	Stores running configuration as startup configuration or into given file name in flash.
<a href="#">set startup-config</a>	This command configures the default restoration file.
<a href="#">copy</a>	Copies flash files or remote files to flash.
<a href="#">copy startup-config</a>	Copies startup configuration to other flash file or remote flash file.
<a href="#">copy- file</a>	Copies files from flash to remote vice versa.
<a href="#">erase</a>	Deletes startup configuration file or any flash file.
<a href="#">list files</a>	Lists all the configuration files stored in flash.
<a href="#">show file</a>	Displays the file contents
<a href="#">show startup-config</a>	Displays the startup config file contents
<a href="#">show stored-config</a>	Displays the given configuration file contents

### Interface Commands

Command	Description
<a href="#">interface</a>	This command selects an interface to configure, which can be a physical interface or a port-channel interface or a VLAN interface or OOB (Out of Band) interface. The no form of the command is used to delete a VLAN / port-channel interface. On execution of this command, the user enters the interface configuration mode for that interface.
<a href="#">description</a>	This command configures the description string to the port interfaces.
<a href="#">switchport</a>	This command configures the port as switch port. The no form of the command configures the port as router port.
<a href="#">ip address</a>	This command sets the IP address of an interface. The no form of the command resets the IP Address for the given Interface.
<a href="#">ip address dynamic</a>	This command configures the current VLAN 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
<a href="#">mtu frame size</a>	This command configures the maximum transmission unit frame size for the interface.
<a href="#">system mtu frame size</a>	This command configures the maximum transmission unit frame size for all the interfaces on the switch.
<a href="#">flowcontrol</a>	This command is used to set the send or receive flow-control value for an interface.
<a href="#">shutdown - physical/VLAN/port-channel</a>	This command disables a physical interface/VLAN interface/port-channel interface
<a href="#">negotiation</a>	This command enables auto-negotiation on the interface and the no form of the command disables auto negotiation on the interface.
<a href="#">capabilities</a>	This command configures the auto negotiation capabilities.

<a href="#">speed</a>	This command sets the speed of the interface and the no form of the command sets the speed of the interface to its default value.
<a href="#">duplex</a>	This command configures the duplex operation and the no form of the command configures the duplex operation to the default value.
<a href="#">monitor session</a>	This command enables port-mirroring in the switch and the no form of the command disables port mirroring in the switch.
<a href="#">hol blocking prevention</a>	This command enables the Head-Of-Line blocking prevention on the interface and the no form of the command disables the same.
<a href="#">storm-control</a>	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.
<a href="#">rate-limit</a>	This command configures the output rate limiting for the interfaces.
<a href="#">snmp trap link-status</a>	This command enables trap generation on either the physical interface or the port-channel interface.
<a href="#">reset interface statistics</a>	This command clears interface counters.
<a href="#">reset interface cpu statistics</a>	This command clears CPU counters.
<a href="#">show ip interface</a>	This command displays the IP interface configuration.
<a href="#">show interfaces</a>	This command displays the interface status and configuration.
<a href="#">show interfaces - counters</a>	This command displays the interface statistics for each port.
<a href="#">show interfaces cpu counters</a>	This command displays the CPU statistics for each port.
<a href="#">show interface mtu</a>	This command shows the Maximum Transmission Unit (MTU) of ports in the switch.
<a href="#">show conf</a>	This command displays the interface specific

	running configuration.
<a href="#">show port-monitoring</a>	This command displays port-monitoring information.
<a href="#">show flow-control</a>	This command displays the flow-control information.
<a href="#">show transceiver</a>	This command displays the information about fiber optic transceiver modules.
<a href="#">show meminfo</a>	This command displays the memory status and utilization.

### System Commands

Command	Description
<a href="#">device name</a>	This command configures the switch name string.
<a href="#">system location</a>	This command configures the switch location information string.
<a href="#">system contact</a>	This command configures the switch contact information.
<a href="#">set boot-up</a>	This command configures the next bootup firmware image selection.
<a href="#">reload</a>	This command restarts the switch.
<a href="#">reset-to-factory-defaults</a>	This command resets the switch to factory defaults configuration.
<a href="#">mac-address-table aging-time</a>	This command sets the maximum age of a dynamically learnt entry in the MAC address table.
<a href="#">copy debugg-logging</a>	This command writes the debug logs to a remote site or to external USB memory.
<a href="#">debug-logging</a>	This command configures where debug logs are to be displayed and the no form of the command displays debug logs in the console.
<a href="#">no startup-config</a>	This command makes no configuration file will be loaded in next reboots of the switch.
<a href="#">show system information</a>	This command displays system information.

<a href="#">show version</a>	This command displays hardware and firmware version numbers.
<a href="#">show debug-logging</a>	This command displays the debug logs stored in file.
<a href="#">show debugging</a>	This command displays state of each debugging option.
<a href="#">show system acknowledgement</a>	This command displays the acknowledgement text describing the open source components used on the switch software.
<a href="#">show system environment</a>	This command displays the temperature, fan status and power supply status information.
<a href="#">show tech-support</a>	This command displays various information that are useful for troubleshooting.
single-blade-slot-num	This command configures the single blade server slots in SBM-XEM-X10SM switches.
show single-blade-slot-num	This command displays the single blade server slots configuration in SBM-XEM-X10SM switches.
split40g	This command splits the 40Gig ports as 10Gig ports in SSE-X3348S(R) and SSE-X3348T(R) switches.
show split40g	This command displays the split configuration of 40Gig ports as 10Gig ports in SSE-X3348S(R) and SSE-X3348T(R) switches.

## 3.1 ip address dhcp

This command configures the default management interface to get IP address through DHCP.

The no form of this command configures the default management interface to use static IP address.

```
ip address dhcp
```

```
no ip address dhcp
```

### Mode

Global Configuration Mode

### Defaults

Static IP

### Example:

```
SMIS(config)# ip address dhcp
```

### Related Commands

show ip int – Displays the management interface IP information.

## 3.2 ip address

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

```
ip address [<ip-address> | <ip-address>/prefix-length] [<subnet-mask>]
```

```
no ip address
```

### Syntax Description

**ip address** - IP address

**subnet-mask** - Subnet Mask

**prefix-length** – Subnet mask as a prefix number

### Mode

Global Configuration Mode

### Defaults

ip address – 192.168.100.2

subnet-mask - 255.255.255.0

### Example:

```
SMIS(config)# ip address 20.0.0.1/8
```

### Related Command

**show ip int** - Displays the management interface IP information.

### 3.3 ip gateway

This command configures the gateway IP address for the management interface.

The “no” form of this command will remove the configure gateway IP.

This command works only for the following blade switch models.

SBM-GEM-X2C

SBM-GEM-X2C+

SBM-GEM-X3S+

SBM-GEM-X10SM

- ➡ For other switch models, use the “ip route” command to configure the required routing entries with the desired gateway addresses.

```
ip gateway <ip-address>
```

```
no ip gateway
```

#### Syntax Description

**ip address** – Gateway IP address

#### Mode

Global Configuration Mode

#### Defaults

0.0.0.0

#### Example:

```
SMIS(config)# ip gateway 20.0.0.1
```

#### Related Command

**show ip int** - Displays the management interface IP and gateway information.



## 3.4 login authentication

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

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

```
no login authentication
```

### Syntax Description

**local** - Local username database for authentication

**radius** - List of all RADIUS servers for authentication

**tacacs** - Terminal Access Controller Access Control System

### Mode

Global Configuration Mode

### Defaults

Local

### Example:

```
SMIS(config)# login authentication radius
```

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

TACACS is an authentication program used on UNIX / Linux systems, few network routers and other network equipment that 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

### 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

## 3.5 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 <passwd>] [privilege <1-15>] [admin]
```

```
no username < user-name >
```

### Syntax Description

**user-name** - User Name

**password** - Password

**privilege** - Privilege Level

**admin** – This keyword indicates this given user will be the default administrative user. The default administrative user cannot be deleted.

### Mode

Global Configuration Mode

### Related Command

**enable password** - Modifies enable password parameters

### Note:

1. Users with privilege level 1 can execute show or similar display commands only, they can not execute any configuration change commands. Users with privilege level 15 only can execute configuration change commands.
2. The default ADMIN user can be deleted only after any other active user configured with “admin” keyword.

## 3.6 listuser

This command lists all valid users, along with their permissible mode.

**listuser**

**Mode**

Privileged EXEC Mode

The command lists the user, mode and groups.

**Related Command**

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

## 3.7 show users

This command displays information about terminal lines.

### **show users**

#### **Mode**

Privileged EXEC Mode

#### **Example:**

```
SMIS# show users
```

```
Line User Peer-Address
```

```
0 con root Local Peer
```

#### **Related Command**

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

## 3.8 show privilege

This command shows current user privilege level.

**show privilege**

**Mode**

Privileged EXEC Mode

**Example:**

```
SMIS# show privilege
```

```
Current privilege level is 15
```

**Note:** Users with privilege level 1 can execute show or similar display commands only, they can not execute any configuration change commands. Users with privilege level 15 only can execute configuration change commands.

## 3.9 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

**Level1** - Privilege Level

### Mode

Global Configuration Mode

- ➔ The enable password command is used to set the password for a particular privilege Level.
- ➔ When this command is configured, the switch prompts for the password, whenever user wants to move from lower privilege level to higher privilege level using enable command

### Related Command

**username** - Creates a user and sets the enable password for that user with the privilege level

## 3.10 enable

This command turns on privileged commands.

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

### Syntax Description

**Enable Level** - Level to enter the system

### Mode

User EXEC Mode

Level 0 is the most restricted level. User created with level 0 has access only to the following commands:

- disable
- enable
- exit
- help
- logout

Level 1 includes all user-level commands at the smis> prompt.

Level 15 is the least restricted level and included all commands

It is possible to configure additional access levels (from level 2 to 14) to meet the needs of the users while protecting the system from unauthorized access.

After a user logs in with a username that has privileges, the full set of CLI commands, including those in User mode can be accessed

Default Privileged level is assigned by the user

### Related Commands

**disable** - Turns off privileged commands

**enable password** - Modifies enable password parameters

## 3.11 **disable**

This command turns off privileged commands.

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

### **Mode**

User EXEC Mode

### **Example:**

In User mode the user can monitor and display ISS parameters, but not change them.

### **Related Command**

**enable** - Turns on privileged commands



## 3.12 logout

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

**logout**

**Mode**

User EXEC Mode

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

**Related Command**

**slot-modtype** - Associates card module type information for a slot

## 3.13 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.

**lock**

**Mode**

Privileged EXEC Mode

The login password has to be reentered by the user to release the console lock and access the CLI command shell.

## 3.14 ip http port

This command sets the HTTP port and the no form of the command resets the HTTP port.

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

```
no ip http port
```

### Mode

Global Configuration Mode

### Defaults

80

### Example:

```
SMIS(config)# ip http port 90
```

➡ HTTP port number will take effect only when HTTP is disabled and enabled again.

### Related commands

**set ip http** - Enables/disables HTTP

## 3.15 set ip http

This command enables/disables HTTP.

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

### Syntax Description

**enable** - Enables HTTP status in the system

**disable** - Disables HTTP status in the system

### Mode

Global Configuration Mode

### Defaults

enable

### Example:

```
SMIS(config)# set ip http disable
```

### Related Commands

**ip http port** - Sets the HTTP port

**show http server status** - Displays the http server status

## 3.16 web session-timeout

This command configures the idle timeout value for web management sessions. The default value is 600 seconds.

```
web session-timeout <timeoutvalue>
```

### Syntax Description

**timeoutvalue** - Any integer number from 1 to 9999 seconds

### Mode

Global Configuration Mode

### Defaults

600

### Example:

```
SMIS(config)# web session-timeout 300
```

## 3.17 show http server status

This command displays the http server status.

**show http server status**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show http server status
HTTP server status : enabled
HTTP port is : 90
```

### Related Commands

**ip http port** – Sets the HTTP port

**set ip http** – Enables/disables HTTP

## 3.18 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> | /
<prefixlength(1-32)>}] [interface [<interface-type <0/a-b, 0/c, ...>]
[<interfacetype <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 > | /
<prefixlength(1-32)>}]
```

### Syntax Description

**ip-address** - Specifies either the Network or Host address

**subnet-mask** - IP address mask to be applied

**prefix-length** - Prefix Length

**interface** - Valid interfaces include physical ports (including type, slot, and port number)

**vlan** - The VLANs in which the IP authorized manager can reside

**cpu0** - Out of Band Management Interface

**service** - Indicates service type. Can be one of the following: telnet, ssh, http, https or snmp

### Mode

Global Configuration Mode

### Defaults

All services are allowed for the configured manager

### Example:

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

➔ An address 0.0.0.0 indicates 'Any Manager'."

### Related Command

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

## 3.19 show authorized-managers

This command displays the configured authorized managers.

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

### Syntax Description

**ip-source** - Specifies either the Network or Host address

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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



## 3.20 debug nm

This command enables the display of debug messages for web module. The no form of this command disables the debug messages for web interface module.

```
debug nm [{all | info | errors | mgmt | data}]
```

```
no debug nm [{all | info | errors | mgmt | data}]
```

### Syntax Description

**all** – Enables all the available debug messages of web module

**info** – Enables only the informative debug messages of web module

**errors** – Enables only the error messages of web module

**mgmt** – Enables only the management control debug messages of web module

**data** – Enables only the packet data related debug messages of web module

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# debug nm all
```

### Related Command

## 3.21 **configure terminal**

This command enters the configuration mode.

**configure terminal**

### **Mode**

Privileged EXEC Mode

### **Related Commands**

**end** - Exits from Configuration mode

**exit** - Exits the current configuration mode to the next highest configuration mode

## 3.22 `exit`

This command exits the current configuration mode to the next highest configuration mode in the CLI.

`exit`

### **Mode**

All modes

The login name and password has to be reentered by the User to gain access to the CLI command shell.

### **Related Command**

`end` - Exits from Configuration mode

## 3.23 end

This command exits from Configuration mode.

**end**

### **Mode**

All modes

This command can be executed from any mode but it reverts back to Privileged Exec mode

### **Related Command**

**exit** - Exits the current configuration mode to the next highest configuration mode

## 3.24 show running-config

This command displays the current operating configuration in the system. This command is common for both Single Instance and Multiple Instance.

```
show running-config [{ syslog | dhcp | dvmrp | qos | stp | la | pnac |
igs | | vlan <vlan-id(1-4069)> | interface { port-channel <port-
channel-id(1-65535)> | <interfacetype> <interfacenum> | vlan <vlan-
id(1-4069)> } | ospf | rip | bgp | ipv6 | rip6 | ssh | ssl | acl | ip |
pim | pimv6 | vrrp | snmp | radius | rmon | rm | mbsm | ospf3 | igmp |
igmp-proxy }]
```

### Syntax Description

**syslog** - Syslog Module

**dhcp** - DHCP Module

**dvmrp** - DVMRP Module

**qos** - Quality of Service Module

**stp** - STP Module

**la** - LA Module

**pnac** - PNAC Module

**igs** - IGS Module

**mlds** - MLD Snooping Module

**vlan** - VLAN Module

**interface** - Port-channel/Physical/VLAN Interface

**ospf** - OSPF Module

**rip** - RIP Module

**bgp** - BGP Module

**ipv6** - IPv6 Module

**rip6** - RIP6 Module

**ssh** - SSH Module

**ssl** - SSL Module

**acl** - ACL Module

**ip** - IP Module

**pim** - PIM Module

**vrrp** - VRRP Module

**snmp** - SNMP Module

**radius** - RADIUS Module  
**rmon** - RMON Module  
**rm** - RM Module  
**mbsm** - MBSM Module  
**ospf3** - OSPFv3 Module  
**igmp** - IGMP Module  
**pimv6** - PIMv6 Module  
**igmp-proxy** - IGMP Proxy Module

**Mode**

Privileged EXEC Mode

**Example:**

SMIS# **show running-config**

Building configuration...

Switch ID	Hardware Version	Firmware Version
0	SSE-G48-TG4 (P2-01)	1.0.13-7

```
ip address dhcp
interface port-channel 1
exit
```

```
vlan 1
  ports gi 0/11-19 untagged
  ports gi 0/41-48 untagged
  ports ex 0/2 untagged
exit
```

```
vlan 10
  ports gi 0/1-10 untagged
  ports gi 0/20-40 untagged
  ports po 1 untagged
exit
```

```
vlan 20,30
exit
```

```
interface vlan 1
  ip address dhcp
exit
```

## 3.25 alias

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** - Replacement string

**token to be replaced** - Abbreviated/short form of the replacement string

### Mode

Global Configuration Mode

- ➡ The purpose of such a replacement string is that commands can be executed using their abbreviated/short form.

### Related Command

**show aliases** - Displays the aliases

## 3.26 help

This command displays help for a particular command.

**help** [ **command** ]

### Syntax Description

**Command** - The privileged command

### Mode

All modes

- ➔ "?" can be used as an alternative for the word "help". When "help" or "?" is typed in the specific mode all commands present in that mode as well as all general commands will be listed.
  
- ➔ When a keyword is typed, all possible commands starting with that keyword are displayed



## 3.27 show history

This command displays command list history.

**show history**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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
```

- ➡ The commands are listed from the first to the latest command. The buffer is kept unchanged when entering to configuration mode and returning.

## 3.28 clear screen

This command clears the screen.

**clear screen**

**Mode**

All Modes

## 3.29 exec-timeout

This command sets EXEC timeout (in seconds) for line disconnection and the no form of the command clears EXEC timeout for line disconnection.

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

```
no exec-timeout
```

### **Mode**

Line Configuration Mode

### **Defaults**

1800 seconds

### **Related Command**

**line** - Configures a console/virtual terminal line

## 3.30 run script

This command runs CLI commands from the specified script file.

```
run script <script file> [<output file>]
```

### Syntax Description

**script file** - The script file to be executed

**output file** - The output file

### Mode

Privileged EXEC Mode

## 3.31 show aliases

This command displays the aliases.

**show aliases**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show aliases
```

```
show -> sh
```

```
previlege -> pr
```

- ➔ The **show aliases** command displays the alias commands and associated CLI commands for the current mode

### Related Command

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

## 3.32 show line

This command displays TTY line information.

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

### Syntax Description

**console** - Console

**vty** - Virtual terminal line

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show line console
```

```
Current Session Timeout (in secs) = 1800
```

➔ The command-line history buffer stores CLI commands that are previously entered.

### Related Command

**line** - Configures a console/virtual terminal line

## 3.33 line

This command configures a console/virtual terminal line.

```
line {console | vty}
```

### Syntax Description

**console** - Console

**vty** - Virtual terminal line

### Mode

Global Configuration Mode

### Related Commands

**end** - Exits from Configuration mode

**exit** - Exits the current configuration mode to the next highest configuration mode

**show line** - TTY line information

## 3.34 cli pagination

This command enables the paginated display. When switch displays large texts on CLI, it breaks the output as multiple pages for better view. This is enabled by default.

The no form of this command disables the pagination. When the pagination is disabled, switch displays the large texts continuously without page breaks.

**cli pagination**

**no cli pagination**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Related Commands



## 3.35 firmware upgrade

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

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

### Syntax Description

**tftp://ipaddress/ filename** - Source URL alias for a network (tftp) file system

**flash:normal** - To write into normal flash area.

**flash:fallback** - To write into fallback flash area.

**usb:filename** - Firmware image file name in external USB memory

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# firmware upgrade tftp://20.0.0.1/SWITCH_FIRMWARE_1.0.13-10.bin  
flash:normal
```

The TFTP protocol is used for getting the image from the remote-site.

In case of stacking, firmware upgrade in master, automatically will upgrade firmware in all slave switches connected in stack. On successful completion of firmware upgrade in slave switches, a message will be displayed.

## 3.36 ntp key

This command is used to add a key to a trusted key list. This command takes key text along with key identifier.

The no form of this command removes the configured key referred by the given key identifier.

```
ntp key <key_number (1- 65535)> <key_text>
```

```
no ntp key <integer(1-65535)>
```

### Syntax Description

key\_number - Any number between 1 to 65535 to identify the key string

key\_text – Any string up to 32 characters to be used as key to handshake with NTP servers.

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# ntp key 1 abcd
```

### Related Command

**ntp broadcast** - enables NTP broadcast with authentication

**ntp enable** - Enables NTP

## 3.37 ntp broadcast

This command enables the switch to accept NTP broadcast messages sent by NTP broadcast servers. This command also enables the authentication for the received NTP broadcast messages if authentication option is given.

The no form of this command configures the switch not to accept NTP broadcast messages.

```
ntp broadcast [authentication]
```

```
no ntp broadcast
```

### Syntax Description

authentication – Accepts NTP broadcasts from NTP servers after the authentication

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# ntp broadcast authentication
```

### Related Command

**ntp server** - Configures NTP server IP address, key, interval and preference

**ntp enable** - Enables NTP

## 3.38 ntp server

This command configures the SNTP server information.

The no form of this command removes the given NTP server configuration.

```
ntp server <ip-address> [key(1-65535)] [interval(6-17)] [prefer]
```

```
no ntp server <ip_address>
```

### Syntax Description

**ip-address** – IP address of NTP sever.

**key** – key number to add into a trusted key list

**interval** – exchange message delay for server

**prefer** – tells which server should have to be more preferable

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# ntp server 10.10.1.100 10 prefer
```

### Related Command

**ntp broadcast** - enables NTP broadcast with authentication

**ntp enable** - Enables NTP

## 3.39 ntp enable

This command enables the NTP

**ntp enable**

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# ntp enable
```

### Related Command

**ntp broadcast** - enables NTP broadcast with authentication

**ntp disable** - Disables NTP

## 3.40 ntp disable

This command disables the NTP

**ntp disable**

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# ntp disable
```

### Related Command

**ntp broadcast** - enables NTP broadcast with authentication

**ntp enable** - Enables NTP

## 3.41 tz offset

This command configures the time zone offset with respect to coordinated universal time (UTC).

**tz offset** <HH>:<MM>

### Syntax Description

**HH** – Hour difference from UTC.

**MM** – Minutes difference from UTC.

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# tz offset 08:00
```

### Related Command

**ntp server** - Configures SNTP server IP address

**ntp broadcast** - Enables SNTP broadcast client

## 3.42 show ntp

This command displays ntp configuration details.

**show ntp**

### Syntax Description

#### Mode

Global Configuration Mode

#### Example:

```
SMIS(config)# show ntp
```

### Related Command

**ntp server** - Configures SNTP server IP address

**ntp broadcast** - Enables SNTP broadcast client



## 3.43 clock set

This command manages the system clock.

```
clock set hh:mm:ss day month year
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# clock set 18:04:10 18 Oct 2005
```

The date is configured in the Switch in the format,

- Hours:minutes:Seconds Date Month Year
- The format for the month is Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec
- The format for the year is yyyy

### Related Command

**show clock** - Displays the system clock

## 3.44 show clock

This command displays the system date and time.

**show clock**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show clock
Tue Oct 18 18:04:11 2005
```

### Related Command

**clock set** - Manages the system clock

## 3.45 `rtc sync`

This command is to sync real time clock from system time.

This command is supported only on the following switch models and specified hardware revision

SSE-X2C+ (B2-01 R.3.0)

SSE-X3S+ (B4-01 R.3.0)

SSE-X24S

SSE-X24SR

SSE-X3348S

SSE-X3348SR

SSE-X3348T

SSE-X3348TR

SSE-XEM-X10SM(B3-01 R.1.04 and B5-01 R.1.04)

**`rtc sync`**

### **Mode**

Privileged EXEC Mode

### **Example:**

```
SMIS# rtc sync
```

### **Related Command**

**`clock set`** - Manages the system clock

## 3.46 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 |  
usb:filename }
```

### Syntax Description

**flash:filename** – File name to be written in to flash memory

**startup-config** - Startup Configuration. If this option is chosen, then the switch will start with the saved configuration on reboot

**tftp** - Copies a file to a TFTP server

**ip-address** - the IP address or host name of the server to receive the file

**filename** - the name assigned to the file on the server

**usb:filename** – File name to be written in to external usb memory

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# write startup-config
```

A startup-config contains configuration information that the ISS uses when it reboots

TFTP is a simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for Example:, username and password)

### Related Commands

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

**show system information** - Displays system information

## 3.47 set startup-config

This command configures the default restoration file.

```
set startup-config <filename>
```

### Mode

Global Configuration Mode

### Defaults

iss.conf

### Example:

```
SMIS(config)# set startup-config /home/iss/restore.conf
```

The file path mentioned in the **<filename>** must exist.

### Related Commands

show nvram – Displays the current information stored in the NVRAM.

## 3.48 copy

This command copies the given configuration file as startup configuration file.

```
copy { tftp://ip-address/filename startup-config | flash: filename
startupconfig | usb:filename startup-config }
```

### Syntax Description

**tftp://ipaddress/ filename startup-config** - File in remote location to be copied

**flash: filename startup-config** - File in flash to be copied

**usb:filename** – File name to be copied in to external usb memory

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# copy flash:clcliser startup-config
```

Filenames and directory names are case sensitive.

For copying a file to a new directory, the directory must already exist

A startup-config contains configuration information that the ISS uses when it reboots

TFTP is a simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for Example:, username and password)

## 3.49 copy mtdoops

This command is to copy crash dump content to a local file or remote file.

This command is supported only on the following switch models

SSE-X2C

SSE-X2C+

SSE-X3S+

SSE-G24-TG4

SSE-G48-TG4

```
copy mtdoops[{flash: filename | tftp://ip-address/filename}]
```

### Syntax Description

**tftp://ipaddress/filename** - File to be copied to remote location

**flash:filename** – File name to be copied to local flash memory

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# copy mtdoops flash:mtdoops.txt
```

```
SMIS# copy mtdoops tftp://192.168.100.1/mtdoops.txt
```

Filenames and directory names are case sensitive.

For copying a file to a new directory, the directory must already exist

TFTP is a simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for Example:, username and password)

## 3.50 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  
usb:filename }
```

### Syntax Description

**flash: filename** - Flash or remote site

**tftp** - Copies a file to a TFTP server

**ip-address** - the IP address or host name of the server to receive the file

**filename** - the name assigned to the file on the server

**usb:filename** - File name to be copied in to external usb memory

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# copy startup-config flash:clcliser
```

A startup-config contains configuration information that the ISS uses when it reboots.

TFTP is a simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for Example:, username and password)



## 3.51 copy-file

This command copies a file from a source remote site /flash / usb to a destination remote site/flash/usb.

```
copy { tftp://ip-address/filename | flash: filename | usb:filename}{  
tftp://ipaddress/filename | flash: filename | usb:filename}
```

### Syntax Description

**tftp** - Copies a log file to a TFTP server

**ip-address** - IP address or host name of the TFTP server to receive the file

**filename** - the name assigned to the file on the server

**flash: filename** - Flash or remote site

**usb:filename** – File name to be used in external usb memory

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# copy tftp://12.0.0.2/clclirel flash:clcliser
```

The filename must be an unquoted text string with the appropriate capitalization, no spaces, and a maximum length of 32 characters.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

## 3.52 erase

This command deletes the given file.

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

### Syntax Description

**startup-config** - Startup Configuration file

**flash:filename** - Local system flash file name

**usb:filename** - File name in external usb memory

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# erase startup-config
```

### Related Commands

**show system information** - Displays system information

## 3.53 list files

This command lists all the configuration and log files stored in the flash memory. If “usb:” option given it lists the files stored in the external USB memory.

For every files it displays the file name, file size and last modified time.

```
list files [usb:path]
```

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Example:

```
smis #list files
```

## 3.54 show file

This command displays the file contents. This can be used to display the files in flash.

```
show file <filename>
```

### Syntax Description

<filename> - File name

### Mode

Privileged EXEC Mode

### Example:

```
smis #show file iss.conf
```

## 3.55 show startup-config

This command displays the startup configuration file contents.

**show startup-config**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Example:

```
smis #show startup-config
```

## 3.56 show stored-config

This command displays the given configuration file contents.

```
show stored-config <filename>
```

### Syntax Description

<filename> - configuration file name

### Mode

Privileged EXEC Mode

### Example:

```
smis #show stored-config iss.conf
```

## 3.57 interface

This command selects an interface to configure, which can be a physical interface or a port-channel interface or a VLAN interface or loopback interface. The no form of this command is used to delete a VLAN / port-channel or loopback interface. On execution of this command, the user enters the interface configuration mode for that interface.

```
interface {vlan <vlan-id (1-4069)> | port-channel <port-channel-id (1-65535)> | <interface-type> <interface-id> | loopback <interface-id (1-100)> }
```

```
no interface { vlan <vlan-id (1-4069)> | port-channel <port-channel-id(1-65535)> | <interface-type> <interface-id> | loopback <interface-id (1-100)> }
```

### Syntax Description

**vlan** - VLAN Identifier any number between 1 to 4069

**port-channel** - Port Channel Identifier any number between 1 to 65535

**interface-type** - Interface type, can either be a gigabit Ethernet or extreme Ethernet (10Gig) or qx Ethernet (40Gig) interface.

**interface-id** - Physical interface ID including slot and port number.

**loopback** - Loopback interface ID any number between 1 to 100

### Mode

Global Configuration Mode

### Defaults

Vlan - 1

interface-type - eth0

### Example:

For VLAN Interface: SMIS(config)# interface Vlan 2

No port-channels are created by default

### Related Command

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

## 3.58 interface range

This command selects multiple interfaces to configure, which can be a physical interfaces or port-channel interfaces or a VLAN interfaces or loopback interfaces. The no form of this command is used to delete multiple VLAN / port-channel or loopback interfaces. On execution of this command, the user enters the interface configuration mode.

```
interface range <iflist_string>
```

```
no interface range <iflist_string>
```

### Syntax Description

**iflist\_string** – List of one or more interface ranges. To provide a range use a hyphen (-) between the start and end interface numbers.

E.g.: int range gi 0/1-10

To provide multiple interfaces or ranges, use separate with a comma (,).

E.g.: int range gi 0/1-10, gi 0/20

### Mode

Global Configuration Mode

### Related Command

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



## 3.59 description

This command configures the description string to port interfaces.

**description** <string>

### Syntax

<string> - Any alphanumeric string up to 64 characters length

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# description strg_lnk1
```

### Related Commands

**show interface description** - Displays the interface description strings.

## 3.60 switchport

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

**switchport**

**no switchport**

### Mode

Interface Configuration Mode

### Defaults

switchport

### Example:

```
SMIS(config-if)# switchport
```

### Related Commands

**show ip interface** - Displays the IP interface statistics and configuration

## 3.61 ip address

This command sets the IP address of an interface. The no form of the command resets the IP Address for the given Interface.

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

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

### Syntax Description

**ip-address** - IP address

**subnet-mask** - Subnet mask for the associated IP subnet

**secondary** - Additional IP address that can be configured for the Interface

### Mode

Interface Configuration Mode

- ➡ This command is applicable in Physical Interface Mode / VLAN Interface Mode/OOB Interface Mode

### Defaults

IP Address specified in issnvram.txt is taken as default.

### Example:

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

If the user deletes / modifies the IP interface that he is connected on, then the connection to the switch is lost.

When the **no ip address** command is executed without the optional parameter **<ip\_addr>**, all the IP addresses configured over the interface are deleted.

### Related Command

**show ip interface** - Displays the IP interface statistics and configuration

## 3.62 ip address dynamic

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.

```
ip address { dhcp | rarp }
```

```
no ip address
```

### Syntax Description

**rarp** - RARP Server

**dhcp** - DHCP Server

### Mode

Interface Configuration Mode

This command is applicable in VLAN Interface Mode.

### Defaults

dhcp

### Example:

```
SMIS(config-if)# ip address dhcp
```

### Related Commands

**show ip dhcp client stats** - Displays the DHCP client statistics information

**release** - Releases the DHCP lease on the interface specified

**renew** - Renews the DHCP lease for the interface specified

## 3.63 mtu frame size

This command configures the maximum transmission unit frame size for the interface.

The no form of this command removes the configured MTU value and resets it to the default value 1500.

```
mtu <frame-size(1500-9216)>
```

```
no mtu
```

### Mode

Interface Configuration Mode

### Defaults

1500

### Example:

```
SMIS(config-if)# mtu 9000
```

### Related Commands

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

**show interface mtu** - Displays the global maximum transmission unit

## 3.64 system mtu frame size

This command configures the maximum transmission unit frame size for all the interfaces in the system.

The no form of this command removes the configured MTU value on all the interfaces and resets it to the default value 1500.

```
system mtu <frame-size(1500-9216)>
```

```
no system mtu
```

### Mode

Interface Configuration Mode

### Defaults

1500

### Example:

```
SMIS(config-if)# mtu 9000
```

### Related Commands

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

**show interface mtu** - Displays the global maximum transmission unit

## 3.65 flowcontrol

This command is used to set the send or receive flow-control value for an interface. If flow control send is on for a device, and if it detects any congestion at its end, then it will notify 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. You can use both the *receive off* and *send off* keywords to disable flow control.

For PFC and DCBX capable switch products, please note that you must not turn on flowcontrol while PFC or DCBX is operating. Please set both the flowcontrol send and receive to off, prior to enabling PFC or DCBX.

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

### Syntax Description

**send** - Interface to send flow control packets to a remote device

**receive** - 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

### Mode

Interface Configuration Mode

### Defaults

The default flow control for the interfaces are flowcontrol receive off, flowcontrol send off

### Example:

```
SMIS(config-if)# flowcontrol send on
```

### Related Commands

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

**show flow-control** - Displays the flowcontrol information

## 3.66 pfc

This command configures the PFC (Priority-based Flow Control) function of an interface for all priorities (0 to 7). This command provides a way to directly enable the PFC to achieve the lossless ethernet with a PFC-enabled peer.

Note that the PFC function must not be enabled in conjunction with CEE-MAP and link-level flow control (IEEE 802.3x).

This feature is supported only on the following switch models

SBM-XEM-X10SM

SSE-X24S/R

```
pfc {enable|disable}
```

### Syntax Description

enable - Enable transmission and reception of PFC frames, for all priorities.

disable - Disable transmission and reception of PFC frames, for all priorities.

### Mode

Interface configuration mode.

### Defaults

The PFC function is disabled by default.

### Related Commands

flowcontrol jV Configures the 802.3x flow control.

cee-map - Create, modify, or delete a cee-map.

lldp tlv-select dcbx-cee-pfc - Configures the PFC feature sub-TLV.



## 3.67 shutdown - physical/VLAN/port-channel Interface

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

**shutdown**

**no shutdown**

### Mode

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

### Defaults

The Physical Interface eth0 is enabled by default  
The interface VLAN 1 is enabled by default for a VLAN interface  
The Port-channel interface is disabled by default

### Example:

```
SMIS(config-if)# shutdown
```

All functions on the specified interface are disabled by the shutdown command  
By default, if OOB interface is enabled, then the Physical Interface eth0 is disabled

### Related Commands

**interface** - Configures an interface, which can be a physical interface or a port-channel interface or a VLAN interface

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

## 3.68 negotiation

This command enables auto-negotiation on the interface and the no form of the command disables auto negotiation on the interface.

**negotiation**

**no negotiation**

### **Mode**

Interface Configuration Mode

### **Example:**

```
SMIS(config-if)# negotiation
```

If set as no negotiation, the configured values for interface speed, duplex mode and flow control will be effective

## 3.69 capabilities

This command configures the auto negotiation capabilities on the given port. By default the switch auto negotiates for all the supported speeds. This includes 1000 full (duplex), 100 full, 100 half, 10 full and 10 half. User can choose the speed setting that can be advertised during auto negotiation process. The "no" form of this command configures the capabilities for all the supported speeds.

```
capabilities [speed-1000full] [speed-100full] [speed 100-half] [speed-10full] [speed-10half]
```

```
no capabilities [speed-1000full] [speed-100full] [speed 100-half] [speed-10full] [speed-10half]
```

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# capabilities speed-1000full speed-100full
```

### Note:

This command is supported only for 1Gbps Ethernet interfaces on the following switch models SSE-G24-TG4, SSE-G48-TG4, SBM-GEM-X2C+ and SBM-GEM-X3S+. On blade switches the internal ports are fixed speed 1Gbps ports, hence capabilities configuration is not supported on those internal ports as well.

## 3.70 speed

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

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

```
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 detects the speed it must run on based on the peer switch.

### Mode

Interface Configuration Mode

### Defaults

auto

### Example:

```
SMIS(config-if)# speed 100
```

The Gigabit Ethernet port speed can be configured to 10, 100, or 1000 Mbps.

If the speed is set to auto, 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.

This parameter cannot be set if the port is automatically negotiating the link parameters with its peer. In that case, use the command "no-negotiation" to be able to set speed of the link and indicate whether it is full or half duplex.

### Related Commands

**negotiation** - Enables auto-negotiation on the interface

**duplex** - Configures the duplex operation

## 3.71 duplex

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

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

```
no duplex
```

### Syntax Description

**full** - Port is in full-duplex mode

**half** - Port is in half-duplex mode

### Mode

Interface Configuration Mode

### Defaults

full

### Example:

```
SMIS(config-if)# duplex half
```

Certain ports can be configured to be either full duplex or half duplex. Applicability of this command depends on the device to which the switch is attached.

### Related Commands

**negotiation** - Enables auto-negotiation on the interface

**speed** - Sets the speed of the interface

## 3.72 Energy Efficient Ethernet (SSE-X3348T/R only)

IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can reduce power used for cable lengths of 60 meters or less, with more significant reduction for cables of 20 meters or less, and continue to ensure signal integrity. IEEE 802.3az specifies a mechanism for reducing power consumption when a link is idle. It is known as “Energy Efficient Ethernet (EEE).”

The power-saving methods provided by this switch include this EEE power saving feature when there is no activity on a link: Under normal operation, the switch continuously auto-negotiates to find a link partner, keeping the MAC interface powered up even if no link connection exists. When using power-savings mode, the switch checks for energy on the circuit to determine if there is a link partner. If none is detected, the switch automatically turns off the transmitter, and most of the receive circuitry (entering Sleep Mode). In this mode, the low-power energy-detection circuit continuously checks for energy on the cable. If none is detected, the MAC interface is also powered down to save additional energy. If energy is detected, the switch immediately turns on both the transmitter and receiver functions, and powers up the MAC interface.

This feature is “Off” by default. To enable the feature on a particular port use the following command:

```
input "interface ex <interface-id>".
SMIS(config)# interface ex 0/1
input "EEE mode" and then input "exit".
SMIS(config-if)# EEE mode
SMIS(config-if)# exit
```

To confirm that the port is configured for EEE:

```
input "show interface ex <interface-id>".
SMIS(config)# show interface ex 0/1
```

To disable this feature:

```
input "interface ex <interface-id>".
SMIS(config)# interface ex 0/1
input "no EEE mode" and then input "exit".
SMIS(config-if)# no EEE mode
SMIS(config-if)# exit
```

To confirm that EEE is disabled on the port:

```
input "show interface ex <interface-id>".
```

```
SMIS(config)# show interface ex 0/1
```

## 3.73 monitor session

This command enables port-mirroring in the switch and the no form of the command disables port mirroring in the switch.

```
monitor session [session_number 1-1] { destination interface  
<interface-type> <interface-id> | source interface <interface-type>  
<interface-id> [{ rx | tx | both }] }
```

```
no monitor session [session_number:1] [{ source interface <interface-  
type> <interface-id> | destination interface <interface-type><interface-  
id > }]
```

### Syntax Description

**session\_number 1-1** - Specifies the session number identified with the session

**destination interface** - Specifies the destination interface or the mirror-to port. Valid interfaces are physical ports. There can only be one mirror-to port per switch.

**source interface** - Specifies the interface for the traffic that is to be mirrored. Valid interfaces include physical ports.

**Rx** - Received traffic is mirrored

**Tx** - Transmitted traffic is mirrored

**Both** - Specifies the traffic direction to monitor. If the traffic direction is not specified, both transmitted and received traffic is mirrored.

### Mode

Global Configuration Mode

### Defaults

Port Mirroring is disabled

### Example:

```
SMIS(config)# monitor session source interface gigabitEthernet 0/2
```

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

### Related Command

**show port-monitoring** - Displays port-monitoring information



## 3.74 hol blocking prevention

This command enables the Head-Of-Line blocking prevention on the interface and the no form of the command disables the same.

**hol blocking prevention**

**no hol blocking prevention**

### **Mode**

Interface Configuration Mode

### **Defaults**

Enabled

### **Example:**

```
SMIS(config-if)#hol blocking prevention
```

## 3.75 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 packets per second.

### Mode

Interface Configuration Mode

### Defaults

Broadcast, multicast, and dlf storm control are disabled.

### Example:

```
SMIS(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

## 3.76 rate-limit

This command configures the egress rate limiting and burst size for the physical interfaces. The given rate and burst size values are adjusted to the closest possible value supported by the hardware. The no form of this command disables the rate limiting on the interface.

```
rate-limit output <rate-value-kbps (1-10000000)> <burst-value-kbits (1-10000000)>
```

```
no rate-limit output
```

### Syntax Description

**rate-value-kbps** - Any number between 1 to 10000000 in kbps.

**burst-value-kbits** - Any number between 1 to 10000000 in kbits

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# rate-limit output 10000000 10000
```

### Related Command

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

## 3.77 snmp trap link-status

This command enables trap generation on either the physical interface or the port-channel interface. The no form of this command disables trap generation on the respective interface.

**snmp trap link-status**

**no snmp trap link-status**

### Mode

Interface Configuration Mode

### Defaults

SNMP trap link status is enabled by default

### Example:

```
SMIS(config-if)# snmp trap link-status
```

### Related Command

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

## 3.78 reset interface statistics

This command resets the interface counters to zero for the given interface. If no interface given, it resets the counters for all the interfaces.

```
reset interfaces [ <interface-type> <interface-id> ] statistics
```

### Syntax Description

**interface-type** - Interface type (gigabit-ethernet, extreme-ethernet, qx-ethernet)

**interface-id** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# reset interfaces statistics
```

### Related Command

**show interfaces counters** - Displays the interface counters

## 3.79 **reset interface cpu statistics**

This command resets the CPU counters to zero for the given interface. If no interface given, it resets the CPU counters for all the interfaces.

```
reset interfaces [ <interface-type> <interface-id> ] cpu statistics
```

### **Syntax Description**

**interface-type** - Interface type (gigabit-ethernet, extreme-ethernet, qx-ethernet)

**interface-id** - Physical interface ID including slot and port number

### **Mode**

Privileged EXEC Mode

### **Example:**

```
SMIS# reset interfaces cpu statistics
```

### **Related Command**

**show interfaces cpu counters** - Displays the CPU counters

## 3.80 single-blade-slot-num

This command configures the given slot numbers as the single blade servers in SBM-XEM-X10S software. This helps the switch software to correct port numbers internally to display correct port names.

By default all the slots are considered as twin server blade slots in the SBM-XEM-X10S switch software. The User must configure the slot numbers that are used for single server blades in SBM-XEM-X10S software using this command.

The “no” form of this command configures the given slots back to default twin blade server slot types.

**single-blade-slot-num <slot number (1-10)>**

**no single-blade-slot-num <slot number (1-10)>**

### Syntax Description

**slot number** – One or more values between 1 and 10.  
The slot number could be a single slot number like 2 or 3.  
Or it could be a range like 2-5.  
Or it could be multiples separated by commands like 2,3,8-9

### Mode

Global Configuration Mode

### Example:

```
SMIS# single-blade-slot-num 1-3
```

### Related Command

**show single-blade-slot-num** - Displays the single blade server slots configuration.

### Note:

1. After configuring this command, the user must save the configuration using the “write startup-config” command and reload the switch.
2. When ever the user moves the servers across different slots, or adds or removes servers, the user must make sure that the switch configuration for single blade servers is correct. If needed, the user must configure the single blade server slots correctly in the switch using this command

## 3.81 split40g

The **split40g** command configures the split of 40Gbps QX ports. The command syntax is given below.

```
split40g mode <number>
```

### Syntax Description

**number** – The number of QX ports to be split. The possible values are explained below.

0 - The default value is 0. It means “no split, all QX ports operated in 40Gig speed”. To remove an existing split configuration, the user can use 0 as a parameter.

1 – This will configure a split of the QX1 port as four 10Gbpsports.

2 – In the X3348S or X3348SR models, this will configure a split of the QX1 and QX2 ports as 10Gbps ports. In the X3348T or X3348TR models, this will configure a split of QX1 and QX3 ports as 10Gbps ports.

3 – In the X3348S or X3348SR models, this will configure a split of the QX1, QX2 and QX3 ports as 10Gbps ports. In the X3348T or X3348TR models, this will configure a split of QX1, QX3 and QX4 ports as 10Gbps ports.

### Mode

Privileged EXEC Mode

### Defaults

0 – No split

### Example:

To split the QX1 port into four 10Gbps ports:

```
SMIS# split40g mode 1
```

### Related Command

**show split40g mode** - Displays split configuration information

**show system information** - Displays split configuration information

### Note:

1. This command is supported only in SSE-X3348S(R) and SSE-X3348T(R) model switches.
2. This command will be effective only after saving the configuration and reloading the switch.



## 3.82 show single-blade-slot-num

This command displays the single blade slots configuration in the SBM-XEM-X10SM switch.

```
show single-blade-slot-num
```

### Syntax Description

#### Mode

Privileged EXEC Mode

### Related Commands

**single-blade-slot-numinterface** - Configures the single blade slot numbers in SBM-XEM-X10SM switch.

## 3.83 `show split40g`

This command displays the 40Gbps ports split configuration in the SSE-X3348S(R) and SSE-X3348T(R) switches.

```
show split40g
```

### **Syntax Description**

#### **Mode**

Privileged EXEC Mode

### **Related Commands**

`split40g` - Configures the split of 40Gbps QX ports as 10Gbps ports.

## show ip interface

This command displays the IP interface configuration.

```
show ip interface [Vlan <vlan-id(1-4069)>] [<interface-type>
<interface-id>] [loopback <loopback-id(1-100)>]
```

### Syntax Description

**vlan** - VLAN Identifier any number between 1 to 4069

**interface-type** - Interface type, can either be a gigabit Ethernet or extreme Ethernet (10Gig) or qx Ethernet (40Gig) interface.

**interface-id** - Physical interface ID including slot and port number.

**loopback** - Loopback interface ID any number between 1 to 100

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip interface
vlan1 is up, line protocol is up
Internet Address is 12.0.0.2/8
Broadcast Address 12.255.255.255
Secondary Address 12.0.0.10/8
Secondary Address 13.0.0.10/
```

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

### Related Commands

**interface** - Configures an interface, which can be a physical interface or a port-channel interface or a VLAN interface

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

## 3.84 show interfaces

This command displays the interface status and configuration.

```
show interfaces [{ [<interface-type> <interface-id>] [{ description |
stormcontrol | flowcontrol | status }] | vlan <vlan-id(1-4069)> | port-
channel <port-channel-id (1-65535)>}]
```

### Syntax Description

**interface-type** - Can be gigabit Ethernet (gi) or extreme Ethernet (ex) or qx-ethernet (qx)

**interface-id** - Physical interface ID including slot and port number

**description** - Description about the interface

**storm-control** - Broadcast, multicast, and unicast storm control suppression levels for an interface

**flowcontrol** - Receive or send flow control value for an interface

**status** - Status of the interface

**vlan** - VLAN Identifier

**port-channel** - Port Channel Identifier

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show interfaces gigabitethernet 0/2
Gi0/2 up, line protocol is up (connected)
Hardware Address is 00:01:02:03:04:22
RARP Client is enabled
MTU 1500 bytes, Full duplex, 100 Mbps, Auto-Negotiation
Input flow-control is off, output flow-control is off
Link Up/Down Trap is enabled
Reception Counters
Octets : 739284
Unicast Packets : 0
Non Unicast Packets : 5963
Discarded Packets : 0
Error Packets : 0
```

```
Unknown Protocol : 5963
Transmission Counters
Octets : 741775
Unicast Packets : 0
Non Unicast Packets : 5985
Discarded Packets : 0
Error Packets : 0
```

```
SMIS# show interfaces description
Interface Status Protocol Description
```

```
-----
Gi0/1 up up
Gi0/2 up up
```

```
SMIS# 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
```

```
SMIS# show interfaces gigabitethernet 0/2 flow-control
Port Tx FlowControl Rx FlowControl Tx Pause Rx Pause
```

```
-----
Gi0/2 off off 0 0
```

```
SMIS# show interfaces vlan 1
vlan1 up, line protocol is up (connected)
```

```
SMIS# show interfaces port-channel 2
po2 up, line protocol is up (connected)
```

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

### Related Commands

**storm-control** - Sets storm control rate for broadcast, multicast and DLF packets

**interface** - Configures an interface which can be a physical interface or a port-channel interface or a vlan interface

**flowcontrol** - Enables flow-control

**show flow-control** - Displays the flow-control information

### 3.85 show interfaces - counters

This command displays the interface statistics for each port.

**show interfaces** [{ <interface-type> <interface-id>] **counters**

**Syntax Description**

**interface-type** - Can be gigabit Ethernet (gi) or extreme Ethernet (ex) or qx-ethernet (qx)

**interface-id** - Physical interface ID including slot and port number

**counters** - Various counters for the switch or for the specific interface

**Mode**

Privileged EXEC Mode

**Example:**

```
SMIS# show interfaces counters
Port InOctet InUcast InNUcast InDiscard InErrs
-----
Gi0/1 943141 0 10910 0 0Gi0/2 743996
0 6001 0 0
vlan1 54987 0 8002 0 0
```

- ➡ If executed without the optional parameters this command displays the counters for all the available interfaces.

**Related Command**

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

## 3.86 show interfaces loopback

This command displays the loopback interface status and configuration.

```
show interfaces loopback <1-100>
```

### Syntax Description

**loopback** - Loopback interface ID

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show interfaces loopback 10
```

### Related Command

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



## 3.87 show interfaces cpu counters

This command displays the statistics of CPU traffic.

```
show interfaces [ <interface-type> <interface-id> ] cpu counters
```

### Syntax Description

**interface-type** - Can be gigabit Ethernet (gi) or extreme Ethernet (ex) or qx-ethernet (qx)

**interface-id** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show interfaces cpu counters
```

### Related Command

**show interfaces counters** - Displays the physical interface counters

## 3.88 show interface mtu

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

```
show interface mtu [{ Vlan <vlan-id (1-4069)> | port-channel <port-  
channel-id (1-65535)> | <interface-type> <interface-id> }]
```

### Syntax Description

**vlan** - VLAN Identifier

**port-channel** - Port Channel Identifier

**interface-type** - Can be **gigabit Ethernet (gi)** or **extreme Ethernet (ex)**  
or **qx-ethernet (qx)**

**interface-id** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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

## 3.89 show conf

This command shows the interface specific running configuration details

**show conf**

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# show conf
```

### Related Command

**show running-config** – Displays the running configuration

## 3.90 show port-monitoring

This command displays port-monitoring information.

**show port-monitoring**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show port-monitoring
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** - Enables port-mirroring in the switch

## 3.91 show flow-control

This command displays the flow-control information.

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

### Syntax Description

**interface-type** - Can be gigabit Ethernet (gi) or extreme Ethernet (ex) or qx-ethernet (qx)

**interface-id** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show flow-control interface gigabitethernet 0/2
```

```
Port Tx FlowControl Rx FlowControl Tx Pause RxPause
```

```
-----
```

```
Gi0/2 off off 0 0
```

If this command is executed without the optional parameter it displays the flow control information of the **SMIS** router. Otherwise it displays the flow control information of the specified interface.

### Related Commands

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

**flowcontrol** - Enables flowcontrol on an interface

## 3.92 show transceiver

This command displays the information about fiber optic transceiver modules.

This command is supported only on the following switch models

SSE-X24S

SSE-X24SR

SSE-X3348S

SSE-X3348SR

SSE-X3348T

SSE-X3348TR

```
show transceiver [interface <interface-type> <interface-id>]
```

### Syntax Description

**interface-type** - Interface type, e.g: ex.

**interface-id** - Physical interface ID including slot and port number.

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show transceiver interface ex 0/1
```

## 3.93 show transceiver diagnostics

This command displays the information about fiber optic transceiver modules.

This command is supported only on the following switch models

SSE-X2C

SSE-X2C+

SSE-X3S+

SSE-X24S

SSE-X24SR

SSE-X3348S

SSE-X3348SR

SSE-X3348T

SSE-X3348TR

```
show transceiver diagnostics [interface <interface-type> <interface-id>]
```

### Syntax Description

**interface-type** - Interface type, e.g: ex.

**interface-id** - Physical interface ID including slot and port number.

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show transceiver diagnostics
```

```
SMIS# show transceiver diagnostics interface ex 0/1
```

## 3.94 show meminfo

This command displays the memory status and utilization on the switch.

**show meminfo**

### **Mode**

Privileged EXEC Mode

### **Example:**

```
SMIS# show meminfo
```



## 3.95 device name

This command configures the switch name string. The default device name is SMIS.

**device name** <devname>

### Syntax Description

<devname] - Any string up to 15 characters length.

### Mode

Global Configuration Mode

### Default

SMIS

### Example:

```
SMIS(config)# device name san_sw_1
san_sw_1(config)#
```

### Related commands

show system information - Displays the switch name along with other system parameters.

## 3.96 system location

This command configures the switch location information string. The default device name is Supermicro.

**system location** <location name>

### Syntax Description

<location name] - Any string up to 255 characters length.

### Mode

Global Configuration Mode

### Default

Supermicro

### Example:

```
SMIS(config)# system location dc1_2ndfloor
```

### Related commands

show system information - Displays the switch location along with other system parameters.

## 3.97 system contact

This command configures the switch contact information. The default contact information is <http://www.supermicro.com/support>.

**system contact** <contact name>

### Syntax Description

<contact name] - Any string up to 255 characters length.

### Mode

Global Configuration Mode

### Default

<http://www.supermicro.com/support>

### Example:

```
SMIS(config)# system contact Michael
```

### Related commands

show system information - Displays the switch location along with other system parameters.

## 3.98 set boot-up

This command configures the next bootup firmware image selection. The default bootup image selection is normal image. User can use this command to boot the switch from fallback image on next reboot.

```
set boot-up {normal | fallback}
```

### Syntax Description

**normal** - Switch boots using normal firmware image on next reboot

**fallback** - Switch boots using fallback firmware image on next reboot

### Mode

Global Configuration Mode

### Default

normal

### Example:

```
SMIS(config)# set boot-up fallback
```

### Related commands

`show system information` - Displays the next boot image selection information along with other system parameters.

## 3.99 reload

This command restarts the switch.

```
reload [ <switch-id> | all] [force]
```

### Syntax Description

**<switch-id>** - In stacking, the required particular switch can be restarted by specifying switch id.

**all** – Use this option to restart all switches in stacking.

**force** – Use this option for a forced restart. When you are trying to restart right after a firmware upgrade of write startup config in stacking environment, you will be prompted to wait to restart the switch until the files are transferred to all slave switches in stacking. To overwrite this waiting and restart forcefully, this option is used.

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# reload
```

## 3.100 reset-to-factory-defaults

This command clears all the configurations on the switch and resets the switch to factory defaults configurations.

➡ This command will reboot the switch.

```
reset-to-factory-defaults [ switch <switch-id> | all]
```

### Syntax Description

**<switch-id>** - In stacking, the required particular switch can be reset to factory defaults by specifying the switch id.

**all** - Use this option to restart all switches in stacking to factory defaults

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# reset-to-factory-defaults
```

## 3.101 mac-address-table aging-time

This command sets the maximum age of a dynamically learnt entry in the MAC address table. The no form of the command sets the maximum age of an entry in the MAC address table to its default value.

```
mac-address-table aging-time <1-1000000 seconds>
```

```
no mac-address-table aging-time
```

### Mode

Global Configuration Mode

### Defaults

300

### Example:

```
SMIS(config)# mac-address-table aging-time 100
```

If traffic on an interface is not very frequent, then the aging time must be increased to record the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding.

### Related Command

```
show mac-address-table aging-time - Displays the MAC address-table ageing time
```

## 3.102 copy debug-logging

This command writes the debug logs to a remote site or to external USB memory.

```
copy debug-logging { tftp://ip-address/filename | usb:filename }
```

### Syntax Description

**tftp** - Copies a log file to a TFTP server

**ip-address** - the IP address or host name of the TFTP server to receive the file

**filename** - the name assigned to the file on the server

**usb:filename** - Copies the log file to this file name in external usb memory.

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# copy debug-logging tftp://10.0.0.10/clcliser
```



## 3.103 debug-logging

This command configures where debug logs are to be displayed and the no form of the command displays debug logs in the console.

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

```
no debug-logging
```

### Syntax Description

**console** - Debug logs are displayed in the Console

**file** - Debug logs are displayed in the file

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# debug-logging console
```

Debug logs are directed to the console screen or to a buffer file, which can later be uploaded, based on the input.

### Related Commands

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

**show debugging** - Displays state of each debugging option

## 3.104 no startup-config

This command makes no configuration file will be loaded in next reboots of the switch.

**no startup-config**

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# no startup-config
```

### Related Commands

set startup-config <file name> - Set the file which will be restored on next reboot of the switch.

## 3.105 show system information

This command displays system information.

**show system information**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show system information
```

```
Switch Name                : SMIS
Serial Number              : MD29S00189
Switch Base MAC Address    : 00:30:48:90:00:e2
Default IP Address         : 10.0.0.1
Default Subnet Mask        : 255.0.0.0
Default IP Address Config Mode : Manual
Default IP Address Allocation Protocol : DHCP
SNMP EngineID             : 80.00.08.1c.04.46.53
System Contact             : support@supermicro.com
System Location            : SUPERMICRO
Logging Option             : Console Logging
Login Authentication Mode  : Local
PIM Mode                   : Dense Mode
Snoop Forward Mode         : MAC based
Config Restore Status      : Successful
Config Restore Option      : Restore
Config Restore Filename    : iss1.conf
Config Save IP Address     : 0.0.0.0
NTP Broadcast Mode        : No
```

### 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

## 3.106 show version

This command displays hardware and firmware versions.

In stacking mode, this command displays the version numbers for all the switches connected in the stack.

**show version**

**Mode:**

Privileged EXEC Mode

**Example::**

SMIS# show version

Switch ID	Hardware Version	Firmware Version	OS Version
0	P1-01	1.0.17-3	1019

SMIS#

## 3.107 show debug-logging

This command displays the debug logs stored in file.

**show debug-logging**

**Mode:**

Privileged EXEC Mode

**Example::**

```
SMIS(config)# debug-logging file
```

```
SMIS(config)# exit
```

```
SMIS# debug spanning-tree events
```

```
SMIS# 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).
```

**Related Command:**

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

## 3.108 show debugging

This command displays state of each debugging option.

**show debugging**

**Mode:**

Privileged EXEC Mode

**Example::**

```
SMIS# 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 module-wise debug traces for VLAN

**debug garp** - Enables module-wise debug traces for GARP

**debug ip dhcp client** - Sets the debug level for tracing the DHCP client module

**debug ip dhcp relay** - Enables the debug level for tracing the DHCP Relay Module

**debug ip dhcp server** - Enables the debug level for tracing the DHCP server Module

**debug ethernet-oam** - Enables/displays the debug level for the EOAM Module

## 3.109 show system acknowledgement

This command displays the acknowledgement text for the open source components used on the switch software.

**show system acknowledgement**

### **Mode**

Privileged EXEC Mode

### **Example:**

```
SMIS# show system acknowledgement
```

## 3.110 show system environment

This command displays the temperature, fan status and power supply status information.

This command is supported only on the following switch models

SSE-X24S

SSE-X24SR

SSE-X3348S

SSE-X3348SR

SSE-X3348T

SSE-X3348TR

```
show system environment [{temperature | fan | power}]
```

### Syntax Description

**temperature** – Displays temperature readings from temperature sensors

**fan** – Displays fan status

**fan** – Displays power supply status

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show system environment temperature
```



## 3.111 show tech-support

This command displays various information that are useful for troubleshooting.

`show tech-support`

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Example:

```
SMIS# show tech-support
```

## 4 Stacking

Stacking is supported on only the following Super Micro Intelligent units:

**SBM-GEM-X2C**  
**SBM-GEM-X2C+**  
**SSE-G24-TG4**  
**SSE-G48-TG4**

Stacking is not supported on the 10G Ethernet switches:

**SBM-XEM-X10SM**  
**SSE-X24S**  
**SSE-X24SR**  
**SSE-3348S**  
**SSE-3348SR**  
**SSE-3348T**  
**SSE-3348TR**

Switch stacking is created by connecting switches in a daisy chain. One of the stacked switches is selected as the “Master” based on configuration. The Master switch provides management support for the entire stack. Other switches in the stack are referred to as “Slave” switches.

- ➡ Make sure all stacked switches run the same version of firmware.

The Master Switch manages the control plane traffic for all stacked switches. When a current Master Switch fails, the backup Master is selected as the current Master. The Master selection algorithm is based on a priority configuration. If two switches have the same priority the switch with the lowest MAC address gets selected as the Master Switch.

### Stacking Cabling

Stacking is supported with CX-4 cables only. Use only CX4 cables from Supermicro: CBL-0474L for 1-meter and CBL-0389L-01 for 3-meter. The CX-4 cable used for stacking should be no more than 3M in length. This is because stacking internally runs at 12Gbps and therefore requires a more robust signal than longer cable lengths might provide reliably. The industry standard stacking cable length is 3M.

**Note:** For stacking ports, you do not need to configure CX4 cable length. It is fixed as “short” for stacking ports.

**Warning:** Use of CX4 cables from suppliers other than Supermicro for stacking is not supported by Supermicro.

When used for 10G Ethernet uplinks, the CX-4 ports can be from 1M to 12M in length; the maximum CX-4 cable length supported on Supermicro switches is 12M.

It is acceptable to use a 1M stacking cable for port 1 and a 12M uplink cable for port 2. You will only need to configure the long cable preference for port 2. The way to configure this is:

```
SMIS# config term
SMIS(config)# int ex 0/2
SMIS(config-if)# cx4-cable-length long
```

This configuration is done on an individual port basis. Thus, you can use “short” for one port and “long” for the other port. Alternatively you might use both “short” or, if neither port is used for stacking, both can be “long” cables.

### Enabling Stacking

Super Micro switches by default act as stand alone switches. This standalone default facilitates using 10G Ethernet ports as **Extreme Ethernet** ports for uplinks.

When stacking is enabled the stacking ports are dedicated for stacking purpose.

Stacking can be enabled by using the command “stack” with a switch identifier and a priority. The detailed command syntax is explained below:

- ➡ When stacking is enabled, the switch needs to be rebooted to take it effective.
- ➡ When a switch is acting as a stand-alone switch with stacking disabled, all physical interfaces are numbered as 0/1 to 0/n. When the switch is in stacking mode, the interfaces are numbered as <switch id>/1 to <switch id> / n. In non-stacking mode, the switch id is considered to be 0.
- ➡ In the stacking mode, any firmware upgrade in the Master Switch will automatically initiate a firmware upgrade to all attached stack member switches. Firmware upgrade confirmation from stack member switches will be displayed in the Master Switch management interface.
- ➡ In the stacking mode, the user can reload all stacked switches or any selected stack member switch from the master management interface.

The interface numbers change between stacking and non stacking cases due to the switch id. Hence configurations saved for stacking are not valid for non stacking cases and vice versa.

- ➡ If the user chooses stacking using the “stack” command while the switch is in a non-stacking state and if the configurations are already saved for restoring; the switch will rename the configuration file by adding a suffix `_nonstack` and will not restore this file when the switch reboots with stacking enabled.

- ▶ Similarly if the user chooses non-stacking using the “no stack” command while the switch is in a stacking state and if the configurations are already saved for restoring; the switch will rename the configuration file by adding a suffix `_stack` and will not restore this file when the switch reboots with stacking disabled.

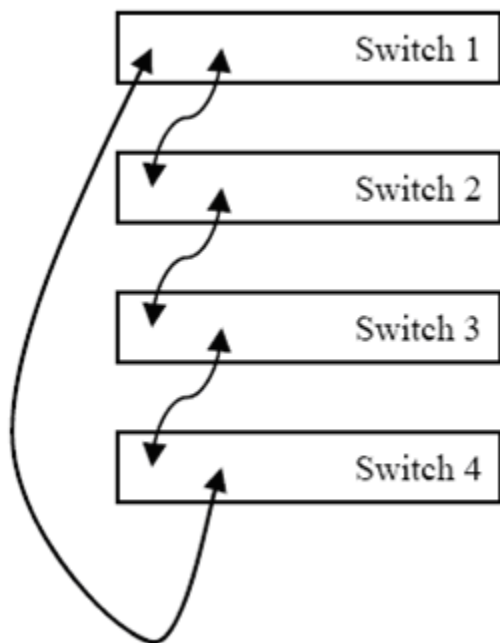
## Adding Stacking Members

Connect the stacked switches using stacking cables. For better redundancy, connect the switches as a daisy chain as shown in the diagram below. This chain connectivity helps to maintain stacking in the case of a single link or switch failure.

Before connecting switches in stacking make sure stacking is enabled in all switches and that switch identifiers and priorities are configured properly.

There is no specific configuration required to add stack switches. If two stacking enabled switches connected through stacking cables, they form the stack.

- Do not use the same switch id for multiple switches on the stack.



- Only one master switch user is allowed to configure a stack. The slave switches will not allow you to configure anything except *stacking disabled*. To login to slave switches, use a login name such as “stackuser” and a password like “stack123”.

## Removing a stacked switch

To remove a switch from stacking follow the below recommended procedure:

1. Disconnect stacking cables.
  2. Reboot the removed switch as a stand-alone switch.
  3. Execute “no stack” command.
  4. Reboot the switch again to operate as regular stand-alone switch.
- ➡ When a switch is moved from stacking to stand-alone mode, the saved stacking configurations can not loaded in stand alone mode. When the “no stack” command is issued, the switch software will rename the existing configuration file to avoid automatic restoration of stacking configurations on a stand-alone switch.

## 4.1 Stack

This command enables stacking and helps configuring stacking ports, priority and switch identifier.

```
stack { priority {PM | BM | PS} } {switchId <NodeId (1-16)>} {ports  
<xg1,xg2,..>}
```

```
no stack
```

### Syntax Description

**priority** – Priority of the switch to decide the master among stacked switches. PM denotes preferred master. BM denotes backup master. PS denotes preferred slave.

**switchId** - Unique number to identify switches. Make sure to use different switch identifier for stack member switches.

**ports** – The list of stacking ports as xg1, xg2..... It is recommended to use two ports for stacking to connect all stacking switches in daisy chain.

### Mode

Privileged EXEC Mode

### Defaults

Stacking is disabled.

### Example:

```
SMIS# stack priority PM switched 1 ports xg3, xg4.
```

### Related Commands

**show stackbrief** – Displays summarized stack information

**show stack details** - Displays stack details

**show stack counters** - Displays stack port statistics

**show stack switchid** - Displays stack details for particular switch.

**show stack link status** – Displays the stacking interface link status.

## 4.2 Show stack brief

This command displays the following stacking information:

Switch Id

Stack Ports

Switch Priority

Switch State

Also Switch ID and Status for all connected stack peer switches.

**show stack brief**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Defaults

Stacking is disabled.

#### Example:

```
SMIS# show stack brief
```

### Related Commands

**stack** – Configures switch identifier, priority and stacking ports.

**show stack details** - Displays stack details

**show stack counters** - Displays stack port statistics

**show stack switchid** - Displays stack details for particular switch.

**show stack link status** – Displays the stacking interface link status.



## 4.3 Show stack details

This command displays the stacking details.

**show stack details**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Defaults

Stacking is disabled.

#### Example:

```
SMIS# show stack details
```

### Related Commands

**stack** – Configures switch identifier, priority and stacking ports.

**show stack brief** – Displays summarized stack information

**show stack counters** - Displays stack port statistics

**show stack switchid** - Displays stack details for particular switch.

**show stack link status** – Displays the stacking interface link status.

## 4.4 Show stack counters

This command shows the port counter statistics for stacking ports.

**show stack counters**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Defaults

Stacking is disabled.

#### Example:

```
SMIS# show stack counters
```

### Related Commands

**stack** – Configures switch identifier, priority and stacking ports.

**show stack brief** – Displays summarized stack information

**show stack details** - Displays stack details

**show stack switchid** - Displays stack details for particular switch.

**show stack link status** – Displays the stacking interface link status.

## 4.5 Show stack switchid

This command displays the details of particular switch stacking member.

```
show stack switched <id>
```

### Syntax Description

**id** – switch identifier

### Mode

Privileged EXEC Mode

### Defaults

Stacking is disabled.

### Example:

```
SMIS# show stack switchid
```

### Related Commands

**stack** – Configures switch identifier, priority and stacking ports.

**show stack brief** – Displays summarized stack information

**show stack details** - Displays stack details

**show stack counters** - Displays stack port statistics

**show stack link status** – Displays the stacking interface link status.

## 4.6 Show stack link status

This command displays the stack interface link status.

**show stack link status**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Defaults

Stacking is disabled.

#### Example:

```
SMIS# show stack link status
```

### Related Commands

**stack** – Configures switch identifier, priority and stacking ports.

**show stack brief** – Displays summarized stack information

**show stack details** - Displays stack details

**show stack counters** - Displays stack port statistics

**show stack switchid** - Displays stack details for particular switch.

## 5 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 enable](#)

[logging disable](#)

[logging ip](#)

[logging buffered](#)

[logging console](#)

[logging facility](#)

[logging trap](#)

[logging file](#)

[cmdbuffs](#)

[service timestamps](#)

[clear logs](#)

[show logging](#)

[show logging file](#)



## 5.1 logging enable

This command enables the syslog feature.

Syslog feature is enabled by default.

**logging enable**

### Mode

Global Configuration Mode

### Defaults

enable

### Example:

```
SMIS(config)# logging enable
```

### Related Commands

**show logging** - Displays Logging status and configuration information

## 5.2 logging disable

This command disables the syslog feature.

Syslog feature is enabled by default.

**logging disable**

### Mode

Global Configuration Mode

### Defaults

enable

### Example:

```
SMIS(config)# logging disable
```

### Related Commands

**show logging** - Displays Logging status and configuration information



## 5.3 logging ip

This command enables Syslog server and configures the Syslog Server IP address.

The no form of the command disables Syslog server and re-sets the configured Syslog server IP address

```
logging <ip-address>
```

```
no logging <ip-address>
```

### Syntax Description

**ip-address** - Host IP address used as a Syslog server

### Mode

Global Configuration Mode

### Defaults

Logging - on

IP address - None

### Example:

```
SMIS(config)# logging 12.0.0.2
```

### Related Command

**show logging** - Displays Logging status and configuration information

## 5.4 logging buffered

This command enables logging to syslog buffers and configures the number of buffers to be used to store syslog messages.

The no form of the command resets the number of buffers to its default value 50.

```
logging buffered <size (1-200)>
```

```
no logging buffered buffer-size
```

### Syntax Description

**buffered** - Limits Syslog messages displayed from an internal buffer

### Mode

Global Configuration Mode

### Defaults

buffers - 50

### Example:

```
SMIS(config)# logging buffered 100
```

### Related Command

**show logging** - Displays Logging status and configuration information

## 5.5 logging console

This command enables the display of syslog messages in to console terminal.

The no form of the command disables the console logging.

**logging console**

**no logging console**

### Syntax Description

**console** - Enables syslog messages logged to the console

### Mode

Global Configuration Mode

### Defaults

Console - disabled

### Example:

```
SMIS(config)# logging console
```

### Related Command

**show logging** - Displays Logging status and configuration information

## 5.6 logging facility

This command configures the syslog facility sent on syslog messages. The no form of this command configure the syslog facility to the default value local0.

```
logging facility {local0 | local1 | local2 | local3 | local4 | local5 |  
local6 | local7| user}
```

```
no logging { <ip-address> | buffered | console | facility | trap | on }
```

### Syntax Description

**facility** - The facility that is indicated in the message. This can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7 or user.

### Mode

Global Configuration Mode

### Defaults

facility – local0

### Example:

```
SMIS(config)# logging facility local1
```

### Related Command

**show logging** - Displays Logging status and configuration information

## 5.7 logging trap

This command configures the syslog trap level. The no form of this command resets the syslog trap level to its default value critical.

```
logging trap [{ <level (0-7)> | alerts | critical | debugging |  
emergencies | errors | informational | notification | warnings }]
```

```
no logging trap
```

### Syntax Description

**trap** - Trap messages

### Mode

Global Configuration Mode

### Defaults

Trap - critical

### Example:

```
SMIS(config)# logging trap informational
```

### Related Command

**show logging** - Displays Logging status and configuration information

## 5.8 logging file

This command enables logging of syslog messages in to a file. The no form of the command disables file logging.

The log file is stored in ASCII text format.

```
logging file <filename> max-entries <short (1-8000)>
```

```
no logging file
```

### Syntax Description

**filename** - Name of the file to which syslog messages are written

**max-entries** - Maximum number of syslog messages that can be written on the file. Once this number is reached the file wrapped to overwrite the oldest entries.

### Mode

Global Configuration Mode

### Defaults

File logging is not enabled.

### Example:

```
SMIS(config)# logging file sw1_log max-entries 5000
```

### Related Command

**show logging** - Displays Logging status and configuration information

**show logging file** - Displays syslog messages stored on the file

## 5.9 cmdbuffs

This command configures the number of syslog buffers for a particular user.

```
cmdbuffs <user name> <no.of buffers (1-200)>
```

### Syntax Description

**user name** - User Name

**no.of buffers** - Number of log buffers to be allocated in the system

### Mode

Global Configuration Mode

### Defaults

50

### Example:

```
SMIS(config)#cmdbuffs supermicro 50
```

CLI related events like commands given by the user, login/logout etc can be logged on to the Syslog Server.

### Related Commands

**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

## 5.10 service timestamps

This command enables timestamp option for logged messages and the no form of the command disables timestamp option for logged messages.

**service timestamps**

**no service timestamps**

### Mode

Global Configuration Mode

### Defaults

Enabled

### Example:

```
SMIS(config)#service timestamps
```

When enabled, the messages (log and email alert messages) will hold the time stamp information.

When disabled, the time stamp information will not be carried with the messages sent to the log and mail servers

### Related Commands

**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



## 5.11 clear log buffer

This command clears the system syslog buffers.

**clear log buffer**

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# clear log buffer
```

### 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

## 5.12 clear log file

This command clears all the syslog messages from the syslog file.

**clear log file**

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# clear log file
```

### 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

## 5.13 show logging

This command displays logging status and configuration information.

**show logging**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show logging
System Log Information
-----
Syslog logging : enabled
Console logging : enabled
TimeStamp option : enabled
Trap logging : Critical
Log server IP : 10.0.0.1
Facility : Default (Mail)
Buffered size : 100
```

### Related Commands

**logging** - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter

**service timestamps** - Enables timestamp option for logged messages

## 5.14 show logging file

This command displays syslog messages from syslog file.

```
show logging file
```

### **Mode**

Privileged EXEC Mode

### **Example:**

```
SMIS# show logging file
```

```
LogFile(4 Entries)
```

```
<134> Nov 17 17:01:59 2012:CLI-6:User logged out
```

```
<134> Nov 17 17:02:08 2012:CLI-6:Login failed : Login incorrect AA
```

```
<134> Nov 17 17:02:10 2012:CLI-6:Login failed : Login incorrect BB
```

```
<134> Nov 17 17:02:13 2012:CLI-6:User ADMIN logged in
```

### **Related Commands**

**logging file** - Enables writing syslog messages into a log file

## 6 SSH

SSH 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](#)

[debug ssh](#)

[show ip ssh](#)

## 6.1 ip ssh

This command enables SSH server on the device and also configures the various parameters associated with SSH server. The no form of the command disables SSH server on the device and also re-sets the various parameters associated with SSH server.

```
ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth
([hmacmd5] [hmac-sha1]) }
```

```
no ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth
([hmac-md5] [hmac-sha1]) }version
```

### Syntax Description

**Compatibility** - The support for the SSH protocol version

**Cipher** - The cipher-algorithm list

**Auth** - Public key authentication for incoming SSH sessions

### Mode

Global configuration Mode

### Defaults

version compatibility - false

cipher - 3des-cbc

auth - hmac-sha1

### Example:

```
SMIS(config)#ip ssh version compatibility
```

```
SMIS(config)# ip ssh cipher des-cbc
```

When version compatibility is set to TRUE, both SSH version-1 and SSH version-2 will be supported. When set to FALSE, SSH version-2 only will be supported. The cipher list takes values as bit mask. Setting a bit indicates that the corresponding cipher-list will be used for Encryption. The auth takes values as bit mask. Setting a bit indicates that the corresponding MAC-list will be used for authentication.

### Related Command

**show ip ssh** - Displays SSH server information

## 6.2 debug ssh

This command sets the given trace levels for SSH and the no form of the command re-sets the given SSH trace level.

```
debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource]
[buffer])
```

```
no debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource]
[buffer])
```

### Syntax Description

**all** - Initialization and Shutdown Messages

**shut** - Shutdown Messages

**mgmt** - Management Messages

**data** - Data Path Messages

**ctrl** - Control Plane Messages

**dump** - Packet Dump Messages

**resource** - Messages related to all resources except Buffers

**buffer** - Buffer Messages

### Mode

Privileged EXEC Mode

### Defaults

Debugging is Disabled

### Example:

```
SMIS# debug ssh all
```

Setting all the bits will enable all the trace levels and resetting them will disable all the trace levels.

### Related Command

**show ip ssh** - Displays SSH server information

## 6.3 show ip ssh

This command displays SSH server information.

**show ip ssh**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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



## 7 SSL

SSL (Secure Sockets Layer), is a protocol developed for transmitting private documents through the 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 (e.g. TCP) for data transmission and reception.

The advantage of the SSL Protocol is that it is application protocol independent. A higher level application protocol (e.g. HTTP, FTP, TELNET, etc.) 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](#)

## 7.1 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-dessha] [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]
[rsades- sha] [rsa-3des-sha] [dh-rsa-des-sha] [dh-rsa-3des-sha] [rsa-
exp1024-dessha] }
```

### Syntax Description

**server** - SSL Server

**ciphersuite** - Configures the cipher-suites list

**crypto key rsa** - Usage Key

### Mode

Global Configuration Mode

### Defaults

Ciphersuite - rsa-null-md5

### Example:

```
SMIS(config)# ip http secure ciphersuite rsa-null-sha
```

The ciphersuite field is a bit mask, setting a bit indicates that the corresponding cipher-list will be involved in the server authentication.

### Related Commands

**show ssl server-cert** - Displays SSL server certificate

**show ip http secure server status** - Displays SSL status and configuration information

## 7.2 ssl gen cert-req algo rsa sn

This command creates a certificate request using RSA key pair and subjectName.

```
ssl gen cert-req algo rsa sn <SubjectName>
```

### Syntax Description

**SubjectName** - Identification of the switch (or) the switch's IP address

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# ssl gen cert-req algo rsa sn 10.6.4.248
```

### Related Commands

**show ssl server-cert** - Displays SSL server certificate

**show ip http secure server status** - Displays SSL status and configuration information

## 7.3 ssl server-cert

This command configures the server cert, input in PEM format. It generates a certificate request, which can be submitted to a CA (Certificate Authority) to obtain the SSL certificate for the device.

**ssl server-cert**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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

## 7.4 debug ssl

This command sets the given debug levels for SSL and the no form of the command re-sets the given SSL debug level.

```
debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource]
[buffer])
```

```
no debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource]
[buffer])
```

### Syntax Description

**all** - Initialization and Shutdown Messages

**shut** - Shutdown Messages

**mgmt** - Management Messages

**data** - Data Path Messages

**ctrl** - Control Plane Messages

**dump** - Packet Dump Messages

**resource** - Messages related to all resources except Buffers

**buffer** - Buffer Messages

### Mode

Privileged EXEC Mode

### Defaults

Debugging is Disabled

### Example:

```
SMIS# debug ssl all
```

Setting all the bits will enable all the debug levels and resetting them will disable all the debug levels.

### Related Commands

**show ssl server-cert** - Displays SSL server certificate

**show ip http secure server status** - Displays SSL status and configuration information

## 7.5 show ssl server-cert

This command displays SSL server certificate.

**show ssl server-cert**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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@supermicro.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

## 7.6 show ip http secure server status

This command displays SSL status and configuration information.

```
show ip http secure server status
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip http secure server status
HTTP secure server status : Enabled
HTTP secure server ciphersuite : RSA-DES-SHA:RSA-3DES-SHA:RSAEXP1024-
DES-SHA:
```

Initially, http secure server, ciphersuite, crypto key must have been configured.

### 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 ssl server-cert** - Displays SSL server certificate



## 8 RMON

RMON (Remote Monitoring) is a standard monitoring specification<sup>5</sup> that enables various network monitors and console systems to exchange network-monitoring data.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

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

[set rmon](#)

[rmon event](#)

[rmon alarm](#)

[rmon collection history](#)

[rmon collection stats](#)

[show rmon](#)

## 8.1 set rmon

This command is used to enable or disable the RMON feature.

```
set rmon {enable | disable}
```

### Syntax Description

**enable** - Enables the RMON feature in the system

**disable** - Disables the RMON feature in the system

### Mode

Global Configuration Mode

### Defaults

The RMON Module is disabled by default

### Example:

```
SMIS(config)# set rmon enable
```

- ➔ All the other RMON Module commands can be executed only when the RMON Module is enabled. Fatal error messages are displayed when commands are executed without enabling the RMON feature.

### Related Command

**show rmon** - Successful execution of this command without any messages indicates that RMON feature is enabled in the system

## 8.2 rmon event

This command adds an event to the RMON event table. The added event is associated with an RMON event number. The no form of the command deletes an event from the RMON event table.

```
rmon event <number (1-65535)> [description <event-description (127)>]  
[log] [owner <ownername (127)>] [trap <community (127)>]
```

```
no rmon event <number (1-65535)>
```

### Syntax Description

**Number** - Event number

**Description** - Description of the event

**Log** - Used to generate a log entry

**Owner** - Owner of the event

**Trap** - Used to generate a trap. The SNMP community string is to be passed for the specified trap.

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# rmon event 1 log owner supermicro trap netman
```

➡ The RMON feature must be enabled for the successful execution of this command.

### Related Commands

**rmon alarm** - Sets an alarm on a MIB object

**show rmon** - Displays the RMON events (show rmon events)

**show snmp community** - Configures the SNMP community details

## 8.3 rmon alarm

This command sets an alarm on a MIB object. The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured. The no form of the command deletes the alarm configured on the MIB object.

```
rmon alarm <alarm-number (1-65535) > <mib-object-id (255)> <sample-
intervaltime (1-65535)> {absolute | delta} rising-threshold <value (0-
2147483647)> <rising-event-number (1-65535)> falling-threshold <value
(0-2147483647)> <falling-event-number (1-65535)> [owner <ownername
(127)>]
```

```
no rmon alarm <number (1-65535)>
```

### Syntax Description

**alarm-number** - Alarm Number

**mib-object-id** - The mib object identifier

**sample-intervaltime** - Time in seconds during which the alarm monitors the MIB variable

**absolute** - Used to test each mib variable directly

**delta** Used to test the change between samples of a variable

**rising-threshold** - A number at which the alarm is triggered

**falling-threshold value** - A number at which the alarm is reset

**rising-eventnumber** - The event number to trigger when the rising threshold exceeds its limit

**falling-eventnumber** - The event number to trigger when the falling threshold exceeds its limit

**owner** - Owner of the alarm

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# rmon alarm 1 1.3.6.1.2.1.16.1.1.1.5.2 20 absolute
rising-threshold 15 2 falling-threshold 14 2
```

- ➔ The RMON Feature must be enabled for the successful execution of this command
- RMON events must have been configured

- ▶ In **SMIS**, we cannot monitor all the mib objects through RMON. This will be applicable only to the Ethernet interfaces

### Related Commands

**rmon collection stats** - Enables RMON statistic collection on the interface

**rmon event** - Adds an event to the RMON event table

**show rmon** - Displays the RMON alarms (show rmon alarms)

## 8.4 rmon collection history

This command enables the collection of MIB history group of statistics on the interfaces.

The no form of this command removes the specified history group of statistics collection from the interfaces.

```
rmon collection history <index (1-65535)> [buckets <bucket-number (1-65535)>] [interval <seconds (1-3600)>] [owner <ownername (127)>]
```

```
no rmon collection history <index (1-65535)>
```

### Syntax Description

**index** – An identifier to refer this history statistics collection configuration. This index is used while deleting this configuration using the no command.

**buckets** – Maximum number of buckets needed to hold this history statistics

**interval** - Time in seconds on which this statistics is collected

**owner** - Owner of this statistics collection

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# rmon collection history 1 buckets 1 interval 10 owner  
abc
```

### Related Commands

**rmon collection stats** - Enables RMON statistic collection on the interface

**rmon event** - Adds an event to the RMON event table

**show rmon** - Displays the RMON information

## 8.5 rmon collection stats

This command enables the collection of RMON statistics on the interfaces.

The no form of this command disables the RMON statistics collection on the interfaces.

```
rmon collection stats <index (1-65535)> [owner <ownername (127)>]
```

```
no rmon collection stats <index (1-65535)>
```

### Syntax Description

**index** – An identifier to refer this statistics collection configuration. This index is used while deleting this configuration using the no command.

**owner** - Owner of this statistics collection

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# rmon collection stats 1 owner abc
```

### Related Commands

**rmon event** - Adds an event to the RMON event table

**show rmon** - Displays the RMON information

## 8.6 show rmon

This command displays the RMON statistics, alarms, events, and history configured on the interface.

```
show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events]
[history [history-index (1-65535)] [overview]]
```

### Syntax Description

**Statistics** - The configured stats index value

**Alarms** - The configured alarm

**events** - The configured event

**history** - The configured history index

**overview** - Displays only the overview of rmon history entries

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show rmon statistics 2
RMON is enabled
Collection 2 on Gi0/2 is active, and owned by fsoft,
Monitors ifEntry.1.2 which has
Received 1240 octets, 10 packets,
2 broadcast and 10 multicast packets,
0 undersized and 1 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of packets received of length (in octets):
64: 0, 65-127: 10, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
```

```
SMIS# show rmon
RMON is enabled
```

```
SMIS# show rmon history
RMON is enabled
Entry 1 is active, and owned by fsoft
```



```
Monitors ifEntry.1.1 every 3000 second(s)
Requested # of time intervals, ie buckets, is 3,
Granted # of time intervals, ie buckets, is 3,
Sample 1 began measuring at 0
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events is 0
Network utilization is estimated at 0
Sample 2 began measuring at 0
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events is 0
Network utilization is estimated at 0
```

```
SMIS# show rmon events
```

```
RMON is enabled
Event 1 is active, owned by
Description is end
Event firing causes nothing,
Time last sent is 0 seconds
Event 2 is active, owned by fsoft
Description is trapcheck
Event firing causes log and trap to community 5,
Time last sent is 3 seconds
```

```
SMIS# show rmon alarms
```

```
RMON is enabled
Alarm 1 is active, owned by
Monitors 1.3.6.1.2.1.16.1.1.1.5.2 every 65 second(s)
Taking absolute samples, last value was 35
Rising threshold is 15, assigned to event 1
```

```
Falling threshold is 14, assigned to event 2
On startup enable rising or falling alarm

SMIS# show rmon statistics 2 alarms events history 2
RMON is enabled
Collection 2 on Gi0/2 is active, and owned by fsoft,
Monitors ifEntry.1.2 which has
Received 4712 octets, 38 packets,
0 broadcast and 38 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of packets received of length (in octets):
64: 0, 65-127: 38, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
Alarm 1 is active, owned by
Monitors 1.3.6.1.2.1.16.1.1.1.5.2 every 65 second(s)
Taking absolute samples, last value was 37
Rising threshold is 15, assigned to event 1
Falling threshold is 14, assigned to event 2
On startup enable rising or falling alarm
Event 1 is active, owned by
Description is end
Event firing causes nothing,
Time last sent is 1708335 seconds
Event 2 is active, owned by fsoft
Description is trapcheck
Event firing causes log and trap to community 5,
Time last sent is 0 seconds
Entry 2 is active, and owned by fsoft
Monitors ifEntry.1.2 every 2000 second(s)
Requested # of time intervals, ie buckets, is 5,
Sample 1 began measuring at 0
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
```

```
0 CRC alignment errors and 0 collisions,  
# of dropped packet events is 0  
Network utilization is estimated at 0  
Sample 2 began measuring at 0  
Received 0 octets, 0 packets,  
0 broadcast and 0 multicast packets,  
0 undersized and 0 oversized packets,  
0 fragments and 0 jabbers,  
0 CRC alignment errors and 0 collisions,  
# of dropped packet events is 0  
Network utilization is estimated at 0
```

```
SMIS# show rmon history overview  
RMON is enabled  
Entry 1 is active, and owned by fsoft  
Monitors ifEntry.1.1 every 3000 second(s)  
Requested # of time intervals, ie buckets, is 3,  
Granted # of time intervals, ie buckets, is 3
```

If the **show rmon** command is executed with out enabling the RMON feature, then the following output is displayed

```
SMIS# show rmon  
RMON feature is disabled
```

### Related Commands

**set rmon** - Enables or disables the RMON feature

**rmon collection history** - Enables history collection of interface statistics in the buckets for the specified time interval

**rmon collection stats** - Enables RMON statistic collection on the interface

**rmon event** - Adds an event to the RMON event table

**rmon alarm** - Sets an alarm on a MIB object

## 9 STP

STP (Spanning-Tree Protocol) is a link management protocol that provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state.

MSTP defines an extension to RSTP that further develops the usefulness of VLANs. This "per-VLAN" MSTP configures a separate Spanning Tree for each VLAN group and blocks the links that are redundant within each Spanning Tree.

If there is only one VLAN in the network, single (traditional) STP works appropriately. If the network contains more than one VLAN, the logical network configured by single STP would work, but it is possible to make better use of the redundant links available by using an alternate spanning tree for different (groups of) VLANs. MSTP allows the formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST).

- The list of CLI commands for the configuration of STP are common to both **Single Instance and Multiple Instance**, except for a difference in the prompt that appears for the Switch with Multiple Instance support.
  - The prompt for the **Global Configuration Mode** is,  
SMIS (config-switch) #
  - The prompt for the **MSTP Configuration Mode** is,  
SMIS (config-switch-mst) #.
- The **parameters** specific to Multiple Instance are stated so, against the respective parameter descriptions in this document.
- The output of the **Show commands** differ for Single Instance and Multiple Instance. Hence both the output are documented while depicting the show command examples

The list of commands to configure STP are:

[spanning-tree mode](#)

[spanning-tree](#)

[spanning-tree compatibility](#)

[spanning-tree timers](#)

[spanning-tree transmit hold-count](#)

[spanning-tree mst max-hops](#)

[spanning-tree priority](#)

[spanning-tree pathcost method](#)

[spanning-tree mst configuration](#)

[name](#)

[revision](#)

[instance](#)

[spanning-tree auto-edge](#)

[spanning-tree - Properties of an interface](#)

[spanning-tree restricted-role](#)

[spanning-tree restricted-tcn](#)

[spanning-tree mst- Properties of an interface for MSTP](#)

[spanning-tree mst hello-time](#)

[clear spanning-tree counters](#)

[clear spanning-tree pathcost dynamic](#)

[clear spanning-tree detected protocols](#)

[debug spanning-tree](#)

[show spanning-tree - Summary, Blockedports, Pathcost](#)

[show spanning-tree - Detail](#)

[show spanning-tree active](#)

[show spanning-tree interface](#)

[show spanning-tree root](#)

[show spanning-tree bridge](#)

[show spanning-tree mst](#)

[show spanning-tree mst configuration](#)

[show spanning-tree mst - Port Specific Configuration](#)

## 9.1 spanning-tree mode

This command sets the spanning tree operating mode.

**spanning-tree mode {mst|rst}**

### Syntax Description

**mst** - MSTP configuration

**rst** - RSTP configuration

### Mode

Global Configuration Mode

### Defaults

mst

### Example:

```
SMIS(config)#spanning-tree mode rst
```

- When ISS boots up, Spanning Tree is enabled by default with MSTP operating in the switch.
- This command only starts and enables the spanning tree mode. However port-roles and states will be computed only after enabling the spanning tree.
- If the user-input for the spanning-tree mode is different from the current mode of operation, then ISS will shutdown the operational spanning-tree and start the spanning-tree as per user-input.

### Related Commands

**show spanning-tree - Detail** - Displays detailed spanning tree information

**show spanning-tree - Active** - Displays spanning tree information of active ports

## 9.2 spanning-tree

This command enables the spanning tree operation and the no form of the command disables the spanning tree operation.

**spanning-tree**

**no spanning-tree**

### Mode

Global Configuration Mode

### Defaults

Spanning tree enabled is MSTP

### Example:

```
SMIS (config) #spanning-tree
```

### Related Commands

**show spanning-tree - Detail** - Displays detailed spanning tree information

**show spanning-tree - Active** - Displays spanning tree information of active ports

## 9.3 spanning-tree compatibility

This command sets the compatibility version for the spanning tree protocol. The no form of the command sets the compatibility version for spanning tree protocol to its default value.

```
spanning-tree compatibility {stp|rst|mst}
```

```
no spanning-tree compatibility
```

### Syntax Description

**mst** - MSTP configuration

**stp** - STP configuration

**rst** - RSTP configuration

### Mode

Global Configuration Mode

### Defaults

If Spanning Tree Protocol enabled is mst, then MSTP compatible

If Spanning Tree Protocol enabled is rst, then RSTP compatible

### Example:

```
SMIS(config)#spanning-tree compatibility stp
```

The option **mst** is available only when MSTP is the operational mode of the spanning tree

### Related Commands

**show spanning-tree - Detail** - Displays detailed spanning tree information

**show spanning-tree - Active** - Displays spanning tree information of active ports



## 9.4 spanning-tree timers

This command sets the spanning tree Timers and the no form of the command sets the spanning tree timers to the default values.

```
spanning-tree {forward-time <seconds(4-30)> | hello-time <seconds(1-2)>
| maxage <seconds(6-40)>}
```

```
no spanning-tree { forward-time | hello-time | max-age }
```

### Syntax Description

**forward-time** - Controls how fast a port changes its spanning tree state from Blocking state to Forwarding state.

**hello-time** - Determines how often the switch broadcasts its hello message to other switches when it is the root of the spanning tree.

**max-age** - The maximum age allowed for the Spanning Tree Protocol information learned from the network on any port before it is discarded.

### Mode

Global Configuration Mode

### Defaults

max-age - 20 secs

forward-time - 15 secs

hello-time - 2 secs

### Example:

```
SMIS(config)#spanning-tree max-age 6
SMIS(config)#spanning-tree hello-time 1
SMIS(config)#spanning-tree forward-time 4
```

The following relation must be observed while configuring the timers:

$2 \times (\text{Forward-time} - 1) \geq \text{Max-age}$

$\text{Max-Age} \geq 2 \times (\text{Hello-time} + 1)$

### Related Commands

**show spanning-tree bridge** - Displays spanning tree configuration of the bridge forward time

**show spanning-tree bridge hello-time** - Displays spanning tree configuration of the bridge hello-time

**show spanning-tree bridge max-age** - Displays spanning tree configuration of the bridge maxage

**show spanning-tree - Detail** - Displays detailed spanning tree information

**show spanning-tree - Active** - Displays spanning tree information of active ports

## 9.5 spanning-tree transmit hold-count

This command sets the transmit hold-count value and the no form of the command sets the transmit holdcount to default value. Transmit hold count value is a counter used to limit the maximum transmission rate of the switch.

```
spanning-tree transmit hold-count <value (1-10)>
```

```
no spanning-tree transmit hold-count
```

### Mode

Global Configuration Mode

### Defaults

3

### Example:

```
SMIS(config)#spanning-tree transmit hold-count 5
```

### Related Commands

**show spanning-tree - Detail** - Displays detailed spanning tree information

**show spanning-tree - Active** - Displays spanning tree information of active ports

## 9.6 spanning-tree mst max-hops

This command sets the maximum number of hops permitted in the MST and the no form of the command sets the maximum number of hops permitted in the MST to the default value.

```
spanning-tree mst max-hops <value(6-40)>
```

```
no spanning-tree mst max-hops
```

### Mode

Global Configuration Mode

### Defaults

20

### Example:

```
SMIS(config)#spanning-tree mst max-hops 10
```

The root switch of the instance always sends a BPDU with a cost of 0 and the hop count set to the maximum value.

### Related Command

**show spanning-tree mst configuration** - Displays multiple spanning tree instance Configuration

## 9.7 spanning-tree priority

This command sets the Bridge Priority for the spanning tree only in steps of 4096 and the no form of the command sets the Bridge Priority to the default value.

```
spanning-tree [mst <instance-id>] priority <value(0-61440)>
```

```
no spanning-tree [mst <instance-id(1-16)>] priority
```

### Syntax Description

**mst** - Range of spanning tree instances

**priority** - Switch priority for the specified spanning-tree instance

### Mode

Global Configuration Mode

### Defaults

32768

### Example:

```
SMIS(config)#spanning-tree priority 4096
```

"spanning-tree priority xxx" configures the priority in RSTP, if RSTP is running or configures the CIST priority if MSTP is running.

"spanning-tree mst instance priority" configures the priority in MSTI and is supported only if MSTP is running.

### Related Commands

**show spanning-tree - Detail** - Displays detailed spanning tree information

**show spanning-tree - Active** - Displays spanning tree information of active ports

## 9.8 spanning-tree pathcost method

This command sets the method to calculate the port path cost and the no form of the command sets the method to calculate the port path cost to its default.

```
spanning-tree pathcost method {long|short}
```

```
no spanning-tree pathcost method
```

### Syntax Description

**long** - 32 bit pathcost

**short** - 16 bit path cost

### Mode

Global Configuration Mode

### Defaults

If MSTP/RSTP is running- path cost method is long

If STP compatible RSTP is running, the path-cost method is short

### Example:

```
SMIS(config)#spanning-tree pathcost method short
```

### Related Command

**show spanning-tree - Summary, Blockedports, Pathcost** - Displays spanning tree pathcost information

## 9.9 spanning-tree mst configuration

This command helps to enter MST configuration submode

**spanning-tree mst configuration**

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)#spanning-tree mst configuration
```

In the MST mode the switch supports up to 16 instances. This MST configuration submode is used to make instance-specific and MST region configurations only.

### Related Command

**show spanning-tree mst configuration** - Displays multiple spanning tree instance Configuration

## 9.10 name

This command sets the configuration name for the MST region and the no form of the command deletes the configuration name.

```
name <string(optional max Length)>
```

```
no name
```

### Mode

MSTP configuration Mode

### Defaults

The default configuration name is 00: 00: 00: 00: 00: 00

### Example:

```
SMIS(config-mst)#name regionone
```

The name string is case sensitive.

### Related Command

```
show spanning-tree mst configuration - Displays Multiple spanning tree instance configuration
```



## 9.11 revision

This command sets the configuration revision number for the MST region and the no form of the command deletes the configuration revision number.

```
revision <value(0-65535)>
```

```
no revision
```

### Mode

MSTP configuration Mode

### Defaults

0

### Example:

```
SMIS(config-mst)#revision 100
```

### Related Command

**show spanning-tree mst configuration** - Displays Multiple spanning tree instance configuration

## 9.12 instance

This command maps VLANs to an MST instance and the no form of the command deletes the instance un-maps specific VLANs from the MST instance.

```
instance <instance-id(1-16)> vlan <vlan-range>
```

```
no instance <instance-id (1-16)> [vlan <vlan-range>]
```

### Syntax Description

**vlan** - VLAN range associated with a spanning-tree instance

### Mode

MSTP configuration Mode

### Defaults

VLANs mapped for instance 0: 1-1024, 1025-2048, 2049-3072,3073-4069

### Example:

```
SMIS(config-mst)#instance 2 vlan 2
```

A single VLAN identified by VLAN ID number is specified by a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

### Related Command

**show spanning-tree mst configuration** - Displays Multiple spanning tree instance configuration

## 9.13 spanning-tree auto-edge

This command enables automatic detection of bridge attached on an interface and the no form of the command disables automatic detection of bridge attached on an interface.

**spanning-tree auto-edge**

**no spanning-tree auto-edge**

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# spanning-tree auto-edge
```

### Related Command

**show spanning-tree bridge** - Displays the spanning-tree configuration of the bridge

## 9.14 spanning-tree - Properties of an interface

This command sets the spanning tree properties of an interface and the no form of the command sets the spanning tree properties of an interface to default value.

```
spanning-tree {cost <value(1-200000000)>|disable|link-type{point-  
topoint| shared}|portfast|port-priority <value(0-240)>}
```

```
no spanning-tree {cost |disable|link-type|portfast|port-priority}
```

### Syntax Description

**port-priority** - Port priority value

**cost** - The pathcost value associated with the port

**disable** - Disables the spanning tree on the port

**link-type** - The link can be a point-to-point link or can be a shared LAN segment on which another bridge is present

**portfast** - Specifies that port has only hosts connected and hence can transition to forwarding rapidly

### Mode

Interface Configuration Mode

### Defaults

The default cost value depends on the interface speed.

Port Speed	Default Cost
10 Mbps	2000000
100 Mbps	200000
1 Gbps	20000
10 Gbps	2000
40 Gbps	500

port-priority - 128

portfast - Not in portfast

link-type - shared

### Example:

```
SMIS(config-if)# spanning-tree cost 2200
```

In case of MSTP this configuration applies to the CIST context.

### **Related Command**

**show spanning-tree interface** - Displays the spanning tree properties of an interface

## 9.15 spanning-tree restricted-role

This command enables the root-guard / restricted role feature (prevents the specific port from becoming the root port) on the port. The no form of the command disables the root-guard / restricted role feature on the port. .

**spanning-tree restricted-role**

**no spanning-tree restricted-role**

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# spanning-tree restricted-role
```

### Related Command

**show spanning-tree - Detail** - Displays spanning tree information

## 9.16 spanning-tree restricted-tcn

This command enables the topology change guard / restricted TCN feature (prevents the Topology change caused by that port ) on the port. The no form of the command disables the topology change guard/ restricted TCN feature on the port.

**spanning-tree restricted-tcn**

**no spanning-tree restricted-tcn**

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# spanning-tree restricted-tcn
```

### Related Command

**show spanning-tree - Detail** - Displays spanning tree information

## 9.17 spanning-tree mst- Properties of an interface for MSTP

This command sets the spanning tree properties of an interface for MSTP and the no form of the command sets the spanning tree properties of an interface to default value.

```
spanning-tree mst <instance-id(1-16)> { cost <value(1-200000)>| port-
priority <value(0-240)> | disable }
```

```
no spanning-tree mst <instance-id(1-16)>{cost|port-priority | disable}
```

### Syntax Description

**cost** - The cost value associated with the port

**port-priority** - Port priority value

**disable** - Disables the spanning tree on the port

### Mode

Interface Configuration Mode

### Defaults

– The default cost value depends on the interface speed.

Port Speed	Default Cost
10 Mbps	2000000
100 Mbps	200000
1 Gbps	20000
10 Gbps	2000
40 Gbps	500

port-priority - 128

### Example:

```
SMIS(config-if)#spanning-tree mst 2 cost 4000
```

MST instance must exist, for this command If all interfaces have the same priority value, the MST puts the interface with the lowest interface number in the forwarding state and blocks other interfaces



**Related Command**

**show spanning-tree mst - CIST or specified mst Instance-** Displays the spanning tree properties of an interface for an MSTP instance

## 9.18 spanning-tree mst hello-time

This command sets the port based hello timer value and the no form of the command sets the port based hello timer value to its default.

```
spanning-tree mst hello-time<value(1-2)>
```

```
no spanning-tree mst hello-time
```

### Mode

Interface Configuration Mode

### Defaults

2 seconds

### Example:

```
SMIS(config-if)#spanning-tree mst hello-time 1
```

On changing the spanning-tree mst hello-time value, all spanning-tree instances active on the interface are affected.

### Related Command

**show spanning-tree mst - Port Specific Configuration** - Displays multiple spanning tree port specific configurations

## 9.19 clear spanning-tree counters

This command resets all bridge and port level statistics counters.

**clear spanning-tree counters**

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# clear spanning-tree counters
```

Valid interfaces include physical ports, VLANs, and port channels

Port protocol migration count gets incremented consistently, when there is a protocol migration

### Related Commands

**show spanning-tree interface** - Displays the spanning tree properties of an interface

**show spanning-tree mst - Port Specific Configuration** - Displays multiple spanning tree port specific configurations

## 9.20 spanning-tree pathcost dynamic

This command enables dynamic pathcost calculation and the no form of the command disables dynamic pathcost calculation.

**spanning-tree pathcost dynamic**

**no spanning-tree pathcost dynamic**

### Mode

Global Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config)# spanning-tree pathcost dynamic
```

On execution of this command, the pathcost of all the ports will be calculated dynamically based on the speed of the interface.

If the cost has already been configured for a cist or an rstp interface, then this command has no effect on those interfaces.

If the cost has been configured previously for an mst instance on a particular interface, then this command has no effect on that instance in the specified interface. Whereas the pathcost of all the other instances on the same interface will be calculated dynamically.

### Related Commands

**spanning-tree pathcost method** – Sets the method to calculate the port path cost

**spanning-tree compatibility**– Sets the compatibility version for the spanning tree protocol

**spanning-tree - Properties of an interface** – Sets the spanning tree properties of an interface

**spanning-tree mst- Properties of an interface for MSTP** – Sets the spanning tree properties of an interface for MSTP

## 9.21 clear spanning-tree detected protocols

This command restarts the protocol migration process on all the interfaces and forces renegotiation with the neighboring switches.

```
clear spanning-tree detected protocols {interface <interface-type>
<interfaceid> }
```

### Syntax Description

**interface** - Restarts the protocol migration process on the specified interface Valid interfaces include physical ports, VLANs, and port channels

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# clear spanning-tree detected protocols interface
gigabitethernet 0/1
```

Port protocol migration count gets incremented consistently, when there is a protocol migration.

### Related Commands

**show spanning-tree interface** - Displays the spanning tree properties of an interface

**show spanning-tree mst - Port Specific Configuration** - Displays multiple spanning tree port specific configurations

## 9.22 debug spanning-tree

This command provides spanning tree debugging support and the no form of the command disables debugging.

```
debug spanning-tree { global | { all | errors | init-shut | management |
memory | bpdu | events | timer | state-machine { port-info | port-
recieve | portrole-selection | role-transition | state-transition |
protocol-migration | topology-change | port-transmit | bridge-detection
} | redundancy | semvariables} }
```

```
no debug spanning-tree {global | {all | errors | init-shut | management
| memory | bpdu |events | timer | state-machine {port-info | port-
recieve | port-role-selection | role-transition | state-transition |
protocol-migration | topology-change | port-transmit | bridge-detection
} redundancy | semvariables} }
```

### Syntax Description

**global** - Global debug messages

**all** - All RSTP / MSTP debug messages

**errors** - Error code debug messages

**init-shut** - Init and Shutdown debug messages

**management** - Management messages

**Memory** - Memory related messages

**bpdu** - BPDU related messages

**timer** - Timer module messages

**events** - Events related messages

**state machine** - State-machine related debug messages

**port-info** - Port information messages

**port-receive** - Port received messages. This parameter is specific to Multiple Instance.

**port-roleselction** - Port role selection messages

**role-transition** - Role transition messages

**state-transition** - State transition messages

**protocolmigration** - Protocol migration messages

**topology-change** - Topology change messages

**port-transmit** - Port transmission messages

**bridge-detection** - Bridge detection messages

**redundancy** - Redundancy related messages

**sem-variables** - State-machine variables debug messages

## **Mode**

Privileged EXEC Mode

## **Defaults**

Debugging is Disabled

## **Example:**

```
SMIS# debug spanning-tree all
```

## **Related Command**

**show spanning-tree - Detail** - Displays detailed spanning tree information for STP/RSTP/MSTP configuration

## 9.23 show spanning-tree - Summary, Blockedports, Pathcost

This command displays spanning tree information.

```
show spanning-tree [{ summary | blockedports | pathcost method }]
```

### Syntax Description

**summary** - Summary of port states

**blockedports** - Blocked ports in the system

**pathcost method** - Pathcost method configured for a bridge

### Mode

Privileged EXEC Mode

### Defaults

When **SMIS** boots up, Spanning Tree is enabled by default with MSTP operating in the switch.

### Example:

#### Single Instance:

```
SMIS# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 0
Port 0 [0]
This bridge is the root
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning tree Protocol Enabled.
S-VLAN Component: MST00 is executing the mstp compatible
Multiple Spanning Tree
Protocol
Bridge Id Priority 32768
Address 00:01:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
```



```
-----  
Gi0/1 Disabled Discarding 200000 128 SharedLan  
Gi0/2 Designated Forwarding 200000 128 SharedLan  
Gi0/3 Designated Forwarding 200000 128 SharedLan  
Gi0/4 Designated Forwarding 200000 128 SharedLan  
Gi0/5 Designated Forwarding 200000 128 SharedLan  
Gi0/6 Designated Forwarding 200000 128 SharedLan  
Gi0/7 Designated Forwarding 200000 128 SharedLan
```

```
SMIS# show spanning-tree blockedports  
Blocked Interfaces List:  
The Number of Blocked Ports in the system is :1
```

```
SMIS# show spanning-tree pathcost method  
Spanning Tree port pathcost method is Long
```

```
SMIS# show spanning-tree summary  
Spanning tree enabled protocol is RSTP  
RSTP Port Roles and States  
Port-Index Port-Role Port-State Port-Status  
-----  
1 Root Forwarding Enabled  
2 Disabled Discarding Enabled  
3 Disabled Discarding Enabled  
4 Disabled Discarding Enabled
```

**Multiple Instance:**

```
SMIS# show spanning-tree  
Switch default  
Root Id Priority 32768  
Address 00:01:02:03:04:01  
Cost 0  
Port 0 [0]  
This bridge is the root  
Max age 20 Sec, forward delay 15 Sec  
MST00  
Spanning tree Protocol Enabled.
```

```
S-VLAN Component: MST00 is executing the mstp compatible
Multiple Spanning Tree
Protocol
Bridge Id Priority 32768
Address 00:01:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
-----
Gi0/1 Disabled Discarding 200000 128 SharedLan
Gi0/2 Designated Forwarding 200000 128 SharedLan
Gi0/3 Designated Forwarding 200000 128 SharedLan
Gi0/4 Designated Forwarding 200000 128 SharedLan
Gi0/5 Designated Forwarding 200000 128 SharedLan
Gi0/6 Designated Forwarding 200000 128 SharedLan
Gi0/7 Designated Forwarding 200000 128 SharedLan
```

```
SMIS# show spanning-tree summary
```

```
Switch - default
```

```
Spanning Tree port pathcost method is Long
```

```
Spanning tree enabled protocol is MSTP
```

```
MST00 Port Roles and States
```

```
Port-Index Port-Role Port-State Port-Status
```

```
-----
49 Disabled Forwarding Disabled
```

```
Switch - cust1
```

```
Spanning Tree port pathcost method is Long
```

```
Spanning tree enabled protocol is MSTP
```

```
MST00 Port Roles and States
```

```
Port-Index Port-Role Port-State Port-Status
```

```
-----
1 Designated Forwarding Enabled
```

```
2 Root Forwarding Enabled
```

```
3 Designated Forwarding Enabled
```

```
4 Disabled Discarding Enabled
```

```
5 Disabled Discarding Enabled
```

```
6 Disabled Discarding Enabled
```

```
Switch - cust2
```

```
Spanning Tree port pathcost method is Long
Spanning tree enabled protocol is MSTP
MST00 Port Roles and States
Port-Index Port-Role Port-State Port-Status
```

```
-----
7 Designated Forwarding Enabled
8 Root Forwarding Enabled
9 Alternate Discarding Enabled
10 Disabled Discarding Enabled
11 Disabled Discarding Enabled
12 Disabled Discarding Enabled
```

This command is the same for both RSTP and MSTP.

### Related Commands

**spanning-tree mode** - Sets the spanning tree operating mode

**spanning-tree** - Enables the spanning tree operation

**spanning-tree provider** - Enables the spanning tree operation

**spanning-tree compatibility** - Sets the compatibility version for the spanning tree protocol

**spanning-tree timers** - Sets the spanning tree Timers

**spanning-tree transmit hold-count** - Sets the transmit hold-count value

**spanning-tree priority** - Sets the Bridge Priority for the spanning tree only in steps of 4096

**spanning-tree - Properties of an interface** - Sets spanning tree properties of an interface

**spanning-tree mst- Properties of an interface for MSTP** - Sets the spanning tree properties of an interface for MSTP

**show spanning-tree bridge** - Displays the spanning-tree configuration of the bridge

**show spanning-tree interface** - Displays Spanning-tree port configuration

**spanning-tree pathcost method** - Sets the method to calculate the default port path cost

## 9.24 show spanning-tree - Detail

This command displays detailed spanning tree information.

**show spanning-tree detail [active]**

### Syntax Description

**active** - Displays the Bridge and details of the active (active ports are those ports that are participating in the spanning-tree) ports

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show spanning-tree detail
Bridge is executing the rstp compatible Spanning Tree
Protocol
Bridge Identifier has priority 32768, Address
00:01:02:03:04:11
Configured Hello time 2 sec, Max Age 20 sec, Forward Delay
15 sec
Number of Topology Changes 1
Time since topology Change 1637 seconds ago
Transmit Hold-Count 3 sec
Timers : Hello Time 2 Sec, Max Age 20 Sec, Forward Delay 15
Sec
Port 1 [Gi0/1] is Root , Forwarding
Port PathCost 2000000, Port Priority 128, Port Identifier
128.1
Designated Root has priority 8192, address 00:01:02:03:04:21
Designated Bridge has priority 8192, address
00:01:02:03:04:21
Designated Port Id is 128.1, Designated PathCost 0
No of Transitions to forwarding State :1
PortFast is disabled
Link Type is Shared
BPDUs : sent 735 , recieved 865
```

### Multiple Instance:

```
SMIS# show spanning-tree detail switch default
Switch default
MST00 is executing the mstp compatible Multiple Spanning
Tree Protocol
Bridge Identifier has Priority 32768, Address
00:51:02:03:04:05
Configured Max age 20 sec, Forward delay 15 sec
Configured Hello Time 2 sec
We are root of the spanning tree
Current Root has priority 32768, address 00:51:02:03:04:05
cost of root path is 0
Number of Topology Changes 1, Time since topology Change 82
seconds ago
Transmit Hold-Count 3
Times : Max age 20 Sec,Forward delay 15 Sec
Port 1 [Gi0/1] of MST00 is Designated, Forwarding
Gi0/1 is operating in the MSTP Mode
Port path cost 200000, Port priority 128,
Port Identifier 128.1. Port HelloTime 2,
Timers: Hello - 0, Forward Delay - 0, Topology Change - 0
Designated root has priority 32768, address
00:51:02:03:04:05
Designated Bridge has priority 32768, address
00:51:02:03:04:05
Designated Port Id is 128.1, Designated pathcost is 0
Operational Forward delay 15, Max age 20
Number of Transitions to forwarding State : 1
PortFast is disabled
Link Type is Shared
BPDUs : sent 58, recieved 0
Restricted Role is disabled.
Restricted TCN is disabled.
```

### Related Commands

**spanning-tree mode** - Sets the spanning tree operating mode

**spanning-tree** - Enables the spanning tree operation

**spanning-tree provider** - Enables the Spanning tree operation

**spanning-tree compatibility**- Sets the compatibility version for the spanning tree protocol

**spanning-tree timers** - Sets the spanning tree Timers

**spanning-tree transmit hold-count** - Sets the transmit hold-count value

**spanning-tree priority** - Sets the Bridge Priority for the spanning tree only in steps of 4096

**spanning-tree - Properties of an interface** - Sets spanning tree properties of an interface

**spanning-tree mst- Properties of an interface for MSTP** - Sets the spanning tree properties of an interface for MSTP

**show spanning-tree bridge** - Displays the spanning-tree configuration of the bridge

**show spanning-tree interface** - Displays Spanning-tree port configuration

## 9.25 show spanning-tree - Active

This command displays spanning tree information of active ports.

**show spanning-tree active [detail]**

### Syntax Description

**detail** - Displays in detail about the port and bridge. This includes designated Bridge details, designated port details, timer values, root bridge, etc.

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show spanning-tree active
Root Id Priority 8192
Address 00:01:02:03:04:21
Cost 2000000
Port Gi0/1
Hello Time 2 Sec, Max Age 20 Sec,
Forward Delay 15 Sec
Spanning Tree Enabled Protocol RSTP
Bridge Id Priority 32768
Address 00:01:02:03:04:11
Hello Time 2 sec, Max Age 20 sec,
Forward Delay 15 sec
Name Role State Cost Prio Type
-----
Gi0/1 Root Forwarding 2000000 128 SharedLan
```

#### Multiple Instance:

```
SMIS# show spanning-tree active switch default
Switch default
Root Id Priority 32768
Address 00:51:02:03:04:05
Cost 0
```

```
Port 0 [0]
This bridge is the root
Max age 20 Sec, forward delay 15 Sec
MST00
MST00 is executing the mstp compatible Multiple Spanning
Tree Protocol
Bridge Id Priority 32768
Address 00:51:02:03:04:05
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
-----
Gi0/1 Designated Forwarding 200000 128 SharedLan
```

## Related Commands

**spanning-tree mode** - Sets the spanning tree operating mode

**spanning-tree** - Enables the spanning tree operation

**spanning-tree provider** - Enables the Spanning tree operation

**spanning-tree compatibility**- Sets the compatibility version for the spanning tree protocol

**spanning-tree timers** - Sets the spanning tree Timers

**spanning-tree transmit hold-count** - Sets the transmit hold-count value

**spanning-tree priority** - Sets the Bridge Priority for the spanning tree only in steps of 4096

**spanning-tree - Properties of an interface** - Sets spanning tree properties of an interface

**spanning-tree mst- Properties of an interface for MSTP** - Sets the spanning tree properties of an interface for MSTP

**show spanning-tree bridge** - Displays the spanning-tree configuration of the bridge

**show spanning-tree interface** - Displays Spanning-tree port configuration



## 9.26 show spanning-tree interface

This command displays Spanning-tree port configuration.

```
show spanning-tree interface <interface-type> <interface-id> [{ cost |
priority | portfast | rootcost | restricted-role | restricted-tcn |
state | stats | detail }]
```

### Syntax Description

**cost** - Spanning tree port cost

**state** - Spanning tree state

**stats** - Displays the input and output packets by switching path for the interface

**priority** - Spanning tree port priority

**portfast** - Spanning tree portfast state

**rootcost** - Spanning tree rootcost (pathcost to reach the root ) value

**restricted-role** Spanning-tree Restricted Role

**restricted-tcn** Spanning-tree Restricted Topology Change

**detail** - Displays in detail about the port and bridge

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show spanning-tree interface gigabitethernet 0/1
Role State Cost Prio Type
---- ----
Root Forwarding 2000000 128 SharedLan
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 cost
Port cost is 2000000
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 priority
Port Priority is 128
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 portfast
PortFast is disabled
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 rootcost
Root Cost is 2000000
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 state
Forwarding
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 stats
Statistics for Port Gi0/1
Number of Transitions to forwarding State : 1
Number of RSTP BPDU Count received : 1692
Number of Config BPDU Count received : 9
Number of TCN BPDU Count received : 0
Number of RSTP BPDU Count Transmitted : 735
Number of Config BPDU Count Transmitted : 11
Number of TCN BPDU Count Transmitted : 0
Number of Invalid BPDU Count Transmitted : 0
Port Protocol Migration Count : 1
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 detail
Port 1 [Gi0/1] is Root , Forwarding
Port PathCost 2000000, Port Priority 128, Port Identifier 128.1
Designated Root has priority 8192, address 00:01:02:03:04:21
Designated Bridge has priority 8192, address 00:01:02:03:04:21
Designated Port Id is 128.1, Designated PathCost 0
No of Transitions to forwarding State :1
```

```
PortFast is disabled
Link Type is Shared
BPDUs : sent 735 , recieved 1729
```

```
SMIS# show spanning-tree interface fast 0/1 restricted-role
Restricted Role is Disabled
```

```
SMIS# show spanning-tree interface fast 0/1 restricted-tcn
Restricted TCN is Disabled
```

### Multiple Instance:

```
SMIS# show spanning-tree interface gigabitethernet 0/1
```

```
Switch - default
```

```
Role State Cost Prio Type
```

```
-----
```

```
Root Forwarding 2000000 128 SharedLan
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 cost
```

```
Port cost is 2000000
```

```
Switch - default
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 priority
```

```
Switch - default
```

```
Port Priority is 128
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 portfast
```

```
Switch - default
```

```
PortFast is disabled
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 rootcost
```

```
Switch - default
```

```
Root Cost is 2000000
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 state
```

```
Switch - default
```

```
Forwarding
```

```
SMIS# show spanning-tree interface gigabitethernet 0/1 stats
```

```
Switch - default
```

```
Statistics for Port Gi0/1
```

```
Number of Transitions to forwarding State : 1
```

```
Number of RSTP BPDU Count received : 1692
```

```
Number of Config BPDU Count received : 9
```

```
Number of TCN BPDU Count received : 0
```

```
Number of RSTP BPDU Count Transmitted : 735
```

```
Number of Config BPDU Count Transmitted : 11
```

```
Number of TCN BPDU Count Transmitted : 0
```

Number of Invalid BPDU Count Transmitted : 0

Port Protocol Migration Count : 1

```
SMIS# show spanning-tree interface gigabitethernet 0/1 detail
Switch - default
Port 1 [Gi0/1] is Root , Forwarding
Port PathCost 2000000, Port Priority 128, Port Identifier 128.1
Designated Root has priority 8192, address 00:01:02:03:04:21
Designated Bridge has priority 8192, address 00:01:02:03:04:21
Designated Port Id is 128.1, Designated PathCost 0
No of Transitions to forwarding State :1
PortFast is disabled
Link Type is Shared
BPDUs : sent 735 , recieved 1729
```

```
SMIS# show spanning-tree interface fast 0/1 restricted-role
Switch - default
Restricted Role is Disabled
```

```
SMIS# show spanning-tree interface fast 0/1 restricted-tcn
Switch - default
Restricted TCN is Disabled
```

Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical ports, VLANs, and port channels.

### Related Commands

**spanning-tree - Properties of an interface** - Sets spanning tree properties of an interface

**spanning-tree mst-** **Properties of an interface for MSTP** - Sets the spanning tree properties of an interface for MSTP

**show spanning-tree - Detail** - Displays detailed spanning tree information

**show spanning-tree - Active** - Displays spanning tree information of active ports

**clear spanning-tree detected protocols** - Restarts the protocol migration process on all the interfaces

**clear spanning-tree counters** - Resets all bridge and port level statistics counters

## 9.27 show spanning-tree root

This command displays Spanning-tree root information.

```
show spanning-tree root [{ address | cost | forward-time | hello-time |
id | max-age | port | priority | detail }]
```

### Syntax Description

**Address** - Root bridge MAC address

**Cost** - Cost value associated with the port

**forward-time** - Root bridge forward time

**hello-time** - Root bridge hello time

**id** - Root bridge ID

**max-age** - Root bridge Max age

**port** - Root port

**priority** - Root bridge priority

**detail** - Displays in detail about the port and bridge. This includes designated Bridge details, designated port details, timer values, root bridge, etc

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show spanning-tree root
Root ID RootCost HelloTime MaxAge FwdDly RootPort
-----
80:00:00:01:02:03:04:11 0 2 20 15 0
```

```
SMIS# show spanning-tree root address
Root Bridge Address is 00:01:02:03:04:11
```

```
SMIS# show spanning-tree root cost
Root Cost is 2000000
```

```
SMIS# show spanning-tree root forward-time
Forward delay is 15 sec
```

```
SMIS# show spanning-tree root id
Root Bridge Id is 80:00:00:01:02:03:04:11
```

```
SMIS# show spanning-tree root hello-time
Hello Time is 2 sec
```

```
SMIS# show spanning-tree root id
Root Bridge Id is 80:00:00:01:02:03:04:11
```

```
SMIS# show spanning-tree root max-age
Root MaxAge is 20
```

```
SMIS# show spanning-tree root port
Root Port is 1
```

```
SMIS# show spanning-tree root priority
Root Priority is 32768
```

```
SMIS# show spanning-tree root detail
We are the root of the Spanning Tree
Root Id Priority 32768
Address 00:01:02:03:04:11
Cost 0
Port 0
Hello Time 2 Sec, Max Age 20 Sec, Forward
Delay 15 Sec
```

**Multiple Instance:**

```
SMIS# show spanning-tree root
Switch - default
Instance Root ID RootCost MaxAge FwdDly RootPort
-----
MST00 80:00:00:01:02:03:04:01 0 20 15 0
Switch - cust1
Instance Root ID RootCost MaxAge FwdDly RootPort
-----
```

```
MST00 00:00:00:01:02:03:04:04 200000 20 15 Gi0/2
```

## Related Commands

**spanning-tree timers** - Sets the spanning tree Timers

**spanning-tree priority** - Sets the Bridge Priority for the spanning tree only in steps of 4096

**show spanning-tree - Detail** - Displays detailed spanning tree information

## 9.28 show spanning-tree bridge

This command displays the spanning-tree configuration of the bridge.

```
show spanning-tree bridge [{ address | forward-time | hello-time | id |  
maxage | protocol | priority | detail }]
```

### Syntax Description

**Address** - Bridge Address

**forward-time** - Bridge Forward Time

**hello-time** - Bridge Hello Time

**id** - Bridge ID

**max-age** - Bridge Max Age

**protocol** - Spanning tree Protocol

**priority** - Bridge Priority

**detail** - Bridge Detail

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show spanning-tree bridge address
```

```
Bridge Address is 00:01:02:03:04:21
```

```
SMIS# show spanning-tree bridge forward-time
```

```
Bridge Forward delay is 15 sec
```

```
SMIS# show spanning-tree bridge
```

```
Bridge ID HelloTime MaxAge FwdDly Protocol
```

```
-----
```

```
80:00:00:01:02:03:04:21 2 20 15 rstp
```

```
SMIS# show spanning-tree bridge hello-time
```



Bridge Hello Time is 2 sec

```
SMIS# show spanning-tree bridge id
Bridge ID is 80:00:00:01:02:03:04:21
```

```
SMIS# show spanning-tree bridge max-age
Bridge Max Age is 20 sec
```

```
SMIS# show spanning-tree bridge protocol
Bridge Protocol Running is RSTP
```

```
SMIS# show spanning-tree bridge priority
Bridge Priority is 32768
```

```
SMIS# show spanning-tree bridge detail
Bridge Id Priority 32768,
Address 00:01:02:03:04:21
Hello Time 2 sec, Max Age 20 sec, Forward
Delay 15 sec
```

### Multiple Instance:

```
SMIS# show spanning-tree bridge
Switch - default
MST Instance Bridge ID MaxAge FwdDly Protocol
-----
MST00 0 :00:00:01:02:03:04:01 20 15 mstp
Switch - cust1
MST Instance Bridge ID MaxAge FwdDly Protocol
-----
MST00 0 :00:00:01:02:03:04:02 20 15 mstp
```

```
SMIS# show spanning-tree bridge address
Switch - default
MST00 00:01:02:03:04:01
Switch - cust1
MST00 00:01:02:03:04:0
```

### Related Commands

**spanning-tree timers** - Sets the spanning tree Timers

**spanning-tree mode** - Sets the spanning tree operating mode

**show spanning-tree - Detail** - Displays detailed spanning tree information

**show spanning-tree - Active** - Displays spanning tree information of active ports

## 9.29 show spanning-tree mst - CIST or specified mst Instance

This command displays multiple spanning tree information for the CIST (Common Internal Spanning Tree) Instance or specified MST Instance.

**show spanning-tree mst [<instance-id(1-16)>] [detail]**

### Syntax Description

**instance-id** - Range of Spanning tree instances

**detail** - Spanning tree mst instance specific details

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show spanning-tree mst 1
## MST01
Vlans mapped: 2
Bridge Address 00:01:02:03:04:11 Priority 32768
Root Address 00:01:02:03:04:11 Priority 32768
Root this switch for MST01
Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Master Forwarding 2000000 128.1 SharedLan
```

```
SMIS# show spanning-tree mst 1 detail
## MST01
Vlans mapped: 2
Bridge Address 00:01:02:03:04:11 Priority 32768
Root Address 00:01:02:03:04:11 Priority 32768
Root this switch for MST01
Gi0/1 of MST01 is Master , Forwarding
Port info port id 128.1 priority 128 cost 2000000
```

```
Designated root address 00:01:02:03:04:11 priority 32768
cost 0
Designated bridge address 00:01:02:03:04:11 priority 32768
port id 128.1
```

**Multiple Instance:**

```
SMIS# show spanning-tree mst 1
Switch - default
## MST01
Vlans mapped: 2
Bridge Address 00:01:02:03:04:11 Priority 32768
Root Address 00:01:02:03:04:11 Priority 32768
Root this switch for MST01
Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Master Forwarding 2000000 128.1 SharedLan
```

The option mst is available only when MSTP is the operational mode of the spanning tree.

**Related Commands**

- instance** - Maps VLANS to an MST instance
- spanning-tree priority** - Sets the Bridge Priority for the spanning tree only in steps of 4096
- spanning-tree mst- Properties of an interface for MSTP** - Sets the spanning tree properties of an interface for MSTP

## 9.30 show spanning-tree mst configuration

This command displays multiple spanning tree instance configuration.

**show spanning-tree mst configuration**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Example:

##### Single Instance:

```
SMIS# show spanning-tree mst configuration
```

```
Name [fsoft]
```

```
Revision 2
```

```
Instance Vlans mapped
```

```
-----  
0 1,3-1024,1025-2048,2049-3072,  
3073-4069
```

```
1 2  
-----
```

##### Multiple Instance:

```
SMIS# show spanning-tree mst configuration
```

```
Switch - default
```

```
Name [00:01:02:03:04:01]
```

```
Revision 0
```

```
Instance Vlans mapped
```

```
-----  
0 1-1024,1025-2048,2049-3072,3073-4069  
-----
```

```
Switch - cust1
```

```
Name [00:01:02:03:04:02]
```

```
Revision 0
```

```
Instance Vlans mapped
```

-----  
0 1-1024,1025-2048,2049-3072,3073-4069  
-----

**Related Commands**

**name** - Sets Configuration name

**revision** - Sets the configuration revision number

**instance** - Maps VLANs to an MST instance

## 9.31 show spanning-tree mst - Port Specific Configuration

This command displays multiple spanning tree port specific configuration.

```
show spanning-tree mst [<instance-id(1-16)>] interface <interface-type>
<interface-id> [{ stats | hello-time | detail }]
```

### Syntax Description

**instance-id** - Range of spanning tree instances

**interface** - Details about a particular interface

**stats** - Displays the input and output packets by switching path for the interface

**hello-time** - Determines how often the switch broadcasts its hello message to other switches when it is the root of the spanning tree

**detail** - Detailed multiple spanning tree port specific configuration

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show spanning-tree mst 1 interface gigabitethernet 0/1
Instance Role Sts Cost Prio.Nbr
----- ---- -
1 Master Forwarding 2000000 128.1
```

```
SMIS# show spanning-tree mst 1 interface gigabitethernet 0/1
stats
MST01 Bpdus sent 2, Received 0
```

```
SMIS# show spanning-tree mst 1 interface gigabitethernet 0/1
hello-time
MST01 2
```

```
SMIS# show spanning-tree mst 1 interface gigabitethernet 0/1
detail
Gi0/1 of MST01 is Master , Forwarding
```

```
Port info port id 128.1 priority 128 cost
2000000
Designated root address 00:01:02:03:04:11 priority 32768
cost 0
Designated bridge address 00:01:02:03:04:11 priority 32768
port id 128.1
```

### Related Commands

**instance** - Maps VLANs to an MST instance

**spanning-tree mst hello-time** - Sets the port based hello timer value

**spanning-tree - Properties of an interface** - Sets spanning tree properties of an interface

**show customer spanning-tree** - Displays the detailed customer spanning information

**show spanning-tree mst - CIST or specified mst Instance**- Displays multiple spanning tree information for the CIST Instance or specified MST Instance

**show spanning-tree interface** - Displays Spanning-tree port configuration

**clear spanning-tree detected protocols** - Restarts the protocol migration process on all the interfaces

**clear spanning-tree counters** - Resets all bridge and port level statistics counters



# 10 PNAC

PNAC (Port Based Network Access Control) is a portable implementation of the IEEE Std 802.1x PNAC. It can be used in both LAN Switches and Wireless LAN Access Points for providing security services. When used in LAN Switches, it offers access control to protected resources existing in the switched network. When used in WLAN Access Points, it not only provides authentication of the WLAN stations, but also improves the security by making use of the periodically exchanged key for encrypting the data. PNAC can be very easily ported to different RTOS environments and interfaced to different switch hardware.

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

[dot1x system-auth-control](#)

[aaa authentication dot1x default](#)

[dot1x local-database](#)

[set nas-id](#)

[dot1x default](#)

[dot1x max-req](#)

[dot1x max-start](#)

[dot1x reauthentication](#)

[dot1x timeout](#)

[dot1x port-control](#)

[dot1x access-control](#)

[dot1x control-direction](#)

[dot1x re-authenticate](#)

[shutdown dot1x](#)

[debug dot1x](#)

[show dot1x](#)

## 10.1 dot1x system-auth-control

This command enables dot1x in the switch and the no form of this command disables dot1x in the switch.

```
dot1x system-auth-control
```

```
no dot1x system-auth-control
```

### Mode

Global Configuration Mode

### Defaults

dot1x is enabled

### Example:

```
SMIS(config)# dot1x system-auth-control
```

It is required to enable authentication, authorization, and accounting (AAA) and specify the authentication method before enabling 802.1x globally.

802.1x can be enabled on interfaces, which have Port-channel configured.

### Related Commands

**shutdown dot1x** - Shuts down dot1x capability

**show dot1x** - Displays dot1x information

## 10.2 aaa authentication dot1x default

This command enables the dot1x local authentication or RADIUS server based remote authentication

method for all ports.

```
aaa authentication dot1x default { group radius | local}
```

### Syntax Description

**group radius** - RADIUS server based authentication

**local** - Local authentication

### Mode

Global Configuration Mode

### Defaults

local

### Example:

```
SMIS(config)# aaa authentication dot1x default group radius
```

Only one method can be specified at a time. The 1st method specified will be used and the rest discarded if more than one are typed in.

### Related Commands

**radius-server host** - Specifies RADIUS query parameters

**dot1x local-database** - Configures the dot1x authentication server database with user name and password

**show dot1x** - Displays dot1x detailed information

## 10.3 dot1x local-database

This command configures the dot1x authentication server database with user name and password and the no form of the command deletes an entry from the dot1x authentication server database.

```
dot1x local-database <username> password <password> permission {allow | deny} [  
<auth-timeout (value(1-7200))>] [interface <interface-type>  
<interface-list>]
```

```
no dot1x local-database username
```

### Syntax Description

**Username** - User name

**Password** - Password

**Permission** - Specifies whether the user must be allowed /denied access on a set of ports

**auth-timeout** - Number of seconds between authentication attempts

**interface** - Port list of the interface on which dot1x authentication can be applied

### Mode

Global Configuration Mode

### Defaults

Permission - allow

interface-list - all the physical interfaces

### Example:

```
SMIS(config)# dot1x local-database fsoft password admin123  
permission allow auth-timeout 6000
```

The command adds users to the local database only for local authentication.

The auth-timeout parameter represents the time in seconds after which the access to the port is denied for the user. When the timeout value is 0, the authenticator uses the re-authentication period of the authenticator port.

If the port list is not configured, the user will be allowed/denied access on all the ports.

**Related Commands**

**aaa authentication dot1x default** - Enables the dot1x local authentication

**show dot1x** - Displays dot1x local database information

## 10.4 set nas-id

This command sets the dot1x network access server id.

```
set nas-id <identifier>
```

### Syntax Description

**identifier** - It is a string length of 16 that specifies dot1x network access server ID

### Mode

Global Configuration Mode

### Defaults

fsNas1

### Example:

```
SMIS(config)#set nas-id Identifier
```

Network Access Server Identifier is set in the RADIUS packets sent to the Remote Authentication Server.

### Related Command

**show dot1x** - Displays dot1x information

## 10.5 dot1x default

This command configures dot1x with default values for this port.

**dot1x default**

### Mode

Interface Configuration Mode

### Defaults

Per-interface 802.1X protocol enable state - Enabled (force-authorized)

Periodic reauthentication - Disabled

Number of seconds between reauthentication attempts - 3600 seconds

Quiet period - 60 seconds

Retransmission time - 30 seconds

Maximum retransmission number - 2 times

Client timeout period - 30 seconds

tx period - 30 seconds

Authentication server timeout period - 30 seconds

### Example:

```
SMIS(config-if)# dot1x default
```

### Related Command

**show dot1x** - Displays dot1x interface information

## 10.6 dot1x max-req

This command sets the maximum number of EAP (Extensible Authentication Protocol) retries to the client before restarting authentication process and the no form of the command sets the maximum number of EAP retries to the client to default value.

```
dot1x max-req <count (1-10)>
```

```
no dot1x max-req
```

### Mode

Interface Configuration Mode

### Defaults

Count - 2

### Example:

```
SMIS(config-if)# dot1x max-req 5
```

The default value of this command must be changed only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with RADIUS server/local clients.

### Related Command

```
show dot1x - Displays dot1x information
```



## 10.7 dot1x max-start

This command sets the maximum number of EAPOL retries to the authenticator and the no form of the command sets the maximum number of EAPOL retries to the authenticator to default value.

```
dot1x max-start <count(1-65535)>
```

```
no dot1x max-start
```

### Mode

Interface Configuration Mode

### Defaults

3

### Example:

```
SMIS(config-if)# dot1x max-start 2
```

### Related Command

**show dot1x** - Displays dot1x information

## 10.8 dot1x reauthentication

This command enables periodic re-authentication from authenticator to client and the no form of the command disables periodic re-authentication from authenticator to client.

**dot1x reauthentication**

**no dot1x reauthentication**

### Mode

Interface Configuration Mode

### Defaults

Periodic re-authentication is disabled

### Example:

```
SMIS(config-if)# no dot1x reauthentication
```

The amount of time between periodic re-authentication attempts can be configured by using the dot1x timeout reauth-period interface configuration command.

### Related Commands

**dot1x default** - Configures dot1x with default values for this port

**dot1x timeout** - Sets the dot1x timers

**show dot1x** - Displays dot1x information

## 10.9 dot1x timeout

This command sets the dot1x timers and the no form of the command sets the dot1x timers to the default values.

```
dot1x timeout {quiet-period <value (0-65535)> | {reauth-period |
servertimeout | supp-timeout | tx-period | start-period | held-period |
auth-period }<value (1-65535)>}
```

```
no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-
timeout | tx-period | start-period | held-period | auth-period}
```

### Syntax Description

**quiet-period** - Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client

**reauth-period** - Number of seconds between re-authentication attempts

**server-timeout** - Number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server

**supp-timeout** - Number of seconds that the switch waits for the retransmission of packets by the switch to the client

**tx-period** - Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request

**start-period** - Number of seconds that the supplicant waits between successive retries to the authenticator

**held-period** - Number of seconds that the supplicant waits before trying to acquire the authenticator

**auth-period** - Number of seconds that the supplicant waits before timing-out the authenticator

### Mode

Interface Configuration Mode

### Defaults

quiet-period - 60 seconds

reauth-period - 3600 seconds

server-timeout - 30 seconds

supp-timeout - 30 seconds

tx-period - 30 seconds

start-period - 30 seconds

held-period - 60 seconds

auth-period - 30 seconds

**Example:**

```
SMIS(config-if)# dot1x timeout quiet-period 30
```

```
SMIS(config-if)# dot1x timeout supp-timeout 25
```

Only one timer can be configured using this command, that is, the user can configure either the quiet-period or tx-period, but not both.

**Related Commands**

**dot1x default** - Configures dot1x with default values for this port

**dot1x max-req** - Sets the maximum number of EAP retries to the client before restarting authentication process

**dot1x reauthentication** - Enables periodic re-authentication of the client

**show dot1x** - Displays dot1x information

## 10.10 dot1x port-control

This command configures the authenticator port control parameter and the no form of the command sets the authenticator port control state to force authorized.

```
dot1x port-control {auto|force-authorized|force-unauthorized}
```

```
no dot1x port-control
```

### Syntax Description

**force-authorized** - All the traffic will be allowed without any restrictions

**forceunauthorized** - All the traffic over the interface will be blocked

**auto** - Enables 802.1x authentication on the interface and cause the port to transition to the authorized or unauthorized state based on the 802.1x authentication exchange between the server and the client

### Mode

Interface Configuration Mode

### Defaults

force-authorized

### Example:

```
SMIS(config-if)# dot1x port-control auto
```

The auto keyword can be used only if the port is not configured.

The 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3 routed ports.

### Related Commands

**dot1x default** - Configures dot1x with default values for this port

**show dot1x** - Displays dot1x information

## 10.11 dot1x access-control

This command configures the supplicant access control and the no form of the command sets the access control to inactive.

```
dot1x access-control {active | inactive}
```

```
no dot1x access-control
```

### Syntax Description

**active** - The port status is the combined port status of the authenticator and supplicant

**inactive** - The port status is the port status of authenticator

### Mode

Interface Configuration Mode

### Defaults

inactive

### Example:

```
SMIS(config-if)# dot1x access-control active
```

### Related Command

**show dot1x** - Displays dot1x information

## 10.12 dot1x control-direction

This command configures port control direction and the no form of the command sets the authenticator port control direction to both.

```
dot1x control-direction {in | both}
```

```
no dot1x control-direction
```

### Syntax Description

**in** - Authentication control is imposed only on the incoming packets

**both** - Authentication control is imposed on both incoming and outgoing packets

### Mode

Interface Configuration Mode

### Defaults

both

### Example:

```
SMIS(config-if)# dot1x control-direction in
```

### Related Command

**show dot1x** - Displays dot1x information

## 10.13 dot1x re-authenticate

This command initiates re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port.

```
dot1x re-authenticate [interface <interface-type><interface-id>]
```

### Syntax Description

**Interface** - Port number of the interface to re-authenticate

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# dot1x re-authenticate interface fastethernet 0/1
```

The command re-authenticates a client without waiting for the configured number of seconds between re-authentication attempts (re-authperiod) and automatic reauthentication.

If no interface is specified, reauthentication is initiated on all dot1x ports.

### Related Command

**show dot1x** - Displays dot1x information



## 10.14 shutdown dot1x

This command shuts down dot1x capability and the no form of the command starts and enables dot1x capability.

**shutdown dot1x**

**no shutdown dot1x**

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# shutdown dot1x
```

When shutdown, all resources acquired by dot1x Module are released to the system.

### Related Commands

**dot1x system-auth-control** - Enables dot1x in the switch

**show dot1x** - Displays dot1x information

## 10.15 debug dot1x

This command enables debugging of dot1x module and the no form of the command disables debugging of dot1x module.

```
debug dot1x {all | errors | events | packets | state-machine |  
redundancy}
```

```
no debug dot1x {all | errors | events | packets | state-machine |  
redundancy}
```

### Syntax Description

**all** - All dot1x debug messages

**errors** - dot1x error code debug messages

**events** - dot1x event debug messages

**packets** - dot1x packet debug messages

**state-machine** - State-machine related-event debug messages

**redundancy** - Redundancy related debug messages

### Mode

Privileged EXEC Mode

### Defaults

Events Debugging is enabled

### Example:

```
SMIS# debug dot1x all
```

A four byte integer is used for enabling the level of tracing. Each BIT in the four byte integer, represents a particular level of Trace.

### Related Command

**show dot1x** - Displays dot1x information

## 10.16 show dot1x

This command displays dot1x information.

```
show dot1x [{ interface <interface-type> <interface-id> | statistics
interface <interface-type> <interface-id> | supplicant-statistics
interface <interfacetype> <interface-id>|local-database | mac-info
[address <aa.aa.aa.aa.aa.aa>] | mac-statistics [address
<aa.aa.aa.aa.aa.aa>] | all }]
```

### Syntax Description

**interface** - dot1x status for the specified interface

**statistics interface** - dot1x authenticator statistics for the switch or the specified interface

**supplicantstatistics interface** - dot1x supplicant statistics for the switch or the specified interface

**local-database** - dot1x authentication server database with user name and password

**mac-info** - dot1x MAC session

**mac-statistics** - dot1x MAC statistic

**all** - dot1x status for all interfaces

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show dot1x
Sysauthcontrol = Enabled
Dot1x Protocol Version = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
Dot1x Authentication Method = Local
Nas ID = fsNas1
```

```
SMIS# show dot1x local-database
Pnac Authentication Users Database
-----
User name : brg2
```

```
Protocol : 4
Timeout : 0 seconds
Ports : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6, Gi0/7,
Gi0/8, Gi0/9,
Gi0/10, Gi0/11, Gi0/12, Gi0/13, Gi0/14, Gi0/15, Gi0/16, Gi0/17,
Gi0/18, Gi0/19,
Gi0/20, Gi0/21, Gi0/22, Gi0/23, Gi0/24
Permission : Allow
```

-----

```
SMIS# show dot1x all
When access-control is made inactive for Gi0/1 and Gi0/2:
Dot1x Info for Gi0/1
```

-----

```
PortStatus = AUTHORIZED
AccessControl = INACTIVE
AuthSM State = FORCE AUTHORIZED
BendSM State = INITIALIZE
AuthPortStatus = AUTHORIZED
ControlDirection = BOTH
MaxReq = 2
Port Control = Force Authorized
QuietPeriod = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
Tx Period = 30 Seconds
Dot1x Info for Gi0/2
```

-----

```
PortStatus = AUTHORIZED
AccessControl = INACTIVE
AuthSM State = INITIALIZE
BendSM State = INITIALIZE
AuthPortStatus = AUTHORIZED
ControlDirection = BOTH
MaxReq = 2
```

Port Control = Force Authorized

QuietPeriod = 60 Seconds

Re-authentication = Disabled

ReAuthPeriod = 3600 Seconds

ServerTimeout = 30 Seconds

SuppTimeout = 30 Seconds

Tx Period = 30 Seconds

If access-control for only Gi0/1 is made active then display will be as given below:

Dot1x Info for Gi0/1

-----

PortStatus = UNAUTHORIZED

AccessControl = ACTIVE

AuthSM State = CONNECTING

SuppSM State = AUTHENTICATED

BendSM State = IDLE

AuthPortStatus = UNAUTHORIZED

SuppPortStatus = AUTHORIZED

ControlDirection = BOTH

MaxReq = 2

Port Control = Auto

QuietPeriod = 60 Seconds

Re-authentication = Disabled

ReAuthPeriod = 3600 Seconds

ServerTimeout = 30 Seconds

SuppTimeout = 30 Seconds

Tx Period = 30 Seconds

Start Period = 30 Seconds

Held Period = 60 Seconds

Auth Period = 30 Seconds

Dot1x Info for Gi0/2

-----

PortStatus = AUTHORIZED

AccessControl = INACTIVE

AuthSM State = INITIALIZE

BendSM State = INITIALIZE

AuthPortStatus = AUTHORIZED

```
ControlDirection = BOTH
MaxReq = 2
Port Control = Force Authorized
QuietPeriod = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
Tx Period = 30 Seconds
```

```
SMIS# show dot1x statistics interface gigabitethernet 0/1
```

```
PortStatistics Parameters for Dot1x
```

```
-----
TxReqId = 1
TxReq = 0
TxTotal = 1
RxStart = 0
RxLogoff = 0
RxRespId = 0
RxResp = 0
RxInvalid = 0
RxLenErr = 0
RxTotal = 0
RxVersion = 0
LastRxSrcMac = 00:00:00:00:00:00
```

```
SMIS# show dot1x supplicant-statistics interface gigabitethernet 0/1
```

```
PortStatistics Parameters for Dot1x-Supplicant
```

```
-----
TxStart = 2
TxRespId = 0
TxResp = 0
TxLogoff = 0
TxTotal = 2
RxReqId = 0
RxReq = 0
RxInvalid = 0
```

```
RxLenErr = 0
RxTotal = 0
RxVersion = 0
LastRxSrcMac = 00:00:00:00:00:00
```

If an interface is not specified, global parameters and a summary appear.

Expressions are case sensitive.

If address is not specified for mac-info and mac-statistics, then this command displays the MAC sessions and MAC statistics of all the supplicant MAC addresses.

### **Related Command**

**dot1x default** - Configures dot1x with default values for that port.

# 11 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, mode servers, switches, etc. 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.
- 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](#)



## 11.1 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 <ip-address> [timeout <1-120>] [retransmit <1-254>]  
key <secret-key-string>
```

```
no radius-server host <ip address>
```

### Syntax Description

**timeout** - The time period in seconds for which a client will wait for a response from the server before re-transmitting the request.

**Retransmit** - The maximum number of attempts the client undertakes to contact the server

**key** - Per-server encryption key. Specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server. The string length is 46.

### Mode

Global Configuration Mode

### Defaults

Timeout - 3 seconds

Retransmit - 3 attempts

Key - empty string

### Example:

```
SMIS(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

## 11.2 debug radius

This command enables RADIUS debugging options and the no form of the command disables RADIUS debugging options.

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

```
no debug radius
```

### Syntax Description

**all** - All the RADIUS server messages

**errors** - Error code debug messages

**events** - Events related messages

**packets** - Packets related messages

**responses** - Server response related messages

**timers** - Timer module related messages

### Mode

Privileged EXEC Mode

### Defaults

Debugging is Disabled

### Example:

```
SMIS# debug radius all
```

### Related Command

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

## 11.3 show radius server

This command displays RADIUS server configuration.

**show radius server**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show radius server
Radius Server Host Information
-----
Index : 1
Server address : 10.0.0.1
Shared secret : admin123
Radius Server Status : Enabled
Response Time : 20
Maximum Retransmission : 8
-----
```

### Related Command

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

## 11.4 show radius statistics

This command displays RADIUS Server Statistics.

**show radius statistics**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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

# 12 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 Network Access Security (NAS). NAS ensures secure access from remotely connected users. TACACS implements the TACACS Client and provides the Authentication, Authorization and Accounting (AAA) 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](#)

[aaa authentication tacacs](#)

[aaa authorization group tacacs](#)

[debug tacacs](#)

[show tacacs](#)

## 12.1 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 <ip-address> [single-connection] [port <TCP port>]  
[timeout <time out in seconds>] [key <secret key>]
```

```
no tacacs-server host <ip-address>
```

### Syntax Description

**single-connection** - Establishes Single TCP connection to communicate with TACACS Server

**port** - TCP Port number

**timeout** - The time period in seconds for which a client will wait for a response from the server before closing the connection

**key** - Per-server encryption key. Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The string length is 64.

### Mode

Global Configuration Mode

### Defaults

Port - 40

Timeout - 5 seconds

### Example:

```
SMIS(config)# tacacs-server host 10.0.0.100 key SuperMicroTACACS
```

### Related Commands

**show tacacs** - Displays the statistical log information and server for TACACS client

## 12.2 tacacs use-server address

This command selects a server from the list of servers maintained in the TACACS client and makes the TACACS client to use the specified server. The no form of the command disables the configured TACACS active server.

```
tacacs use-server address<ip-address>
```

```
no tacacs use-server
```

### **Mode**

Global Configuration Mode

### **Example:**

```
SMIS(config)# tacacs use-server address 10.0.0.100
```

### **Related Commands**

**show tacacs** - Displays the statistical log information and server for TACACS client

## 12.3 tacacs-server retransmit

This command specifies the number of times the client searches the active server from the list of servers maintained in the TACACS client, when active server is not configured. The no form of the command sets the default retries.

```
tacacs-server retransmit <1-100>
```

```
no tacacs-server retransmit
```

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# tacacs-server retransmit 3
```



## 12.4 aaa authentication tacacs

This command selects the authentication method used for transmitting a password to the TACACS server. The default method used is pap. The “no” form of the command selects the default method pap.

```
aaa authentication tacacs { chap | pap }
```

```
no aaa authentication tacacs
```

### Mode

Global Configuration Mode

### Default

pap

### Example:

```
SMIS(config)# aaa authentication tacacs chap
```

### Related Commands

**show running-config** - Displays the currently running configuration

## 12.5 **aaa authorization group tacacs**

This command configures the switch to receive and process a privilege level from the TACACS+ server. By default the switch does not request and use the privilege level from TACACS+ server. The “no” form of this command makes the switch not request and use the privilege level from TACACS+ server.

```
aaa authorization group tacacs
```

```
no aaa authorization group tacacs
```

### **Mode**

Global Configuration Mode

### **Default**

No authorization.

### **Example:**

```
SMIS(config)# aaa authorization group tacacs
```

### **Related Commands**

**show running-config** - Displays the currently running configuration

## 12.6 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 Description

**all** - All TACACS debug messages

**info** - TACACS Server information messages

**errors** - Error code debug messages

**dumptx** - Transmitted packet dump messages

**dumprx** - Received packet dump messages

### Mode

Privileged EXEC Mode

### Defaults

Debugging is Disabled

### Example:

```
SMIS# debug tacacs all
```

## 12.7 show tacacs

This command displays the statistical log information and server for TACACS+ client.

**show tacacs**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show tacacs
Server : 1
Address : 10.0.0.5
Single Connection : no
TCP port : 49
Timeout : 5
Secret Key : SuperMicroTACACS
Server : 2
Address : 12.0.0.5
Single Connection : no
TCP port : 49
Timeout : 5
Secret Key : SuperMicroTACACS
Client uses server: 12.0.0.5
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
Acct. Errors rcvd. : 0
Acct. Follows rcvd. : 0
Acct. Sess. timeouts : 0
Malformed Pkts. rcvd. : 0
Socket failures : 0
Connection failures : 0
```

### Related Commands

**tacacs-server host** - Configures the TACACS server with the parameters

**tacacs use-server address** - Selects a server from the list of servers maintained in the TACACS client and makes the TACACS client to use the specified server

## 13 Link Aggregation (LA)

**Link Aggregation (LA)** is a method of combining multiple parallel physical connections into a single logical connection(trunk), thus allowing increased bandwidth for a particular network path beyond what a single connection could sustain. By taking multiple LAN connections and treating them as a unified, aggregated link, practical benefits in many applications can be achieved. For example, link aggregation provides redundancy in case one of the links fails. Link Aggregation also provides load balancing so that processing and communication activity is distributed across several links in a trunk ensuring that no single link is overwhelmed.

Other terms often used to describe this Link Aggregation method include **port trunking**, **link bundling**, **bonding**, or **teaming**. These umbrella terms encompass industry standards such as IEEE 802.1ax Link Aggregation Control Protocol (LACP) for wired Ethernet, or the previous **IEEE 802.3ad**, as well as various proprietary solutions. In this manual we will also refer to a particular group of aggregated links as a **Port Channel**.

Supermicro switches support both static link aggregation and dynamic link aggregation using IEEE 802.3ad and LACP. Up to 24 Port Channels can be configured on an individual switch and each Port Channel can contain up to 8 members.

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

[set port-channel](#)

[lACP system-priority](#)

[port-channel load-balance](#)

[lACP port-priority](#)

[channel-group](#)

[lACP wait-time](#)

[lACP timeout](#)

[show etherchannel](#)

[show interfaces](#)

[show lACP](#)

[debug la](#)

## 13.1 set port-channel

This command enables/disables link aggregation in the switch.

```
set port-channel { enable | disable }
```

### Syntax Description

**enable** - Enables link aggregation in the switch

**disable** - Disables link aggregation in the switch

### Mode

Global Configuration Mode

### Defaults

Enable

### Example:

```
SMIS(config)# set port-channel enable
```

### Related Command

**show etherchannel** - Displays etherchannel information

## 13.2 lacp system-priority

This command sets the LACP priority for the system and the no form of the command sets the LACP priority for the system to the default value. System Priority represents a 2-octet value indicating the priority value associated with the system involved in link aggregation.

```
lacp system-priority <0-65535>
```

```
no lacp system-priority
```

### Mode

Global Configuration Mode

### Defaults

0x8000 or 32768

### Example:

```
SMIS(config)# lacp system-priority 5
```

The switch with the lowest system priority value decides the standby and active links in the aggregation.

Although this is a global configuration command, the priority only takes effect on EtherChannels that have physical interfaces with LACP enabled.

### Related Command

```
show etherchannel - Displays lacp system-priority value
```



## 13.3 port-channel load-balance

This command sets the load balancing policy and the no form of the command sets the load balancing policy to the default value.

```
port-channel load-balance {src-mac | dest-mac | src-dest-mac| src-ip |  
dest-ip | src-dest-ip } [ <port-channel-index(1-65535)>]
```

```
no port-channel load-balance [ <port-channel-index(1-65535)> ]
```

### Syntax Description

**src-mac** - Load distribution is based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port

**dest-mac** - Load distribution is based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel

**src-dest-mac** - Load distribution is based on the source and destination MAC address

**src-ip** - Load distribution is based on the source IP address

**dest-ip** - Load distribution is based on the destination IP address

**src-dest-ip** - Load distribution is based on the source and destination IP address

**port-channelindex** - Port channel number

### Mode

Global Configuration Mode

### Defaults

source and destination MAC address based

### Example:

```
SMIS(config)# port-channel load balance dest-mac 28
```

If the port-channel index is not mentioned in this command the load-balancing must apply for all port-channels configured in the system.

Initially, the port channel interface must have been configured for this command.

### Related Command

**show etherchannel** - Displays etherchannel load balance information

## 13.4 lacp port-priority

This command sets the LACP port priority and the no form of the command sets the LACP port priority to the default value. Port priority determines whether the link is an active link or a standby link, when the number of ports in the aggregation exceeds the maximum number supported by the hardware

```
lacp port-priority <0-65535>
```

```
no lacp port-priority
```

### Mode

Interface Configuration Mode

### Defaults

port-priority - 128

### Example:

```
SMIS(config-if)# lacp port-priority 1
```

This command takes effect only on EtherChannel interfaces that are already configured for LACP.

If the number of links in an aggregation exceeds the maximum supported by the hardware, then the links with lower priority become active links.

### Related Commands

**lacp system-priority** - Globally sets the LACP priority

**show etherchannel** - Displays etherchannel detailed / port information

## 13.5 channel-group

This command configures an Etherchannel and the no form of the command removes an interface from the Etherchannel.

```
channel-group <channel-group-number(1-65535)> mode {active | passive | on}
```

```
no channel-group
```

### Syntax Description

**channel-group-number** - The port channel number to which this interface is to be added. If there is no port channel configured with the given channel group number, switch will create a port channel automatically and add this interface.

**mode** - mode represents any one of the following:

**active** - LACP negotiation is started un-conditionally

**passive** - LACP negotiation is started only when LACP packet is received from peer

**on** - Force the interface to channel without LACP. This is equivalent to manual aggregation

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# channel-group 1 mode active
```

### Related Command

**show etherchannel** - Displays etherchannel detailed / port information

## 13.6 lacp wait-time

This command sets the LACP wait-time and the no form of the command sets the LACP wait-time to the default value.

```
lacp wait-time <0-10>
```

```
no lacp wait-time
```

### Mode

Interface Configuration Mode

### Defaults

2

### Example:

```
SMIS(config-if)# lacp wait-time 1
```

Configuring the wait-time value as 0 ensures that links get aggregated immediately.

### Related Command

```
show etherchannel - Displays etherchannel detailed / port information
```

## 13.7 lacp allow-zero-partner-key

This command allows the Supermicro Intelligent Switch to establish a connection with some particular switch (such as a Cisco Nexus OS) which uses an admin key of zero to negotiate an LACP connection.

```
lacp allow-zero-partner-key { enable | disable }
```

### Mode

Interface Configuration Mode

### Defaults

Disable

### Example:

```
SMIS(config-if)# lacp allow-zero-partner-key enable
```

### Related Command

```
show etherchannel - Displays etherchannel detailed / port information
```

## 13.8 lacp timeout

This command sets the LACP timeout period and the no form of the command sets the LACP timeout period to the default value.

```
lacp timeout {long | short }
```

```
no lacp timeout
```

### Syntax Description

**long** - Long timeout value

**short** - Short timeout value

### Mode

Interface Configuration Mode

### Defaults

long

### Example:

```
SMIS(config-if)# lacp timeout short
```

The long timeout value means that LACP PDU will be sent every 30 seconds and LACP timeout value (no packet is received from peer ) is 90 seconds.

The short timeout value means that LACP PDU will be sent every 1 second and timeout value is 3 seconds.

### Related Command

**show etherchannel** - Displays etherchannel detailed / portinformation

## 13.9 show etherchannel

This command displays etherchannel information.

```
show etherchannel [[channel-group-number] { detail | load-balance |
port | port-channel | summary | protocol}]
```

### Syntax Description

**channel-groupnumber** - Number of the channel group. Valid numbers range from maximum number of ports in the system to maximum number of aggregations supported

**detail** - Detailed EtherChannel information

**load-balance** - Load-balance or frame-distribution scheme among ports in the port channel

**port** - EtherChannel port information

**port-channel** - Port-channel information

**summary** - Protocol that is being used in the EtherChannel

**protocol** - One-line summary per channel-group

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show etherchannel
Port-channel is enabled
Max Port Channels is 24 with maximum 8 active ports per port
channel
Channel Group Listing
-----
Group : 1
-----
Protocol : LACP
```

```
SMIS# show etherchannel 1 detail
Port-channel is enabled
Max Port Channels is 24 with maximum 8 active ports per port
channel
LACP System Priority: 32768
Channel Group Listing
```



-----

Group: 1

-----

Protocol :LACP

Ports in the Group

-----

Port : Gi0/1

-----

Port State = Up in Bundle

Channel Group : 1

Mode

: Active

Pseudo port-channel = Po1

LACP port-priority = 128

LACP Wait-time = 2 secs

LACP Activity : Active

LACP Timeout : Long

Aggregation State : Aggregation, Sync, Collecting, Distributing,

Port : Gi0/2

-----

Port State = Up in Bundle

Channel Group : 1

Mode

: Active

Pseudo port-channel = Po1

LACP port-priority = 128

LACP Wait-time = 2 secs

LACP Activity : Active

LACP Timeout : Long

Aggregation State : Aggregation, Sync, Collecting, Distributing

Port-channel : Po1

-----

```
Number of Ports = 2
HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = LACP
MAC selection = Dynamic
```

```
SMIS# show etherchannel 1 port
```

```
Channel Group Listing
```

```
-----
```

```
Group: 1
```

```
-----
```

```
Protocol :LACP
```

```
Ports in the Group
```

```
-----
```

```
Port : Gi0/1
```

```
-----
```

```
Port State = Up in Bundle
```

```
Channel Group : 1
```

```
Mode
```

```
: Active
```

```
Pseudo port-channel = Po1
```

```
LACP port-priority = 128
```

```
LACP Wait-time = 2 secs
```

```
LACP Port Identifier = 2
```

```
LACP Activity : Active
```

```
LACP Timeout : Long
```

```
Aggregation State : Aggregation, Sync, Collecting, Distributing,
```

```
Port : Gi0/2
```

```
-----
```

```
Port State = Up in Bundle
```

```
Channel Group : 1
```

```
Mode
```

```
: Active
```

```
Pseudo port-channel = Po1
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Activity : Active
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing,
LACP Port Admin Oper Port Port
Port State Priority Key Key Number State
```

```
-----
Gi0/1 Bundle 128 1 1 0x1 0xbc
Gi0/2 Bundle 128 1 1 0x2 0xbc
```

```
SMIS# show etherchannel 1 port-channel
Port-channel is enabled
Max Port Channels is 24 with maximum 8 active ports per port
channel
```

```
Channel Group Listing
```

```
-----
Group : 1
```

```
-----
Port-channels in the group:
```

```
-----
Port-channel : Po1
```

```
-----
Number of Ports = 2
HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = LACP
MAC selection = Dynamic
```

```
SMIS# show etherchannel 1 summary
```

```
Flags:
```

```
D - down P - in port-channel
I - stand-alone S - suspended
H - Hot-standby (LACP only)
```

```
Port-channel is enabled
```

```
Port-channel System Identifier is 00:01:02:03:04:05
```

Number of channel-groups in use: 1

Number of aggregators: 1

Group Port-channel Protocol Ports

-----  
1 Po1(P) LACP Gi0/1(P),Gi0/2(P)

SMIS# show etherchannel 1 protocol

Channel Group Listing

-----  
Group : 1

-----  
Protocol : LACP

SMIS# show etherchannel load-balance

Channel Group Listing

-----  
Group : 1

-----  
Source IP Address

If the channel group number is not specified details on all channels are displayed.

#### Related Commands

**channel-group** - Assigns an Ethernet interface to an EtherChannel group

**set port-channel** - Enables/disables link aggregation in the switch

**lACP system-priority** - Sets the LACP priority for the system

**port-channel load-balance** - Sets the load balancing policy

**lACP port-priority** - Sets the LACP port priority

**lACP wait-time** - Sets the LACP wait-time

**lACP timeout** - Sets the LACP timeout period

**show interfaces** - Displays interface specific port-channel information

## 13.10 show interfaces

This command displays interface specific port-channel information.

```
show interfaces [<interface-type> <interface-id> ] etherchannel
```

### Syntax Description

**Etherchannel** - Interface EtherChannel information

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show interfaces gigabitethernet 0/1 etherchannel
```

```
Port : Gi0/1
```

```
-----
```

```
Port State = Up in Bundle
```

```
Channel Group : 2
```

```
Mode
```

```
: Active
```

```
Pseudo port-channel = Po2
```

```
LACP port-priority = 128
```

```
LACP Port Identifier = 2
```

```
LACP Wait-time = 2 secs
```

```
LACP Activity : Passive
```

```
LACP Timeout : Long
```

```
Aggregation State : Aggregation, Sync, Collecting, Distributing,
```

```
LACP Port Admin Oper Port Port
```

```
Port State Priority Key Key Number State
```

```
-----
```

```
Gi0/1 Bundle 128 2 2 0x1 0x3c
```

```
SMIS# show interfaces etherchannel
```

```
Port : Gi0/1
```

```
-----
```

```
Port State = Up in Bundle
```

Channel Group : 2

Mode

: Active

Pseudo port-channel = Po2

LACP port-priority = 128

LACP Wait-time = 2 secs

LACP Activity : Passive

LACP Timeout : Long

Aggregation State : Aggregation, Sync, Collecting, Distributing,

Port : Gi0/2

-----

Port State = Up in Bundle

Channel Group : 2

Mode

: Active

Pseudo port-channel = Po2

LACP port-priority = 128

LACP Wait-time = 2 secs

LACP Activity : Passive

LACP Timeout : Long

Aggregation State : Aggregation, Sync, Collecting, Distributing,

LACP Port Admin Oper Port Port

Port State Priority Key Key Number State

-----

Gi0/1 Bundle 128 2 2 0x1 0x3c

Gi0/2 Bundle 128 2 2 0x2 0x3c

Port-channel : Po2

```
-----  
Number of Ports = 2  
HotStandBy port = null  
Port state = Port-channel Ag-Inuse  
Protocol = LACP  
MAC selection = Dynamic
```

Expressions are case sensitive.

The port-channel range is 1 to 64.

### Related Commands

**set port-channel** - Enables/disables link aggregation in the switch

**channel-group** - Assigns an Ethernet interface to an EtherChannel group

**port-channel load-balance** - Sets the load balancing policy

**lacp port-priority** - Sets the LACP port priority

**lacp wait-time** - Sets the LACP wait-time

**lacp timeout** - Sets the LACP timeout period

**show etherchannel** - Displays etherchannel information

## 13.11 show lacp

This command displays port-channel traffic/neighbor information.

```
show lacp [<port-channel(1-65535)>] { counters | neighbor [detail] }
```

### Syntax Description

**port-channel** - Number of the channel group

**counters** - Traffic information

**neighbor** - Neighbor information

**detail** - Neighbor detail information

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show lacp 1 counters
LACPDU  Marker  Market  Response  LACPDUs
Port  Sent  Recv  Sent  Recv  Sent  Recv  Pkts  Err
-----
Channel group: 1
-----
Gi0/1  394  352  0  0  0  0  0  0
Gi0/2  318  297  0  0  0  0  0  0
```

```
SMIS# show lacp neighbor detail
Flags:
A - Device is in Active mode
P - Device is in Passive mode

Channel group 1 neighbors
Port Gi0/1
-----
Partner System ID : 00:01:02:03:04:21
Flags : P
LACP Partner Port Priority : 128
LACP Partner Oper Key : 2
```



```
LACP Partner Port State : 0x3c
Port State Flags Decode
-----
Activity : Passive
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting,
Distributing
Port Gi0/2
-----
Partner System ID : 00:01:02:03:04:21
Flags : P
LACP Partner Port Priority : 128
LACP Partner Oper Key : 2
LACP Partner Port State : 0x3c
Port State Flags Decode
-----
Activity : Passive
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting,
Distributing
```

Expressions are case sensitive

### Related Commands

**lACP wait-time** - Sets the LACP wait-time

**lACP timeout** - Sets the LACP timeout period

**channel-group** - Assigns an Ethernet interface to an EtherChannel group

**show interfaces** - Displays interface specific port-channel information

**show etherchannel** - Displays etherchannel detailed information

## 13.12 debug la

This command enables the display of link aggregation debug messages.

The no form of this command disables the display of link aggregation debug messages.

```
debug la [{all | [init-shut] [mgmt] [data] [ctrl] [pkt-dump] [resource]
[all-fail] [buf] [sel] [pdu <iftype> <ifnum>] }]
```

```
no debug la [{all | [init-shut] [mgmt] [data] [ctrl] [pkt-dump]
[resource] [all-fail] [buf] [sel] [pdu <iftype> <ifnum>] }]
```

### Syntax Description

**all** – displays all debug messages

**init-shut** – displays initialization and shutdown messages

**mgmt** – displays management messages

**data** – displays all data path messages

**ctrl** – displays all control messages

**pkt-dump** – displays the contents of all LACP packets

**resource** – displays the resources (like memory) utilization debug messages

**all-fail** – displays all failure events

**buf** – displays the buf utilization debug messages

**sel** – displays the selector related debug messages

**pdu** – displays all the LACP packets received and transmitted on the given interface

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged/User EXEC Mode

### Defaults

Disabled

### Example:

```
SMIS# debug la all
```

### Related Commands

## 14 IGMP Snooping

IGMP (Internet Group Multicast Protocol), is the protocol a host uses to inform a router when it joins (or leaves) an Internet multicast group. IGMP is only used on a local network; a router must use another multicast routing protocol to inform other routers of group membership. IGS (IGMP Snooping), is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers. In IGS, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. If another computer snoops such packets, the other computer can learn the multicast sessions to which other computers on the local network are listening. IGMP snooping significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

The list of CLI commands for the configuration of IGS are common to both **Single Instance and Multiple Instance** except for a difference in the prompt that appears for the Switch with Multiple Instance support.

The prompt for the **Global Configuration Mode** is,

```
SMIS (config-switch) #
```

The **parameters** specific to Multiple Instance are stated so, against the respective parameter descriptions in this document.

The output of the **Show commands** differ for Single Instance and Multiple Instance. Hence both the output are documented while depicting the show command Example:s.

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

[ip igmp snooping](#)

[ip igmp snooping proxy-reporting](#)

[snooping multicast-forwarding-mode](#)

[ip igmp snooping mrouter-time-out](#)

[ip igmp snooping port-purge-interval](#)

[ip igmp snooping report-suppression interval](#)

[ip igmp snooping retry-count](#)

[ip igmp snooping group-query-interval](#)

[ip igmp snooping report-forward](#)

[ip igmp snooping version](#)

[ip igmp snooping fast-leave](#)

[ip igmp snooping querier](#)

[ip igmp snooping query-interval](#)

[ip igmp snooping mrouter](#)

[ip igmp snooping send-query](#)

[ip igmp snooping clear counters](#)

[shutdown snooping](#)

[debug ip igmp snooping](#)

[show ip igmp snooping mrouter](#)

[show ip igmp snooping globals](#)

[show ip igmp snooping](#)

[show ip igmp snooping groups](#)

[show ip igmp snooping forwarding-database](#)

[show ip igmp snooping statistics](#)

## 14.1 ip igmp snooping

This command enables IGMP snooping in the switch/a specific VLAN and the no form of the command disables IGMP snooping in the switch/a specific VLAN.

```
ip igmp snooping
```

```
no ip igmp snooping
```

### Mode

Global Configuration Mode / Config-VLAN Mode

### Defaults

IGMP snooping is globally disabled

### Example:

```
SMIS(config)# ip igmp snooping
SMIS(config-vlan)# ip igmp snooping
```

When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces. When IGMP snooping is disabled globally, it is disabled in all the existing VLAN interfaces.

GMRP has to be disabled for the IGMP snooping to be enabled.

### Related Commands

**shutdown snooping** - Shuts down IGMP snooping in the switch

**show ip igmp snooping** - Displays IGMP snooping information for all VLANs or a specific VLAN

**show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN

**snooping multicast-forwarding-mode**

– Specifies the snooping multicast forwarding mode

## 14.2 ip igmp snooping proxy-reporting

This command enables proxy reporting in the IGMP snooping switch and the no form of the command disables proxy reporting in the IGMP snooping switch.

```
ip igmp snooping proxy-reporting
```

```
no ip igmp snooping proxy-reporting
```

### Mode

Global Configuration Mode

### Defaults

Proxy-reporting is enabled

### Example:

```
SMIS(config)# ip igmp snooping proxy-reporting
```

### Related Command

`show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a specific VLAN

## 14.3 snooping multicast-forwarding-mode

This command specifies the snooping multicast forwarding mode (IP based or MAC based).

```
snooping multicast-forwarding-mode {ip | mac}
```

### Syntax Description

**ip** - IP Address based

**mac** - MAC Address based

### Mode

Global Configuration Mode

### Defaults

ip

### Example:

```
SMIS(config)# snooping multicast-forwarding-mode mac
```

### Related Command

**show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN

## 14.4 ip igmp snooping mrouter-time-out

This command sets the IGMP snooping router port purge time-out after which the port gets deleted if no IGMP router control packets are received. The no form of the command sets the IGMP snooping router port purge time-out to default value.

```
ip igmp snooping mrouter-time-out <(60 - 600) seconds>
```

```
no ip igmp snooping mrouter-time-out
```

### Mode

Global Configuration Mode

### Defaults

125

### Example:

```
SMIS(config)#ip igmp snooping mrouter-time-out 70
```

### Related Command

```
show ip igmp snooping mrouter - Displays the router ports for all VLANs or specific VLAN
```



## 14.5 ip igmp snooping port-purge-interval

This command sets the IGMP snooping port purge time interval after which the port gets deleted if no IGMP reports are received. The no form of the command sets the IGMP snooping port purge time to default value.

```
ip igmp snooping port-purge-interval <(130 - 1225) seconds>
```

```
no ip igmp snooping port-purge-interval
```

### Mode

Global Configuration Mode

### Defaults

260

### Example:

```
iss (config)# ip igmp snooping port-purge-interval 150
```

### Related Command

**show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN

## 14.6 ip igmp snooping report-suppression interval

This command sets the IGMP snooping report-suppression time interval for which the IGMPv2 report messages for the same group will not get forwarded onto the router ports. The no form of the command sets the IGMP snooping report-suppression interval time to the default value.

```
ip igmp snooping report-suppression-interval <(1 - 25) seconds>
```

```
no ip igmp snooping report-suppression-interval
```

### Mode

Global Configuration Mode

### Defaults

5

### Example:

```
SMIS(config)# ip igmp snooping report-suppression-interval 20
```

### Related Command

**show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN

## 14.7 ip igmp snooping retry-count

This command sets the maximum number of group specific queries sent on a port on reception of a IGMPv2 leave message. The no form of the command sets the number of group specific queries sent on a port on reception of leave message to default value.

```
ip igmp snooping retry-count <1 - 5>
```

```
no ip igmp snooping retry-count
```

### Mode

Global Configuration Mode

### Defaults

2

### Example:

```
iss (config)# ip igmp snooping retry-count 4
```

### Related Command

**show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN

## 14.8 ip igmp snooping group-query-interval

This command sets the time interval after which the switch sends a group specific query on a port. The no form of the commands sets the group specific query interval time to default value.

```
ip igmp snooping group-query-interval <2-5> seconds>
```

```
no ip igmp snooping group-query-interval
```

### Mode

Global Configuration Mode

### Defaults

2

### Example:

```
SMIS(config)# ip igmp snooping group-query-interval 3
```

### Related Commands

**show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN

**show ip igmp snooping statistics** - Displays IGMP snooping statistics for all VLANs or a specific VLAN

**show ip igmp snooping groups** - Displays IGMP group information for all VLANs or a specific VLAN

## 14.9 ip igmp snooping report-forward

This command specifies if IGMP reports must be forwarded on all ports or router ports of a VLAN and the no form of the command sets IGMP report-forwarding status to default value.

```
ip igmp snooping report-forward {all-ports | router-ports}
```

```
no ip igmp snooping report-forward
```

### Syntax Description

**all-ports** - IGMP reports forwarded on all the ports of a VLAN

**router-ports** - IGMP reports forwarded on router ports of a VLAN

### Mode

Global Configuration Mode

### Defaults

router-ports

### Example:

```
SMIS(config)# ip igmp snooping report-forward all-ports
```

### Related Command

**show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN

## 14.10 ip igmp snooping version

This command sets the operating version of the IGMP snooping switch for a specific VLAN.

```
ip igmp snooping version { v1 |v2 | v3}
```

### Syntax Description

v1 - IGMP snooping Version 1

v2 - IGMP snooping Version 2

v3 - IGMP snooping Version 3

### Mode

Config-VLAN Mode

### Defaults

v3

### Example:

```
SMIS(config-vlan)#ip igmp snooping version v2
```

### Related Command

**show ip igmp snooping** - Displays IGMP snooping information for all VLANs or a specific VLAN

## 14.11 ip igmp snooping fast-leave

This command enables fast leave processing for a specific VLAN and the no form of the command disables fast leave processing for a specific VLAN.

```
ip igmp snooping fast-leave
```

```
no ip igmp snooping fast-leave
```

### Mode

Config-VLAN Mode

### Defaults

Disabled

### Example:

```
iss (config-vlan)# ip igmp snooping fast-leave
```

### Related Command

**show ip igmp snooping** - Displays IGMP snooping information for all VLANs or a specific VLAN

## 14.12 ip igmp snooping querier

This command configures the IGMP snooping switch as a querier for a specific VLAN. The `no` form of the command configures the IGMP snooping switch as non-querier for a specific VLAN.

```
ip igmp snooping querier
```

```
no ip igmp snooping querier
```

### Mode

Config-VLAN Mode

### Defaults

Non-querier

### Example:

```
iss (config-vlan)# ip igmp snooping querier
```

### Related Command

`show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN



## 14.13 ip igmp snooping query-interval

This command sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN. The no form of the command sets the IGMP querier interval to default value.

```
ip igmp snooping query-interval <(60 - 600) seconds>
```

```
no ip igmp snooping query-interval
```

### Mode

Config-VLAN Mode

### Defaults

125

### Example:

```
iss (config-vlan) # ip igmp snooping query-interval 200
```

### Related Command

**show ip igmp snooping** - Displays IGMP snooping information for all VLANs or a specific VLAN

## 14.14 ip igmp snooping mrouter

This command configures statically the router ports for a VLAN and the no form of the command deletes the statically configured router ports for a VLAN.

```
ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>
```

```
no ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>
```

### Mode

Config-VLAN Mode

### Example:

```
iss (config-vlan)# ip igmp snooping mrouter gigabitethernet 0/1-3
```

### Related Command

**show ip igmp snooping mrouter** - Displays the router ports for all VLANs or specific VLAN

## 14.15 ip igmp snooping send-query

This command configures IGMP snooping send-query function. When send-query is enabled, switch sends IGMP query messages on all the ports when spanning tree topology changes.

```
ip igmp snooping send-query { enable | disable }
```

### Mode

Global Configuration Mode

### Default

Disable

### Example:

```
iss (config)# ip igmp snooping send-query enable
```

### Related Command

**show ip igmp snooping globals** - Displays IGMP snooping global configuration parameters

## 14.16 ip igmp snooping clear counters

This command clears the IGMP snooping statistics. If any VLAN identifier is provided it clears the IGMP snooping statistics for the given VLAN.

```
ip igmp snooping clear counters [Vlan <vlan-id>]
```

### Syntax

<vlan-id> - Any valid VLAN identifier between 1 to 4069

### Mode

Global Configuration Mode

### Example:

```
iss (config)# ip igmp snooping clear counters
```

### Related Command

**show ip igmp snooping statistics** - Displays IGMP snooping statistics

## 14.17 shutdown snooping

This command shuts down snooping in the switch and the no form of the command starts and enables snooping in the switch.

**shutdown snooping**

**no shutdown snooping**

### Mode

Global Configuration Mode

### Defaults

no shutdown snooping

### Example:

```
SMIS(config)# shutdown snooping
```

When shutdown, all resources acquired by the Snooping Module are released to the system.

For the IGS feature to be functional on the switch, the 'system-control' status must be set as 'start' and the 'state' must be 'enabled'

### Related Command

**ip igmp snooping** - Enables IGMP snooping in the switch/a specific VLAN

## 14.18 debug ip igmp snooping

This command specifies the debug levels for IGMP snooping module and the no form of the command resets debug options for IGMP snooping module.

```
debug ip igmp snooping {[init][resources][tmr][src][grp][qry]
[vlan][pkt][fwd][mgmt][redundancy] | all }
```

```
no debug ip igmp snooping {[init][resources][tmr][src][grp][qry]
[vlan][pkt][fwd][mgmt][redundancy] | all }
```

### Syntax Description

**init** - Init and Shutdown Messages

**resources** - System Resources management Messages

**tmr** - Timer Messages

**src** - Source Information Messages

**grp** - Group Information Messages

**qry** - Query Related Messages

**vlan** - VLAN Information Messages

**pkt** - Packet Dump Messages

**fwd** - Forwarding Database Messages

**mgmt** - Management Related Messages

**redundancy** - Redundancy Related messages

**all** - All Messages

### Mode

Privileged EXEC Mode

### Defaults

Debugging is Disabled.

### Example:

```
SMIS# debug ip igmp snooping fwd
```

### Related Command

**show debugging-** Displays state of each debugging option

## 14.19 show ip igmp snooping mrouter

This command displays the router ports for all VLANs or a specific VLAN.

```
show ip igmp snooping mrouter [Vlan <vlan index>]
```

### Syntax Description

**vlan** - Vlan ID value

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance

```
SMIS# show ip igmp snooping mrouter
```

```
Vlan Ports
```

```
-----
```

```
1 Gi0/1(dynamic), Gi0/2(static)
```

```
2 Gi0/1(static), Gi0/2(dynamic)
```

#### Multiple Instance

```
SMIS# show ip igmp snooping mrouter
```

```
Switch cust1
```

```
Vlan Ports
```

```
-----
```

```
1 Gi0/1(static)
```

```
2 Gi0/1(static)
```

```
Switch cust2
```

```
Vlan Ports
```

```
-----
```

```
1 Gi0/9(static)
```

```
2 Gi0/9(static)
```

### Related Command

**ip igmp snooping mrouter** - Configures statically the router ports for a VLAN

## 14.20 show ip igmp snooping globals

This command displays the IGMP snooping information for all VLANs or a specific VLAN.

```
show ip igmp snooping globals
```

### Syntax

#### Mode

Privileged EXEC Mode

#### Example:

##### Single Instance

```
SMIS# show ip igmp snooping globals
IGMP Snooping Configuration
-----
IGMP Snooping globally enabled
Proxy reporting globally enabled
Multicast forwarding mode
is MAC based

Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Report forward interval is 5 seconds
Group specific query interval is 2 seconds
IGMP reports are forwarded to router ports
Group specific query retry count is 2
```

##### Multiple Instance

```
SMIS# show ip igmp snooping globals
Switch default
Snooping Configuration
-----
IGMP Snooping globally disabled
IGMP Snooping is operationally disabled
Multicast forwarding mode
is MAC based
Proxy reporting globally enabled
```



```
Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Report forward interval is 5 seconds
Group specific query interval is 2 seconds
Reports are forwarded on router ports
Group specific query retry count is 2
Switch cust1
```

Snooping Configuration

```
-----
IGMP Snooping globally enabled
IGMP Snooping is operationally enabled
Multicast forwarding mode
is MAC based
```

```
IGMP Snooping is operationally enabled
Multicast forwarding mode
is MAC based
```

```
Proxy reporting globally enabled
Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Report forward interval is 5 seconds
Group specific query interval is 2 seconds
Reports are forwarded on router ports
Group specific query retry count is 2
Switch cust2
```

Snooping Configuration

```
-----
IGMP Snooping globally enabled
IGMP Snooping is operationally enabled
Multicast forwarding mode
is MAC based
```

```
Proxy reporting globally enabled
Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Report forward interval is 5 seconds
```

Group specific query interval is 2 seconds

Reports are forwarded on router ports

Group specific query retry count is 2

### Related Commands

**ip igmp snooping** - Enables IGMP snooping in the switch/a specific VLAN

**ip igmp snooping proxy-reporting** - Enables proxy reporting in the IGMP snooping switch

**snooping multicast-forwarding-mode** - Specifies the forwarding mode (IP based or MAC based) that will be effective on switch restart

**ip igmp snooping port-purge-interval** - Sets the IGMP snooping port purge time interval after which the port gets deleted if no IGMP reports are received

**ip igmp snooping report-suppression interval** - Sets the IGMP report-suppression interval

**ip igmp snooping retry-count** - Sets the maximum number of group specific queries sent on a port on reception of a IGMPV2 leave message

**ip igmp snooping version** - Specifies the IGMP snooping operating mode of the switch

**ip igmp snooping report-forward** - Specifies if IGMP reports must be forwarded on all ports or router ports of a VLAN

## 14.21 show ip igmp snooping

This command displays IGMP snooping information for all VLANs or a specific VLAN.

```
show ip igmp snooping [Vlan <vlan id>]
```

### Syntax Description

**vlan** - VLAN ID

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance

```
SMIS# show ip igmp snooping vlan 2
IGMP Snooping VLAN Configuration for VLAN 2
IGMP Snooping enabled
IGMP Operating version is V3
Fast leave is disabled
IGMP snooping switch is Non-Querier
Query interval is 125 seconds
```

#### Multiple Instance

```
SMIS# show ip igmp snooping
Switch cust1
Snooping VLAN Configuration for the VLAN 1
IGMP Snooping enabled
IGMP configured version is V2
IGMP Operating version is V2
Fast leave is disabled
Snooping switch is acting as Non-Querier
Query interval is 125 seconds
Snooping VLAN Configuration for the VLAN 2
IGMP Snooping enabled
IGMP configured version is V2
IGMP Operating version is V2
Fast leave is disabled
Snooping switch is acting as Non-Querier
Query interval is 125 seconds
```

```
Switch cust2
Snooping VLAN Configuration for the VLAN 1
IGMP Snooping enabled
IGMP configured version is V2
IGMP Operating version is V2
Fast leave is disabled
Snooping switch is acting as Non-Querier
Query interval is 125 seconds
Snooping VLAN Configuration for the VLAN 2
IGMP Snooping enabled
IGMP configured version is V2
IGMP Operating version is V2
Fast leave is disabled
Snooping switch is acting as Non-Querier
Query interval is 125 seconds
```

### Related Commands

**ip igmp snooping** - Enables IGMP snooping in the switch/a specific VLAN

**ip igmp snooping version** - Specifies the IGMP snooping operating mode of switch

**ip igmp snooping fast-leave** - Enables fast leave processing for a specific VLAN

**ip igmp snooping querier** - Configures the IGMP snooping switch as a querier for a specific VLAN

**ip igmp snooping query-interval** - Sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN

## 14.22 show ip igmp snooping groups

This command displays IGMP group information for all VLANs or a specific VLAN or a specific VLAN and group address.

```
show ip igmp snooping groups [Vlan <vlan id> [Group <Address>]]
```

### Syntax Description

**vlan** - VLAN index value

**Group** - Group Address of the VLAN ID

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance

```
/* IP based */
SMIS# show ip igmp snooping groups
IGMP Snooping Group information
-----
VLAN ID:2 Group Address: 227.1.1.1
```

#### Filter Mode

```
EXCLUDE
```

```
Exclude sources: None
```

```
V1/V2 Receiver Ports:
```

```
Gi0/4
```

```
V3 Receiver Ports:
```

```
Port Number: Gi0/2
```

```
Include sources: None
```

```
Exclude sources:
```

```
12.0.0.10, 12.0.0.20
```

```
Port Number: Gi0/3
```

```
Include sources: None
```

```
Exclude sources:
```

```
12.0.0.40, 12.0.0.30
```

```
/* MAC based */
SMIS# show ip igmp snooping groups
IGMP Snooping Group information
-----
VLAN ID:2 Group Address: 227.1.1.1
```

```
Filter Mode
  EXCLUDE
```

```
Exclude sources: None
Receiver Ports:
Gi0/2, Gi0/3, Gi0/4, Gi0/5
```

## Multiple Instance

```
SMIS# show ip igmp snooping groups
Switch cust1
Snooping Group information
-----
VLAN ID:2 Group Address: 227.2.2.2
```

```
Filter Mode
  EXCLUDE
```

```
Exclude sources: None
Receiver Ports:
Gi0/3, Gi0/5, Gi0/6
Switch cust2
Snooping Group information
-----
VLAN ID:2 Group Address: 227.2.2.2
```

```
Filter Mode
  EXCLUDE
```

```
Exclude sources: None
Receiver Ports:
```

Gi0/10

**Related Command**

**ip igmp snooping** - Enables IGMP snooping in the switch/a specific VLAN

## 14.23 show ip igmp snooping forwarding-database

This command displays the multicast forwarding entries for all VLANs or a specific VLAN.

**show ip igmp snooping forwarding-database [Vlan <vlan id>]**

### Syntax Description

**Vlan** - VLAN ID

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance

```
/* IP based */
SMIS# show ip igmp snooping forwarding-database
Vlan Source Address Group Address Ports
-----
2 12.0.0.10 227.1.1.1 Gi0/1, Gi0/3, Gi0/4
2 12.0.0.20 227.1.1.1 Gi0/1, Gi0/3, Gi0/4
2 12.0.0.30 227.1.1.1 Gi0/1, Gi0/2, Gi0/4
2 12.0.0.40 227.1.1.1 Gi0/1, Gi0/2, Gi0/
```

```
/* MAC based */
SMIS# show ip igmp snooping forwarding-database
Vlan MAC-Address Ports
-----
2 01:00:5e:01:01:01 Gi0/2, Gi0/3, Gi0/4, Gi0/5
2 01:00:5e:02:02:02 Gi0/2, Gi0/3
```

#### Multiple Instance

```
SMIS# show ip igmp snooping forwarding-database
Switch cust1
Vlan MAC-Address Ports
-----
2 01:00:5e:02:02:02 Gi0/2, Gi0/3, Gi0/5, Gi0/6
```



```
Switch cust2
```

```
Vlan MAC-Address Ports
```

```
-----
```

```
2 01:00:5e:02:02:02 Gi0/9, Gi0/10
```

IGS must be enabled in the switch prior to the execution of this command.

## **Related Command**

**ip igmp snooping** - Enables IGMP snooping in the switch/a specific VLAN

## 14.24 show ip igmp snooping statistics

This command displays IGMP snooping statistics for all VLANs or a specific VLAN.

```
show ip igmp snooping statistics [Vlan <vlan id>]
```

### Syntax Description

**Vlan** - VLAN index

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance

```
SMIS# show ip igmp snooping statistics
IGMP Snooping Statistics for VLAN 1
IGMP Snooping General queries received : 3
IGMP Snooping Group specific queries received : 0
IGMP Snooping Group and source specific queries received : 0
IGMP Snooping V1/V2 reports received : 10
IGMP Snooping V3 reports received : 0
IGMP Snooping V3 IS_INCLUDE messages received : 0
IGMP Snooping V3 IS_EXCLUDE messages received : 0
IGMP Snooping V3 TO_INCLUDE messages received : 0
IGMP Snooping V3 TO_EXCLUDE messages received : 0
IGMP Snooping V3 ALLOW messages received : 0
IGMP Snooping V3 Block messages received : 0
IGMP Snooping V2 Leave messages received : 0
IGMP Snooping General queries transmitted : 0
IGMP Snooping Group specific queries transmitted : 2
IGMP Snooping V1/V2 reports transmitted : 0
IGMP Snooping V3 reports transmitted : 3
IGMP Snooping V2 leaves transmitted : 0
IGMP Snooping Packets dropped : 1
```

#### Multiple Instance

```
SMIS# show ip igmp snooping statistics
Switch cust1
```

Snooping Statistics for VLAN 1

General queries received : 0  
Group specific queries received : 0  
Group and source specific queries received : 0  
ASM reports received : 20  
SSM reports received : 0  
IS\_INCLUDE messages received : 0  
IS\_EXCLUDE messages received : 0  
TO\_INCLUDE messages received : 0  
TO\_EXCLUDE messages received : 0  
ALLOW messages received : 0  
Block messages received : 0  
Leave messages received : 0  
General queries transmitted : 0  
Group specific queries transmitted : 0  
ASM reports transmitted : 1  
SSM reports transmitted : 0  
Leaves transmitted : 0  
Packets dropped : 0

Snooping Statistics for VLAN 2

General queries received : 0  
Group specific queries received : 0  
Group and source specific queries received : 0  
ASM reports received : 19  
SSM reports received : 18  
IS\_INCLUDE messages received : 0  
IS\_EXCLUDE messages received : 0  
TO\_INCLUDE messages received : 0  
TO\_EXCLUDE messages received : 0  
ALLOW messages received : 0  
Block messages received : 0  
Leave messages received : 0  
General queries transmitted : 0  
Group specific queries transmitted : 0  
ASM reports transmitted : 2  
SSM reports transmitted : 0  
Leaves transmitted : 0

```
Packets dropped : 0
Switch cust2
Snooping Statistics for VLAN 1
General queries received : 0
Group specific queries received : 0
Group and source specific queries received : 0
ASM reports received : 0
SSM reports received : 0
IS_INCLUDE messages received : 0
IS_EXCLUDE messages received : 0
TO_INCLUDE messages received : 0
TO_EXCLUDE messages received : 0
ALLOW messages received : 0
Block messages received : 0
Leave messages received : 0
General queries transmitted : 0
Group specific queries transmitted : 0
ASM reports transmitted : 0
SSM reports transmitted : 0
Leaves transmitted : 0
Packets dropped : 0
Snooping Statistics for VLAN 2
General queries received : 0
Group specific queries received : 0
Group and source specific queries received : 0
ASM reports received : 0
SSM reports received : 0
IS_INCLUDE messages received : 0
IS_EXCLUDE messages received : 0
TO_INCLUDE messages received : 0
TO_EXCLUDE messages received : 0
ALLOW messages received : 0
Block messages received : 0
Leave messages received : 0
General queries transmitted : 0
Group specific queries transmitted : 0
ASM reports transmitted : 0
```

SSM reports transmitted : 0

Leaves transmitted : 0

Packets dropped : 0

### **Related Command**

**ip igmp snooping** - Enables IGMP snooping in the switch/a specific VLAN

## 15 VLAN

VLANs (Virtual LANs) can be viewed as a group of devices on different physical LAN segments which can communicate with each other as if they were all on the same physical LAN segment, i.e. a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible.

VLAN provides the following benefits for switched LANs: Improved administration efficiency  
Optimized Broadcast/Multicast Activity Enhanced network security

The list of commands to configure VLAN are:

[vlan](#)

[protocol-vlan](#)

[map protocol](#)

[set gvrp](#)

[set port gvrp](#)

[set gmrp](#)

[set port gmrp](#)

[mac-vlan](#)

[mac-address-table static unicast](#)

[mac-address-table static multicast](#)

[mac-address-table aging-time](#)

[wildcard mac-address](#)

[ports](#)

[name](#)

[vlan active](#)

[switchport pvid](#)

[switchport access vlan](#)

[switchport trunk native vlan](#)

[switchport trunk allowed vlan](#)

[switchport acceptable-frame-type](#)

[switchport ingress-filter](#)

[port protocol-vlan](#)

[switchport map protocols-group](#)

[switchport priority default](#)

[switchport mode](#)

[switchport protected](#)

[set garp timer](#)

[vlan restricted](#)

[group restricted](#)

[vlan map-priority](#)

[shutdown garp](#)

[debug vlan](#)

[debug garp](#)

[show vlan](#)

[show vlan device info](#)

[show vlan device capabilities](#)

[show vlan traffic-classes](#)

[show garp timer](#)

[show vlan port config](#)

[show vlan protocols-group](#)

[show switchport protected](#)

[show protocol-vlan](#)

[show mac-vlan](#)

[show mac-address-table](#)

[show mac-address-table count](#)

[show mac-address-table static unicast](#)

[show mac-address-table static multicast](#)

[show mac-address-table dynamic unicast](#)

[show mac-address-table dynamic multicast](#)

[show mac-address-table aging-time](#)

[show wildcard](#)

## 15.1 vlan

This command configures a VLAN in the switch and is also used to enter into the config-VLAN mode. The no form of the command deletes a VLAN from the switch.

```
vlan <vlan-list>
```

```
no vlan <vlan-list>
```

### Syntax

**vlan-list** – may be any VLAN number between 1 to 4069 or list of VLAN numbers. Multiple VLAN numbers can be provided as comma separated values. Consecutive VLAN numbers can be provided as ranges such as 5-10.

### Mode

Global Configuration Mode

### Defaults

vlan-id - 1

### Example:

```
SMIS(config)# vlan 4
```

### Related Command

**show vlan** - Displays VLAN information in the database



## 15.2 protocol-vlan

This command enables Protocol-VLAN based classification on all the ports. The no form of the command disables Protocol-VLAN based classification on all ports.

**protocol-vlan**

**no protocol-vlan**

### Mode

Global Configuration Mode

### Defaults

Enabled

### Example:

```
SMIS(config)# protocol-vlan
```

### Related Commands

**show vlan device info** - Displays the VLAN related global status variables

**show protocol-vlan** - Displays the entries in the protocol-VLAN database

## 15.3 map protocol

This command configures the group ID for a specific encapsulation and protocol value combination. This command adds a protocol to a protocol group for protocol based VLAN learning. The no form of the command removes the protocol from the entire group.

```
map protocol {ip | novell | netbios | appletalk | other <aa:aa or
aa:aa:aa:aa:aa>} {enet-v2 | snap | llcOther | snap8021H | snapOther}
protocols-group <Group id>
```

```
no map protocol {ip | novell | netbios | appletalk | other <aa:aa or
aa:aa:aa:aa:aa>} {enet-v2 | snap | llcOther | snap8021H | snapOther}
```

### Syntax Description

**ip | novell | netbios | appletalk |** - Protocol types

**other** - MAC address of any other protocol type not included in the list

**enet-v2 | snap | llcOther | snap8021H | snapOther** - Encapsulation Frame Types

**protocols-group** - Group ID

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# map protocol ip enet-v2 protocols-group 1
```

### Related Command

**show vlan protocols-group** - Displays the protocol group database

## 15.4 set gvrp

This command enables or disables GVRP on a global basis.

```
set gvrp { enable | disable }
```

### Syntax Description

**enable** - Enables GVRP in the switch

**disable** - Disables GVRP in the switch

### Mode

Global Configuration Mode

### Defaults

**disable**

### Example:

```
SMIS(config)# set gvrp disable
```

GVRP needs to be explicitly enabled even after GARP is enabled.

### Related Commands

**show vlan** - Displays VLAN information in the database

**show vlan device info** - Displays the VLAN related global status variables

## 15.5 set port gvrp

This command enables or disables GVRP on the interface.

```
set port gvrp <interface-type> <interface-id> { enable | disable }
```

### Syntax Description

**interface-type** - Interface type

**interface-id** - Interface Id

**enable** - Enables GVRP on the interface

**disable** - Disables GVRP on the interface

### Mode

Global Configuration Mode

### Defaults

**disable**

### Example:

```
SMIS(config)# set port gvrp gigabitethernet 0/1 disable
```

- ▶ The value **enable** indicates that GVRP is enabled on the current port, as long as global GVRP status is also enabled for the device.

If port GVRP state is disabled, but global GVRP status is still enabled, then GVRP is disabled on current port. Any GVRP packet received will be discarded and no GVRP registrations will be propagated from other ports

### Related Command

**show vlan port config** - Displays the vlan related parameters specific for ports

## 15.6 set gmrp

This command enables or disables GMRP globally on the device.

```
set gmrp { enable | disable }
```

### Syntax Description

**enable** - Enables GMRP on the device

**disable** - Disables GMRP on the device

### Mode

Global Configuration Mode

### Defaults

**disable**

### Example:

```
SMIS(config)# set gmrp disable
```

GMRP needs to be explicitly enabled even after GARP is enabled.

### Related Commands

**show vlan** - Displays VLAN information in the database

**show vlan device info** - Displays the VLAN related global status variables

## 15.7 set port gmrp

This command enables or disables GMRP on the port.

```
set port gmrp <interface-type> <interface-id> { enable | disable }
```

### Syntax Description

**interface-type** - Interface type

**interface-id** - Interface ID

**enable** - Enables GMRP on the interface

**disable** - Disables GMRP on the interface

### Mode

Global Configuration Mode

### Defaults

**disable**

### Example:

```
SMIS(config)# set port gmrp gigabitethernet 0/1 disable
```

- The value **enable** indicates that GMRP is enabled on this port in all VLANs as long as GMRP Status is also enabled globally.
- The value **disable** indicates that GMRP is disabled on this port in all VLANs; any GMRP packet received will be silently discarded and no GMRP registrations will be propagated from other ports

### Related Command

**show vlan port config** - Displays the vlan related parameters specific for ports

## 15.8 mac-vlan

This command configures the VLAN-MAC address mapping. The no form of this command is used to delete the specific vlan mac mapping entry. User also need to configure port membership for the mapped VLAN to allow MAC-Based Vlan to work properly.

```
mac-vlan <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)>
```

```
no mac-vlan <aa:aa:aa:aa:aa:aa>
```

### Syntax Description

**aa:aa:aa:aa:aa:aa** - MAC address

**vlan** - VLAN Identifier

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# mac-vlan 00:11:22:33:44:55 vlan 2
```

### Related Commands

**show mac-vlan** - Displays the entries in the MAC-VLAN database

[vlan](#) – Create or access a vlan.

[ports](#) – Configure a port membership for a VLAN.

## 15.9 mac-address-table static unicast

This command configures a static unicast MAC address in the forwarding database. The no form of the command deletes a configured static Unicast MAC address from the forwarding database.

```
mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> [recv-port <interface-type> <interface-id>] interface  
([<interface-type> <0/ab, 0/c, ...>] [<interface-type> <0/a-b, 0/c,  
...>] [port-channel <a,b,c-d>]) [status { permanent | deleteOnReset |  
deleteOnTimeout }]
```

```
no mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-  
id(1-4069)> [recv-port <interface-type> <interface-id>]
```

### Syntax Description

**aa:aa:aa:aa:aa:aa** - Destination MAC address

**vlan** - VLAN Identifier

**recv-port** - Received port's Interface type and ID

**interface** - Member Ports Interface type and ID. Interface can be of fastethernet type [or gigabitethernet type]

**<interface-type> <0/a-b, 0/c, ...>** - Member Ports Interface type and ID. Interface can be of gigabitethernet type [or fastethernet type]

**port-channel** - Port-channel ID

**status** - Status of the Static unicast entry

### Mode

Global Configuration Mode

### Defaults

status

- permanent

### Example:

```
SMIS(config)# mac-address-table static unicast 00:11:22:33:44:55  
vlan 3 recv-port gigabitethernet 0/2 interface gigabitethernet  
0/1 status deleteOnTimeout
```



- ▶ VLAN must have been configured and member ports must have been configured for
- ▶ the specified VLAN.

### Related Commands

**show mac-address-table static unicast** - Displays the statically configured unicast address from the MAC address table

---

## 15.10 mac-address-table static multicast

This command configures a static multicast MAC address in the forwarding database.

```
mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> [recv-port <interface-type> <interface-id>] interface  
([<interface-type> <0/ab, 0/c, ...>] [<interface-type> <0/a-b, 0/c,  
...>] [port-channel <a,b,c-d>]]) [forbidden-ports ([<interface-type>  
<0/a-b, 0/c, ...>] [<interface-type> <0/ab, 0/c, ...>] [port-channel  
<a,b,c-d>]]) [status { permanent | deleteOnReset | deleteOnTimeout }]
```

```
no mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan <vlan-  
id(1- 4069)> [recv-port <interface-type> <interface-id>]
```

### Syntax Description

**aa:aa:aa:aa:aa:aa** - Multicast MAC address

**vlan** - VLAN Identifier

**recv-port** - Received port's Interface type and ID

**interface** - Member Ports Interface type and ID. Interface can be of fastethernet type [or gigabitethernet type]

**<interface-type> <0/a-b, 0/c, ...>** - Member Ports Interface type and ID. Interface can be of gigabitethernet type [or fastethernet type]

**port-channel** - Port channel ID

**forbidden-ports** - Forbidden ports interface type and ID. Interface can be of fastethernet type [or gigabitethernet type]

**<interface-type> <0/a-b, 0/c, ...>** - Forbidden ports interface type and ID. Interface can be of gigabitethernet type [or fastethernet type]

**port-channel** - Port-channel ID

**status** - Status of the static multicast entry

### Mode

Global Configuration Mode

### Defaults

Status - permanent

**Example:**

```
SMIS(config)# mac-address-table static multicast  
01:02:03:04:05:06 vlan 2 interface gigabitethernet 0/1
```

- ➔ VLAN must have been configured and member ports must have been configured for the specified VLAN.

**Related Command**

**show mac-address-table static multicast** - Displays the statically configured multicast entries

## 15.11 mac-address-table aging-time

This command sets the maximum age of a dynamically learnt entry in the MAC address table. The no form of the command sets the maximum age of an entry in the MAC address table to its default value.

```
mac-address-table aging-time <10-1000000 seconds>
```

```
no mac-address-table aging-time
```

### Mode

Global Configuration Mode

### Defaults

300

### Example:

```
SMIS(config)# mac-address-table aging-time 200
```

- ➔ If traffic on an interface is not very frequent, then the aging time must be increased to record the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding.

### Related Command

**show mac-address-table aging-time** - Displays the MAC address-table with ageing time

## 15.12 wildcard mac-address

This command adds wildcard or broadcast MAC address to layer 2 MAC table with the given interfaces.

The no form of this command removes the wildcard MAC addresses from layer 2 MAC table.

```
wildcard {mac-address <mac_addr> | broadcast} interface  
([<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c,  
...>] [port-channel <a,b,c-d>])
```

```
no wildcard {mac-address <mac_addr> | broadcast}
```

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# wildcard mac-address 03:04:06 int gi 0/1
```

### Related Command

**show wildcard** - Displays the wildcard entries from layer 2 MAC table.

## 15.13 ports

This command configures a static VLAN entry with the required member ports, untagged ports and forbidden ports.

```
ports <ports-list> {tagged | untagged | forbidden}
```

```
no ports [<ports-list>] {tagged | untagged | forbidden}
```

### Syntax Description

**<ports-list>** - List of member ports – up to three ranges or ports separated by spaces. The range of ports is provided in a format like gi 0/1-10, which refer to ports from gi 0/1 to gi 0/10. The ports can be gigabit ethernet, extreme-ethernet, qx-ethernet or port channel interfaces.

Note: All of ports in <ports-list> must be in hybrid mode. If any port in list is not a hybrid mode port, use switchport mode command to set the port to hybrid mode.

**tagged** – The given ports will be configured as tagged ports to the vlan.

**untagged** – The given ports will be configured as untagged ports to the vlan.

**forbidden** – The given ports will be configured as forbidden ports to the vlan.

### Mode

Config-VLAN Mode

### Example:

```
SMIS(config-vlan)# ports gigabitethernet 0/1 untagged
```

### Related Command

**show vlan** - Displays VLAN information in the database

## 15.14 name

This command configures name to static VLANs. The no form of this command removes the configured name from static VLANs.

**name** <string(32)>

**no name**

### Syntax Description

<string> - Alphanumerical string up to 32 characters long

### Mode

Config-VLAN Mode

### Example:

```
SMIS(config-vlan)# name devstack_vlan
```

### Related Command

**show vlan** - Displays VLAN information in the database

## 15.15 switchport pvid

This command configures the PVID (VLAN Identifier) that would be assigned to untagged/priority-tagged frames. The no form of this command sets the PVID to the default value. Usually the default PVID is 1. Note: This command only work when the port is in hybrid mode. If it is not a hybrid port, the command only set the configuration value without changing hardware setup. The no form of this command resets the PVID to default PVID.

```
switchport pvid <vlan-id(1-4069)>
```

```
no switchport pvid
```

### Mode

Interface Configuration Mode

### Defaults

vlan-id - 1

### Example:

```
SMIS(config-if)# switchport pvid 3
```

### Related Command

**show vlan port config** - Displays the VLAN related parameters specific for ports



## 15.16 switchport access vlan

This command configures the access vlan for the port. The no form of this command resets the access vlan to the default management vlan 1.

```
switchport access vlan <vlan-id(1-4069)>
```

```
no switchport access vlan
```

### Mode

Interface Configuration Mode

### Defaults

vlan-id - 1

### Example:

```
SMIS(config-if)# switchport access vlan 3
```

### Related Command

**show vlan port config** - Displays the VLAN related parameters specific for ports

## 15.17 Switchport trunk native vlan

This command configures the trunk native vlan for the port. The no form of this command resets the trunk native vlan to the default vlan 1.

```
switchport trunk native vlan <vlan-id(1-4069)>
```

```
no switchport trunk native vlan
```

### Mode

Interface Configuration Mode

### Defaults

Vlan 1

### Example:

```
SMIS(config-if)# switchport trunk native vlan 3
```

### Related Command

```
show vlan port config - Displays the VLAN related parameters specific for ports
```

## 15.18 switchport trunk allowed vlan

This command configures the allowed vlans for trunk ports. By default, all the VLANs configured on a switch are allowed on the trunk interfaces. User can limit the allowed vlans on the trunk ports using this command.

```
switchport trunk allowed vlan { <vlan-list> | add <vlan-list> | all | none | except <vlan-list> | remove <vlan-list> }
```

### Syntax

**<vlan-list>** - This can be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10.

**add** – Adds the given vlans to the allowed vlans list

**all** – Configures all the vlans on the switches as the allowed vlans on this port

**none** – Removes the all the allowed vlans configured on this port

**except** – Configures all the vlans of the switch except the given vlans as the allowed vlan on this port

**remove** – Removes the given vlans from the allowed vlans list configured on this port

### Mode

Interface Configuration Mode

### Defaults

All vlans

### Example:

```
SMIS(config-if)# switchport trunk allowed vlan 3-10
```

### Related Command

**show vlan port config** - Displays the VLAN related parameters specific for ports

## 15.19 switchport acceptable-frame-type

This command configures the acceptable frame type for the port. The no form of this command sets the default value of acceptable frame type - "all" where all frames will be accepted.

```
switchport acceptable-frame-type {all | tagged |
untaggedAndPrioritytagged }
```

```
no switchport acceptable-frame-type
```

### Syntax Description

**all** - All frames

**tagged** - Tagged frames

**untaggedAndPrioritytagged** - Untagged and priority tagged frames

### Mode

Interface Configuration Mode

### Defaults

all

### Example:

```
SMIS(config-if)# switchport acceptable-frame-type tagged
```

- ➔ When set to "tagged" the device will discard untagged and priority tagged frames received on the port and will process only the VLAN tagged frames. When set to "all" untagged frames or priority-tagged frames received on the port are also accepted. When set to "untaggedAndPrioritytagged", untagged and priority tagged frames alone are accepted and tagged frames are dropped.

### Related Command

**show vlan port config** - Displays the VLAN related parameters specific for ports

## 15.20 switchport ingress-filter

This command enables ingress filtering on the port. The no form of this command disables ingress filtering on the port.

```
switchport ingress-filter
```

```
no switchport ingress-filter
```

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# switchport ingress-filter
```

- ➔ When ingress-filtering is enabled, the device discards those incoming frames for VLANs which do not include this port in its member set.  
When the ingress filtering is disabled using the no form of the command, the device accepts all incoming frames.

### Related Command

**show vlan port config** - Displays the VLAN related parameters specific for ports

## 15.21 port protocol-vlan

This command enables port protocol based VLANs. The no form of the command disables port Protocol based VLANs.

```
port protocol-vlan
```

```
no port protocol-vlan
```

### Mode

Interface Configuration Mode

### Defaults

Enabled

### Example:

```
SMIS(config-if)# port protocol-vlan
```

- ➔ The value enable indicates that the VLAN classification on this port is port and protocol based as long as the port and protocol based classification is enabled globally for the device.

### Related Command

**show vlan port config** - Displays the VLAN related parameters specific for ports

## 15.22 switchport map protocols-group

This command maps the protocol group configured to a particular VLAN identifier for the specified interface. The no form of the command un-maps the VLAN identifier to group Id mapping.

```
switchport map protocols-group <Group id> vlan <vlan-id(1-4069)>
```

```
no switchport map protocols-group <Group id>
```

### Syntax Description

**Group id** - Group ID

**Vlan** - VLAN ID

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# switchport map protocols-group 1 vlan 2
```

Protocol group must have been configured.

### Related Commands

**map protocol** - Adds a protocol to a protocol group for protocol based VLAN learning

**show protocol-vlan** - Displays the entries in protocol-VLAN database

**show vlan protocols-group** - Displays the protocol group database

## 15.23 switchport priority default

This command sets the default user priority for the port. The no form of the command sets the default user priority for the port to the default value.

```
switchport priority default <priority value (0-7)>
```

```
no switchport priority default
```

### Mode

Interface Configuration Mode

### Defaults

0

### Example:

```
SMIS(config-if)# switchport priority default 5
```

### Related Command

**show vlan port config** - Displays the VLAN related parameters specific for ports



## 15.24 switchport mode

This command configures the VLAN port mode. The no form of the command configures the default VLAN port mode

```
switchport mode { access | trunk | hybrid }
```

```
no switchport mode
```

### Syntax Description

**access** - Access port Mode

**trunk** - Trunk port Mode

**hybrid** - Hybrid VLAN port Mode

**Mode** - Interface Configuration Mode

### Defaults

Hybrid Mode

### Example:

```
SMIS(config-if)# switchport mode access
```

- ➡ ~~It is not possible to configure the switchport mode status to trunk if the port is an untagged member of a VLAN.~~

### Related Commands

```
switchport mode
```

**dot1q-tunnel** - Enables dot1q-tunneling on the specified interface

**show vlan port config** - Displays the VLAN related parameters specific for ports

## 15.25 switchport protected

This command configures the given port as the protected port. If the group option is provided, it configures the given port as a community port. The “no” form of this command configures the given port as an unprotected port.

The unprotected port can communicate with all the unprotected ports, protected ports and community ports. The protected port can communicate only with unprotected ports. The protected port is also called an isolated port. The community port can communicate with other ports in same community as well as with unprotected ports.

```
switchport protected [ group <integer(1-10000000)>]
```

```
no switchport protected
```

### Syntax Description

**group** – Community group number

### Defaults

Unprotected

### Example:

```
SMIS(config-if)# switchport protected group 10
```

### Related Commands

[show switchport protected](#) - Displays the protected ports configuration

### Note:

This command is supported only for the physical interfaces. It is not supported for port channel and layer 3 VLAN interfaces.

## 15.26 set garp timer

This command configures the GARP join time, leave time, and leave all time in milli-seconds.

```
set garp timer {join | leave | leaveall} <time in milli seconds>
```

### Syntax Description

**join** - Join Time

**leave** - Leave Time

**leaveall** - Leaveall Time

### Mode

Interface Configuration Mode

### Defaults

Join - 20

leave - 60

leaveall - 1000

### Example:

```
SMIS(config-if)# set garp timer join 500
```

- ▶ Leave Timer must be greater than 2 times Join Timer and Leaveall Timer must be greater than Leave Timer.  
Timer values cannot be set to zero.  
The GARP timer configuration will be applied to the GARP applications (GMRP and GVRP) on the specified interface.

### Related Command

**show garp timer** - Displays the GARP timer information of the available interfaces

## 15.27 vlan restricted

This command enables/disables restricted VLAN registration on the port.

```
vlan restricted {enable | disable}
```

### Syntax Description

**enable** - Enables restricted VLAN registration

**disable** - Disables restricted VLAN registration

### Mode

Interface Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config-if)# vlan restricted enable
```

- ➡ If restricted VLAN registration rules are enabled, then a VLAN is learnt dynamically from the GVRP frame only if the specific VLAN is statically configured in the switch. If restricted VLAN registration rules are disabled, then GVRP packets are processed normally and the VLANs are learnt dynamically even if they are not statically configured in the switch.

### Related Command

**show vlan port config** - Displays the VLAN related parameters specific for ports

## 15.28 group restricted

This command enables or disables restricted group registration on a port.

```
group restricted {enable | disable }
```

### Syntax Description

**enable** - Enables restricted group registration

**disable** - Disables restricted group registration

### Mode

Interface Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config-if)# group restricted enable
```

- ➡ If restricted group registration rules are enabled, then a multicast group attribute/service requirement attribute is learnt dynamically from the GMRP frame only if the specific multicast group attribute/service requirement attribute is statically configured in the switch. If restricted group registration rules are disabled, then GMRP packets are processed normally and the multicast group attribute/service requirement attribute are learnt dynamically even if they are not statically configured in the switch.

### Related Command

**show vlan port config** - Displays the VLAN related parameters specific for ports

## 15.29 vlan map-priority

This command maps a priority to a traffic class. The frame received with the configured priority will be processed in the configured traffic class..

The no form of the command maps the default priority to traffic class value.

```
vlan map-priority <priority value(0-7)> traffic-class <Traffic class value(0-7)>
```

```
no vlan map-priority <priority value (0-7)>
```

### Syntax Description

**traffic-class** - Traffic class value

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# vlan map-priority 2 traffic-class 2
```

The default traffic class value depends upon the configured priority value.

Following is the list of default traffic class values for different priority values

Priority	Default traffic class
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

### Related Command

**show vlan traffic-classes** - Displays the traffic classes information

## 15.30 shutdown garp

This command shuts down the GARP Module. The no form of the command starts and enables the GARP Module.

**shutdown garp**

**no shutdown garp**

### Mode

Global Configuration Mode

### Defaults

GARP Module is Started and enabled by default

### Example:

```
SMIS(config)# shutdown garp
```

- ➔ GARP cannot be started if VLAN is shutdown.  
GARP cannot be shutdown if GVRP and/or GMRP are enabled

### Related Command

**shutdown vlan** - Shuts down VLAN switching

## 15.31 debug vlan

This command enables module-wise debug traces, which can be any of the following: Forwarding or Priority .

```
debug vlan { global | [{fwd | priority | | redundancy} [initshut]
[mgmt] [data] [ctp1] [dump] [os] [failall] [buffer] [all]] }
```

```
no debug vlan { global | [{fwd | priority | | redundancy} [initshut]
[mgmt] [data] [ctp1] [dump] [os] [failall] [buffer] [all]] }
```

### Syntax Description

**global** - Global related debug messages

**fwd** - Forwarding Module

**priority** - VLAN Priority Module

**redundancy** - Redundancy related debug messages

**initshut** - Init and Shutdown

**mgmt** - Management

**data** - Data path

**ctp1** - Control Plane

**dump** - Packet dump

**os** - Traces related to all Resources except Buffer

**failall** - All Failures

**buffer** - Buffer

**all** - All Traces

### Mode

Privileged Exec Mode

### Defaults

Disabled

### Example:

```
SMIS# debug vlan fwd all
```

### Related Command

**show debugging** - Displays state of each debugging option



## 15.32 debug garp

This command enables module-wise debug traces, which can be GARP, GVRP or GMRP.

```
debug garp { global | [{protocol | gmrp | gvrp | redundancy} [initshut]
[mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]] }
```

```
no debug garp { global | [{protocol | gmrp | gvrp | redundancy}
[initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]] }
```

### Syntax Description

**global** - Global related debug messages

**protocol** - Protocol related traces

**gmrp** - GMRP related traces

**gvrp** - GVRP related traces

**redundancy** Redundancy related debug messages

**initshut** - Init and Shutdown

**mgmt** - Management

**data** - Data path

**ctpl** - Control Plane

**dump** - Packet dump

**os** - Traces related to all Resources except Buffer

**failall** - All Failures

**buffer** - Buffer

**all** - All Traces

### Mode

Privileged Exec Mode

### Defaults

Disabled

### Example:

```
SMIS# debug garp fwd all
```

### Related Command

**show debugging** - Displays state of each debugging option

## 15.33 show vlan

This command displays the VLAN information in the database.

```
show vlan [brief | id <vlan-id(1-4069)> | summary]
```

### Syntax Description

**brief** - Information about all the VLANs in brief

**id** - Information specific to the VLAN Id

**summary** - Summary of the VLAN

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show vlan brief
```

```
Vlan database
```

```
-----
```

```
Vlan ID           : 1
Member Ports      : gi 0/1-48 ex 0/1-4
Tagged Ports      : None
Untagged Ports    : gi 0/1-48 ex 0/1-4
Forbidden Ports   : None
Access Ports      : None
Trunk Ports       : None
Name              :
Status            : Permanent
```

```
-----
```

```
SMIS# show vlan summary
```

```
Number of vlans : 1
```

#### Multiple Instance:

```
SMIS# show vlan
```

```
Switch - default
```

```
Vlan database
```

```
-----
```

Vlan ID : 1  
Member Ports : Gi0/49Untagged Ports : Gi0/49  
Forbidden Ports : None  
Name :  
Status : Permanent

-----  
Switch - cust1  
Vlan database

-----  
Vlan ID : 1  
Member Ports : Gi0/1-6Tagged Ports : None  
Untagged Ports : Gi0/1-6  
Forbidden Ports : None  
Access Ports : None  
Trunk Ports : None  
Name :  
Status : Permanent

-----  
Vlan ID : 20  
Member Ports : Gi0/1  
Tagged Ports : None  
Untagged Ports : Gi0/1  
Forbidden Ports : None  
Access Ports : None  
Trunk Ports : None  
Name :  
Status : Permanent

-----  
Vlan ID : 30  
Member Ports : Gi0/2  
Tagged Ports : None  
Untagged Ports : None  
Forbidden Ports : None  
Access Ports : None  
Trunk Ports : None  
Name :  
Status : Dynamic Gvrp

- ➔ If the optional parameter is not specified then this command displays the VLAN information of all the available interfaces.

### Related Commands

**shutdown vlan** - Shuts down VLAN switching. The no form of the command starts and enables

VLAN switching

**set vlan** - Enables/disables VLAN in the switch

**vlan** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode

**ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports

## 15.34 show vlan device info

This command displays the VLAN related global status variables.

**show vlan device info**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Example:

##### Single Instance:

```
SMIS# show vlan device info
Vlan device configurations
-----
Vlan Status : Enabled
Vlan Oper status : Enabled
Gvrp status : Enabled
Gmrp status : Disabled
Gvrp Oper status : Enabled
Gmrp Oper status : Disabled
Mac-Vlan Status : Disabled
Protocol-Vlan Status : Enabled

Bridge Mode
: Provider Edge

Bridge
Traffic Classes : Enabled

Vlan Operational Learning Mode
: IVL

Version number : 1
Max Vlan id : 4069
Max supported vlans : 1024
```

### Multiple Instance:

```
SMIS# show vlan device info
Switch default
Vlan device configurations
-----
Vlan Status : Enabled
Vlan Oper status : Enabled
Gvrp status : Enabled
Gmrp status : Disabled
Gvrp Oper status : Enabled
Gmrp Oper status : Disabled
Mac-Vlan Status : Disabled
Protocol-Vlan Status : Enabled

Bridge Mode
: Provider Edge

Bridge
Traffic Classes : Enabled

Vlan Operational Learning Mode
: IVL

Version number : 1
Max Vlan id : 4069
Max supported vlans : 1024
```

### Related Commands

**shutdown vlan** - Shuts down VLAN switching. The no form of the command starts and enables VLAN switching

**set vlan** - Enables/disables VLAN in the switch

**vlan** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode

**ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports

**set gvrp** - Enables or disables GVRP on a global basis

**set port gvrp** - Enables or disables GVRP on the interface

**set gmrp** - Enables or disables GMRP on a global basis

**set port gmrp** - Enables or disables GMRP on the interface

**set vlan traffic-classes** - Enables or disables traffic classes

**port protocol-vlan** - Enables port protocol based VLANs

**vlan learning mode** - Configures the VLAN learning mode

**show vlan traffic-classes** - Displays the traffic classes information of all the available interfaces.

**show protocol-vlan** - Displays the entries in the protocol-VLAN database.

## 15.35 show vlan device capabilities

This command displays VLAN capabilities of the device.

**show vlan device capabilities**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Example:

##### Single Instance:

```
SMIS# show vlan device capabilities
```

```
Vlan device capabilities
```

```
-----
```

```
Extended filtering services
```

```
Traffic classes
```

```
Static Entry Individual port
```

```
IVL capable
```

```
SVL capable
```

```
Hybrid capable
```

```
Configurable Pvid Tagging
```

##### Multiple Instance:

```
SMIS# show vlan device capabilities
```

```
Switch - default
```

```
Vlan device capabilities
```

```
-----
```

```
Extended filtering services
```

```
Traffic classes
```

```
Static Entry Individual port
```

```
IVL capable
```

```
SVL capable
```

```
Hybrid capable
```

```
Configurable Pvid Tagging
```

```
Switch - cust1
```

```
Vlan device capabilities
```



-----  
Extended filtering services  
Traffic classes  
Static Entry Individual port  
IVL capable  
SVL capable  
Hybrid capable  
Configurable Pvid Tagging

## 15.36 show vlan traffic-classes

This command displays the VLAN traffic classes mapping.

```
show vlan traffic-classes
```

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Example:

```
SMIS# show vlan traffic-classes
```

#### Related Commands

**vlan** - Configures a VLAN in the switch and is used to enter into the VLAN mode

**ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports

**set vlan traffic-classes** - Enables / disables traffic classes

## 15.37 show garp timer

This command displays the GARP timer information of the available interfaces.

```
show garp timer [{ port <interface-type> <interface-id>}]
```

### Syntax Description

**port** - Interface type and ID of the port

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show garp timer port gigabitethernet 0/1
Garp Port Timer Info (in milli seconds)
-----
Port Join-time Leave-time Leave-all-time
-----
Gi0/1 200 600 10000
```

#### Multiple Instance:

```
SMIS# show garp timer
Switch - default
Garp Port Timer Info (in milli seconds)
-----
Port Join-time Leave-time Leave-all-time
-----
Gi0/49 200 600 10000
Switch - cust1
Garp Port Timer Info (in milli seconds)
-----
Port Join-time Leave-time Leave-all-time
-----
Gi0/1 200 600 10000
Gi0/2 200 600 10000
Gi0/3 200 600 10000
Gi0/4 200 600 10000
```

```
Gi0/5 200 600 10000
```

```
Gi0/6 200 600 10000
```

➔ The timer information is the same for GVRP and GMRP.

### Related Commands

**ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports

**show vlan device info** - Displays the VLAN related global status variables

**set garp timer** - Configures the GARP join time, leave time, and leave all time in milliseconds

## 15.38 show vlan port config

This command displays the VLAN related parameters specific for ports..

```
show vlan port config [{port <interface-type> <interface-id> }]
```

### Syntax Description

**port** - Interface type and ID of the port

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show vlan port config port gi 0/1
```

```
Vlan Port configuration table
```

```
-----
Port Gi0/1
Port Vlan ID           : 1
Port Access Vlan ID   : 1
Port Acceptable Frame Type : Admit All
Port Ingress Filtering : Enabled
Port Mode              : Hybrid Port
Gvrp Status           : Enabled
Port Gmrp Status      : Enabled
Port Gvrp Failed Registrations : 0
Gvrp last pdu origin  : 00:01:02:03:04:21
Port Restricted Vlan Registration : Disabled
Port Restricted Group Registration : Disabled
Mac Based Support     : Enabled
Port-and-Protocol Based Support : Enabled
Default Priority      : 0
Allowed Vlans on Trunk : 1-4069
Trunk Native Vlan Id : 1
-----
Port Gi0/2
Port Vlan ID           : 1
Port Access Vlan ID   : 1
Port Acceptable Frame Type : Admit All
```

```
Port Ingress Filtering           : Enabled
Port Mode                       : Hybrid
Port Gvrp Status                : Enabled
Port Gmrp Status                : Enabled
Port Gvrp Failed Registrations  : 0
Gvrp last pdu origin            : 01:02:03:04:05:06
Port Restricted Vlan Registration : Disabled
Port Restricted Group Registration : Disabled
Mac Based Support                : Disabled
Port-and-Protocol Based Support  : Enabled
Default Priority                 : 5
Allowed Vlans on Trunk           : 1-4069
Trunk Native Vlan Id            : 1
```

---

- ➡ If executed without the optional parameter this command displays the port information of all the available ports.

### Related Commands

**set port gvrp** - Enables or disables GVRP on the interface

**set port gmrp** - Enables or disables GMRP on the interface

**switchport pvid** - Configures the PVID (VLAN ID) that would be assigned to untagged/prioritytagged frames/VLAN tagged frames

**switchport acceptable-frame-type** - Configures the acceptable frame type for the port

**switchport ingress-filter** - Enables ingress filtering on the port

**port mac-vlan** - Enables MAC-based VLAN on the port

**port protocol-vlan** - Enables port protocol based VLANs

**vlan restricted** - Enables/disables restricted VLAN registration on the port

## 15.39 show vlan protocols-group

This command displays the protocol group database.

**show vlan protocols-group**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Example:

##### Single Instance:

```
SMIS# show vlan protocols-group
```

```
Protocol Group Table
```

```
-----
```

```
-----
```

```
Frame Type Protocol Group
```

```
-----
```

```
Enet-v2 IP 1
```

```
Snap Novell 2
```

```
-----
```

##### Multiple Instance:

```
SMIS# show vlan protocols-group
```

```
Switch - default
```

```
Protocol Group Table
```

```
-----
```

```
-----
```

```
Frame Type Protocol Group
```

```
-----
```

```
Enet-v2 IP 1
```

```
Snap Novell 2
```

```
-----
```

#### Related Commands

**map protocol** - Configures the group ID for a specific encapsulation and protocol value combination

**show protocol-vlan** - Displays the entries in the protocol-VLAN database

**switchport map protocols-group** - Maps the protocol group configured to a particular VLAN identifier for the specified interface



## 15.40 show switchport protected

This command displays the protected port configuration. If the group number is provided, it displays the protected port configuration for the given community group number.

```
show switchport protected [group <integer(1-10000000)>]
```

### Syntax Description

**group** – community number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show switchport protected
```

### Related Commands

[switchport protected](#) – Configures the protected port parameters for the given port.

## 15.41 show protocol-vlan

This command displays the entries in protocol-VLAN database.

**show protocol-vlan**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Example:

##### Single Instance:

```
SMIS# show protocol-vlan
```

```
Port Protocol Table
```

```
-----
```

```
Port Group Vlan ID
```

```
-----
```

```
Gi0/2 1 2
```

```
Gi0/1 2 3
```

```
-----
```

##### Multiple Instance:

```
SMIS# show protocol-vlan
```

```
Switch - default
```

```
Port Protocol Table
```

```
-----
```

```
Port Group Vlan ID
```

```
-----
```

```
Gi0/2 1 2
```

```
Gi0/1 2 3
```

```
-----
```

#### Related Command

**switchport map protocols-group** - Maps the protocol group configured to a particular VLAN identifier for the specified interface

## 15.42 show mac-vlan

This command displays the entries in the MAC-VLAN database.

**show mac-vlan**

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Example:

```
SMIS# show mac-vlan
Mac Address          Vlan ID
-----
00:25:90:13:6a:15   10
00:25:90:13:6a:8c   10
00:25:90:13:6a:9b   10
```

#### Related Commands

**mac-vlan** - Enables MAC-based VLAN for all the available interfaces of the VLAN

**show vlan device info** - Displays the VLAN global status variables

## 15.43 show mac-address-table

This command displays the static and dynamic unicast and multicast MAC address table.

```
show mac-address-table [vlan <vlan-id(1-4069)>] [address
<aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> }]
```

### Syntax Description

**vlan** - VLAN ID

**address** - MAC address

**interface** - Interface type and ID

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show mac-address-table vlan 2
```

```
Vlan Mac Address Type Ports
```

```
----
```

```
2 00:01:02:03:04:21 Learnt Gi0/1
```

```
Total Mac Addresses displayed: 1
```

```
SMIS# show mac-address-table interface gigabitethernet 0/1
```

```
Vlan Mac Address Type Ports
```

```
----
```

```
2 00:01:02:03:04:21 Learnt Gi0/1
```

```
1 01:02:03:04:05:06 Static Gi0/1
```

```
Total Mac Addresses displayed: 2
```

- ➡ If executed without the optional parameters this command displays all the static and dynamic MAC entries.

### Related Commands

**vlan** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode

**ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports

**mac-address-table static unicast** - Configures a static unicast MAC address in the

forwarding database

**mac-address-table static multicast** - Configures a static multicast MAC address in the forwarding database

## 15.44 show mac-address-table count

This command displays the number of MAC addresses present on all the VLANs or on the specified VLAN.

```
show mac-address-table count [vlan <vlan-id(1-4069)>]
```

### Syntax Description

**vlan** - VLAN ID

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show mac-address-table count
```

```
Mac Entries for Vlan 1:
```

```
-----
```

```
Dynamic Unicast Address Count : 1
```

```
Dynamic Multicast Address Count : 0
```

```
Static Unicast Address Count : 1
```

```
Static Multicast Address Count : 1
```

```
-----
```

```
Mac Entries for Vlan 2:
```

```
-----
```

```
Dynamic Unicast Address Count : 1
```

```
Dynamic Multicast Address Count : 0
```

```
Static Unicast Address Count : 1
```

```
Static Multicast Address Count : 0
```

```
-----
```

#### Multiple Instance:

```
SMIS# show mac-address-table count switch cust1
```

```
Switch - cust1
```

```
Mac Entries for Vlan 1:
```

```
-----
```

```
Dynamic Unicast Address Count : 1
```

```
Dynamic Multicast Address Count : 0
```

```
Static Unicast Address Count : 0
Static Multicast Address Count : 0
-----
Mac Entries for Vlan 20:
-----
Dynamic Unicast Address Count : 0
Dynamic Multicast Address Count : 0
Static Unicast Address Count : 0
Static Multicast Address Count : 0
-----
Mac Entries for Vlan 30:
-----
Dynamic Unicast Address Count : 0
Dynamic Multicast Address Count : 0
Static Unicast Address Count : 0
Static Multicast Address Count : 0
-----
```

- ➡ If executed without the optional parameter this command displays the MAC addresses present on all the VLANs.

**Related Commands**

**vlan** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode

**ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports

**mac-address-table static unicast** - Configures a static unicast MAC address in the forwarding database

**mac-address-table static multicast** - Configures a static multicast MAC address in the forwarding database

## 15.45 show mac-address-table static unicast

This command displays the statically configured unicast addresses from the MAC address table.

```
show mac-address-table static unicast [vlan <vlan-id(1-4069)>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> }]
```

### Syntax Description

**vlan** - VLAN Id

**Address** - MAC address

**interface** - Interface type and ID

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show mac-address-table static unicast
Vlan Mac Address RecvPort Status Ports
---- -
2 00:11:22:33:44:55 Gi0/2 Del-OnTimeout Gi0/3
```

#### Multiple Instance:

```
SMIS# sh mac-address-table static unicast switch cust1
Switch - cust1
Vlan Mac Address RecvPort Status Ports
---- -
1 00:11:22:33:44:55 Gi0/2 Permanent Gi0/3
Total Mac Addresses displayed: 1
```

- ➡ If executed without the optional parameters this command displays the MAC address table for all the available interfaces.

### Related Commands

**vlan** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode

**ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports



**mac-address-table static unicast** - Configures a static unicast MAC address in the forwarding database

**show mac-address-table dynamic unicast** - Displays the dynamic MAC address table for the specified address or for all the addresses

## 15.46 show mac-address-table static multicast

This command displays the statically configured multicast entries.

```
show mac-address-table static multicast [vlan <vlan-id(1-4069)>]
[address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-
id>]
```

### Syntax Description

**vlan** - VLAN Id

**address** - MAC address

**interface** - Interface type and ID

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show mac-address-table static multicast
```

```
Static Multicast Table
```

```
-----
```

```
Vlan : 1
```

```
Mac Address : 01:02:03:04:05:06
```

```
Receive Port : Gi0/1
```

```
Member Ports : Gi0/1
```

```
Forbidden Ports : Gi0/2
```

```
Status : Permanent
```

```
-----
```

```
Total Mac Addresses displayed: 1
```

#### Multiple Instance:

```
SMIS# sh mac-address-table static multicast switch cust1
```

```
Switch - cust1
```

```
Static Multicast Table
```

```
-----
```

```
Vlan : 1
```

```
Mac Address : 01:02:03:04:05:06
```

Receive Port : Gi0/2

Member Ports : Gi0/3

Status : Permanent

-----

Total Mac Addresses displayed: 1

### Related Commands

**vlan** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode

**ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports

**mac-address-table static multicast** - Configures a static multicast MAC address in the forwarding database

**show mac-address-table dynamic multicast** - Displays the dynamic MAC address table for the specified address or for all the addresses

## 15.47 show mac-address-table dynamic unicast

This command displays the dynamically learnt unicast entries from the MAC address table.

```
show mac-address-table dynamic unicast [vlan <vlan-id(1-4069)>]
[address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-
id> }]
```

### Syntax Description

**vlan** - VLAN Id

**address** - MAC address

**interface** - Interface type and ID

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show mac-address-table dynamic unicast vlan 2
```

```
Vlan Mac Address Type Ports
```

```
---- -
```

```
2 00:01:02:03:04:21 Learnt Gi0/1
```

```
Total Mac Addresses displayed: 1
```

#### Multiple Instance:

```
SMIS# show mac-address-table dynamic unicast
```

```
Switch - default
```

```
Vlan Mac Address Type Ports
```

```
---- -
```

```
1 00:02:02:03:04:04 Learnt Gi0/2
```

```
1 00:03:02:03:04:04 Learnt Gi0/3
```

```
2 00:02:02:03:04:04 Learnt Gi0/2
```

```
2 00:03:02:03:04:04 Learnt Gi0/3
```

```
3 00:02:02:03:04:04 Learnt Gi0/2
```

```
3 00:03:02:03:04:04 Learnt Gi0/3
```

```
Total Mac Addresses displayed: 6
```

- ▶ If executed without the optional parameters this command displays the MAC address table of all the available interfaces

### Related Commands

**vlan** - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode

**ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports

**mac-address-table static unicast** - Configures a static unicast MAC address in the forwarding database

**show mac-address-table static unicast** - Displays the statically configured unicast address from the MAC address table

## 15.48 show mac-address-table dynamic multicast

This command displays the dynamically learnt multicast MAC address.

```
show mac-address-table dynamic multicast [vlan <vlan-id(1-4069)>]
[address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-
id> }]
```

### Syntax Description

**vlan** - VLAN Id

**address** - MAC address

**interface** - Interface type and ID

### Mode

Privileged EXEC Mode

### Example:

#### Single Instance:

```
SMIS# show mac-address-table dynamic multicast
```

```
Vlan Mac Address Type Ports
```

```
---- -
```

```
2 01:03:05:07:09:04 Learnt Gi0/1
```

```
Total Mac Addresses displayed: 1
```

#### Multiple Instance:

```
SMIS# show mac-address-table dynamic multicast
```

```
Switch - default
```

```
Vlan Mac Address Type Ports
```

```
---- -
```

```
2 01:02:02:02:02:02 Learnt Gi0/2, Gi0/3
```

```
3 01:02:02:02:02:02 Learnt Gi0/2
```

```
3 01:03:03:03:03:03 Learnt Gi0/3
```

```
Total Mac Addresses displayed: 3
```

- ➔ If executed without the optional parameters this command displays the MAC address table of all the available interfaces.

### Related Commands

**vlan** - Configures a VLAN in the switch and is also used to enter into the config-VLAN mode

**ports** - Configures a static VLAN entry with the required member ports, untagged ports and forbidden ports

**mac-address-table static multicast** - Configures a static multicast MAC address in the forwarding database

**show mac-address-table static multicast** - Displays the statically configured multicast entries

## 15.49 show mac-address-table aging-time

This command displays the MAC address-table ageing time.

```
show mac-address-table aging-time
```

### Syntax Description

#### Mode

Privileged EXEC Mode

#### Example:

##### Single Instance:

```
SMIS# show mac-address-table aging-time  
Mac Address Aging Time: 300
```

### Related Commands

**show mac-address-table** - Displays the static and dynamic MAC entries

**mac-address-table aging-time** - Configures the MAC address table entry maximum age



## 15.50 show wildcard

This command displays the wildcard MAC address entries from MAC table.

```
show wildcard {mac-address <mac_addr> | broadcast}
```

### Syntax Description

<mac\_addr> - MAC address

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show wildcard mac-address 03:04:06
```

Wild Card Entries:

```
-----  
      Mac Address      Ports  
----- , -----  
00:03:00:04:00:06  Gi0/1
```

### Related Commands

**wildcard mac-address** – Add wildcard MAC address entries to MAC address table.

## 16 DHCP

DHCP (Dynamic Host Configuration Protocol) allows dynamic configuration of a host computer. When a DHCP client is turned on, it initially does not have an IP address assigned to it. It issues a broadcast message to any DHCP servers which are on the network. An exchange takes place during which the DHCP server assigns an IP address to the client and tells the client certain key network configuration parameters.

Many Internet service providers (ISPs) require that their customers use a DHCP client so the ISP may dynamically assign IP addresses and control other network settings. Another use is for laptop computers which may be connected to more than one network. For example: a laptop may be connected to a network in the office and also at home. This is an ideal use for DHCP as the laptop doesn't need to be manually reconfigured for use in the 2 different networks. In this case, there needs to be a DHCP server both on the office network and the home network and the laptop needs a DHCP client.

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

### **DHCP Client**

[release](#)

[renew](#)

[debug ip dhcp client](#)

[show ip dhcp client stats](#)

### **DHCP Relay**

[service dhcp-relay](#)

[ip dhcp server](#)

[ip dhcp relay information option](#)

[ip dhcp relay circuit-id](#)

[ip dhcp relay remote-id](#)

[debug ip dhcp relay](#)

[show ip dhcp relay information](#)

[show dhcp server](#)

## **DHCP Server**

[service dhcp-server](#)

[ip dhcp pool](#)

[ip dhcp next-server](#)

[ip dhcp bootfile](#)

[ip dhcp](#)

[ip dhcp option](#)

[network](#)

[excluded-address](#)

[domain-name](#)

[dns-server](#)

[netbios-name-server](#)

[netbios-node-type](#)

[default-router](#)

[option](#)

[lease](#)

[utilization threshold](#)

[host hardware-type](#)

[host hardware-type mac binding](#)

[interface ip binding](#)

[debug ip dhcp server](#)

[show ip dhcp server information](#)

[show ip dhcp server pools](#)

[show ip dhcp server binding](#)

[show ip dhcp server statistics](#)



## 16.1 DHCP Client

### 16.1.1 release

This command immediately releases the DHCP lease on the interface specified.

```
release dhcp [{ vlan <short (1-4069)> | <iftype> <ifnum> }]
```

#### Syntax Description

**vlan** - VLAN Identifier

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

#### Mode

Privileged EXEC Mode

#### Defaults

Disabled by default

#### Example:

```
SMIS# release dhcp vlan 1
```

- ➡ VLAN interface must have an IP address assigned by the DHCP server.
- ➡ If the router interface was not assigned a DHCP IP address by the DHCP server, the release dhcp command fails and displays the following error message: Interface does not have a DHCP originated address

#### Related Commands

**ip address** - Configures the current VLAN interface to dynamically acquire an IP address from the DHCP server

**show ip dhcp client stats** - Displays the DHCP client statistics information

**show ip interface** - Displays the IP interface statistics and configuration



## 16.1.2 renew

This command immediately renews the DHCP lease for the interface specified.

```
renew dhcp [{ vlan <short (1-4069)> | <iftype> <ifnum> }]
```

### Syntax Description

**vlan-id** - VLAN Identifier

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Defaults

Disabled

### Example:

```
SMIS# renew dhcp vlan 1
```

- ➔ VLAN interface must have an IP address assigned by the DHCP server
- ➔ If the router interface was not assigned an IP address by the DHCP server, the **renew** DHCP command fails and displays the following error message:  
`Interface does not have a DHCP originated address`

### Related Commands

**ip address** - Configures the current VLAN interface to dynamically acquire an IP address from the DHCP server

**show ip dhcp client stats** - Displays the DHCP client statistics information

### 16.1.3 debug ip dhcp client

This command sets the debug level for tracing the DHCP client module. The no form of the command disables the debug level for the DHCP client.

```
debug ip dhcp client { all | event | packets | errors | bind }
```

```
no debug ip dhcp client { all | event | packets | errors | bind }
```

#### Syntax Description

**all** - All trace messages

**event** - Trace management messages

**packets** - Packets related messages

**errors** - Trace error code debug messages

**bind** - Trace bind messages

#### Mode

Privileged EXEC Mode

#### Defaults

Debugging is Disabled

#### Example:

```
SMIS# debug ip dhcp client all
```

#### Related Command

**show ip dhcp client stats** - Displays the DHCP client statistics information



## 16.1.4 show ip dhcp client stats

This command displays the DHCP client statistics.

**show ip dhcp client stats**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip dhcp client stats
```

```
Dhcp Client Statistics
```

```
-----
```

```
Interface : vlan3
```

```
Client IP Address : 0.0.0.0
```

```
Client Lease Time : 0
```

```
Client Remain Lease Time : 0
```

```
Message Statistics
```

```
-----
```

```
DHCP DISCOVER : 1
```

```
DHCP REQUEST : 0
```

```
DHCP DECLINE : 0
```

```
DHCP RELEASE : 0
```

```
DHCP INFORM : 0
```

```
DHCP OFFER : 1
```

### Related Commands

**ip address** - Configures the current VLAN interface to dynamically acquire an IP address from the DHCP server

**release** - Releases the DHCP lease on the interface specified

**renew** - Renews the DHCP lease for the interface specified

## 16.2 DHCP Relay

### 16.2.1 service dhcp-relay

This command enables the DHCP Relay agent in the switch. The no form of the command disables the DHCP relay agent.

**service dhcp-relay**

**no service dhcp-relay**

#### Mode

Global Configuration Mode

#### Defaults

Disabled

#### Example:

```
SMIS(config)# service dhcp-relay
```

The relay agent becomes active only after it is enabled

#### Related Commands

**show dhcp server** - Displays the DHCP server information

**show ip dhcp relay information** - Displays the DHCP relay information

## 16.2.2 ip dhcp server

This command set the IP address of the DHCP server. The Relay Agent will now start forwarding the packets from the client to a specific DHCP server. The no form of the command deletes the DHCP server IP address.

```
ip dhcp server <ip address>
```

```
no ip dhcp server <ip address>
```

### Mode

Global Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config)# ip dhcp server 12.0.0.1
```

Only when the relay agent is enabled, the Relay Agent shall forward the packets from the client to a specific DHCP server.

### Related Commands

**show ip dhcp relay information** - Displays the DHCP relay information

**show dhcp server** - Displays the DHCP server information

### 16.2.3 ip dhcp relay information option

This command enables the Relay Agent to perform any processing related to relay agent Information Options. When this option is enabled, the agent will insert and remove DHCP relay information in forwarded DHCP request messages to the DHCP server. The no form of this command disables the insertion of relay information.

```
ip dhcp relay information option
```

```
no ip dhcp relay information option
```

#### Mode

Global Configuration Mode

#### Defaults

Disabled

#### Example:

```
SMIS(config)# ip dhcp relay information option
```

- ➔ Only when enabled, the Relay Agent does any processing related to Relay Agent Information Options - like inserting the necessary options while relaying a packet from a client to a server and examining/stripping of options when relaying a packet from a server to a client.

#### Related Commands

**show ip dhcp relay information** - Displays the DHCP relay information

**show dhcp server** - Displays the DHCP server information

## 16.2.4 ip dhcp relay circuit-id

This command configures circuit identifier value to be used by the relay agent on the sub option 1 of the relay information option 82 to DHCP servers. The no form of this command clears the circuit identifier configuration. This is interface specific configuration.

```
ip dhcp relay circuit-id <id>
```

```
no ip dhcp relay circuit-id
```

### Syntax

<id> - Any number between 1 to 2147483647

### Mode

Interface Configuration Mode

### Defaults

No circuit id option sent

### Example:

```
SMIS(config-if)# ip dhcp relay circuit-id 1000
```

### Related Commands

**show ip dhcp relay information** - Displays the DHCP relay information

**show dhcp server** - Displays the DHCP server information

## 16.2.5 ip dhcp relay remote-id

This command configures remote identifier string to be used by the relay agent on the sub option 1 of the relay information option 82 to DHCP servers. The no form of this command clears the remote identifier configuration. This is interface specific configuration.

```
ip dhcp relay remote-id <name>
```

```
no ip dhcp relay remote-id
```

### Syntax

<name> - Any alphanumerical string up to 32 characters length

### Mode

Interface Configuration Mode

### Defaults

None

### Example:

```
SMIS(config-if)# ip dhcp relay remote-id dhc_rell
```

### Related Commands

**show ip dhcp relay information** - Displays the DHCP relay information

**show dhcp server** - Displays the DHCP server information

## 16.2.6 debug ip dhcp relay

This command enables the debug level for tracing the DHCP Relay Module. The no form of the command disables the debug level for tracing the DHCP relay Module.

```
debug ip dhcp relay {all | errors}
```

```
no debug ip dhcp relay {all | errors}
```

### Syntax Description

**all** - All trace messages

**errors** - Trace error code debug messages

### Mode

Privileged EXEC Mode

### Defaults

Debugging is disabled

### Example:

```
SMIS# debug ip dhcp relay all
```

### Related Commands

**show ip dhcp relay information** - Displays the DHCP relay information

**show dhcp server** - Displays the DHCP server information

## 16.2.7 show ip dhcp relay information

This command displays the DHCP Relay Information.

```
show ip dhcp relay information [vlan <integer (1-4069)>] [<iftype>
<ifnum>]
```

### Syntax Description

**vlan** - VLAN ID

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip dhcp relay information
Dhcp Relay : Enabled
Dhcp Relay Servers only : Enabled
Server Ip Address : 40.0.0.4
Dhcp Relay RAI option : Enabled
Debug Level : 0x1
No of Packets inserted RAI option : 0
No of Packets inserted circuit ID suboption : 0
No of Packets inserted remote ID suboption : 0
No of Packets inserted subnet mask suboption : 0
No of Packets dropped : 0
No of Packets which did not inserted RAI option : 0
```

### Related Commands

**service dhcp-relay** - Enables the DHCP relay agent in the switch

**ip dhcp server** - Sets the IP address of the DHCP server

**ip dhcp relay information option** - Enables the Relay Agent to perform any processing related to relay agent Information Options



## 16.2.8 show dhcp server

This command displays the DHCP server information.

**show dhcp server**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show dhcp server
DHCP server: 40.0.0.4
```

### Related Commands

**service dhcp-relay** - Enables the DHCP relay agent in the switch

**ip dhcp server** - Sets the IP address of the DHCP server

**ip dhcp relay information option** - Enables the Relay Agent to perform any processing related to relay agent Information Options

## 16.3 DHCP Server

### 16.3.1 service dhcp-server

This command enables the DHCP server. The no form of this command disables the DHCP server.

**service dhcp-server**

**no service dhcp-server**

#### Mode

Global Configuration Mode

#### Defaults

Disabled

#### Example:

```
iss (config)# service dhcp-server
```

➡ DHCP Relay must be disabled before enabling the DHCP server.

#### Related Command

**show ip dhcp server information** - Displays the DHCP server information

## 16.3.2 ip dhcp pool

This command creates a DHCP server address pool and places the user in the DHCP pool configuration mode.

The no form of the command deletes the DHCP server address pool.

```
ip dhcp pool <index (1-2147483647)>
```

```
no ip dhcp pool <index (1-2147483647)>
```

### Syntax Description

**Index** - Pool Number

### Mode

Global Configuration Mode

### Defaults

Address pools are not created by default

### Example:

```
iss (config)# ip dhcp pool 1
```

- ➡ On execution of this command, the configuration mode changes to DHCP pool configuration mode identified by the `(config-dhcp)#` prompt. In this mode, the administrator can configure pool parameters.

### Related Commands

**network** - Sets the network number and mask in DHCP server configuration parameters

**excluded-address** - Creates an excluded pool to prevent DHCP from assigning certain addresses

**domain-name** - Sets the domain name in the DHCP server configuration parameters

**dns-server** - Specifies the IP address of a DNS server

**netbios-name-server** - Sets the NetBIOS (WINS) name servers in the DHCP server configuration parameters

**netbios-node-type** - Sets the NetBios node type in the DHCP server configuration parameters

**default-router** - Sets the default router in the DHCP server configuration parameters

**option** - Sets the pool specific DHCP server option

**lease** - Sets the lease period

**host hardware-type** - Specifies the hardware address of a Dynamic Host Configuration Protocol (DHCP) client

**show ip dhcp server information** - Displays the DHCP server information

**show ip dhcp server pools** - Displays the DHCP server pools

### 16.3.3 ip dhcp next-server

This command sets the next boot server in the DHCP server configuration parameters. The no form of this command deletes the next boot server from the DHCP server configuration parameters.

```
ip dhcp next-server <ip address>
```

```
no ip dhcp next-server
```

#### Syntax Description

**ip address** - IP address of the server (TFTP server)

#### Mode

Global Configuration Mode

#### Example:

```
iss (config)# ip dhcp next-server 12.0.0.1
```

#### Related Commands

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the DHCP server information

**show ip dhcp server binding** - Displays the DHCP server binding information

**show ip dhcp server pools** - Displays the DHCP server pools

**show ip dhcp server statistics** - Displays the DHCP server statistics

## 16.3.4 ip dhcp bootfile

This command sets the boot file name in the DHCP server configuration parameters. The no form of this command deletes the boot file name from the DHCP server configuration parameters.

```
ip dhcp bootfile <bootfile (63)>
```

```
no ip dhcp bootfile
```

### Syntax Description

**boot file** - Name of the file that specifies the boot image

### Mode

Global Configuration Mode

### Example:

```
iss (config)# ip dhcp bootfile 53
```

### Related Commands

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the DHCP server information

## 16.3.5 ip dhcp

This command sets the DHCP server parameters such as enabling ICMP echo mechanism or offer-reuse timeout. The no form of this command is used to set the DHCP server parameters like disabling ICMP echo mechanism or server offer-reuse to its default value or removing a bind entry from the server binding table.

```
ip dhcp { ping packets | server offer-reuse <timeout (1-120)> }
```

```
no ip dhcp { ping packets | server offer-reuse | binding <ip address> }
```

### Syntax Description

**ping packets** - Enable icmp echoes prior to assigning a pool address. The no form of this command option prevents the server from pinging pool addresses

**server offerreuse** - The amount of time the DHCP server entity would wait for the DHCP REQUEST from the client before reusing the offer

**binding** - The binding option if specified deletes the specified address from binding

### Mode

Global Configuration Mode

### Defaults

server offer-reuse - 10

### Example:

```
iss (config)# ip dhcp ping packets
```

- ➔ The DHCP server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

### Related Commands

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the DHCP server information

**show ip dhcp server binding** - Displays the DHCP server binding information

**show ip dhcp server pools** - Displays the DHCP server pools

**show ip dhcp server statistics** - Displays the DHCP server statistics

## 16.3.6 ip dhcp option

This command sets the DHCP server options.

```
ip dhcp option <code (1-2147483647)> { ascii <string> | hex <Hex
String> | ip <address> }
```

```
no ip dhcp option <code (1-2147483647)>
```

### Syntax Description

**code** - Option Code

**ascii** - ASCII string

**hex** - Hexadecimal string

**ip** - IP address

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# ip dhcp option 19 hex d
```

RFC 2132 provides details about option code to option name mapping and the option length information.

The following is the list of supported/configurable DHCP options with their corresponding option length values

- Options 19, 20, 27, 29, 30, 31, 34, 36, 39, 46 must have length 1
- Options 12, 14, 15, 17, 18, 40, 43, 47, 64, 66, 67 must have length >=1
- Option 16 must have minimum length 4 and the value for this option must be an IP address and Option 25 can have a length of 2 and 2\*n
- Option 68 must have length 4 and the value for this option must be an IP address
- Options 1-11, 41, 42, 44, 45, 48, 49, 65, 69, 70-76 must have a length of 4 . Value for these options must be an IP address
- Options 21, 33 must have minimum length as 8 and 8\*n
- Options 0, 255, 50-60 are non-configurable options

### Related Commands

**service dhcp-server**- Enables the DHCP server



**show ip dhcp server pools** - Displays the DHCP server pools

**option-** Sets the pool specific DHCP server option

## 16.3.7 network

This command sets the network IP address and mask in DHCP server configuration parameters. The no form of the command deletes the network IP address and mask from DHCP server configuration.

```
network <network- IP> [ { <mask> | / <prefix-length (1-31)> } ] [end ip]
```

```
no network
```

### Syntax Description

**network-IP** - Network IP address of the DHCP pool

**mask** - Subnet mask of the DHCP pool

**prefix-length** - The number of bits that comprise the address prefix. Prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

**end ip** - End IP address of the pool

### Mode

DHCP Pool Configuration Mode

### Example:

```
SMIS(dhcp-config)# network 20.0.0.0 255.0.0.0 20.0.0.10
```

➔ This command is valid for DHCP sub network address pools only.

### Related Commands

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the server information

**show ip dhcp server pools** - Displays the DHCP server pools

**show ip dhcp server binding** - Displays the DHCP server binding information

**show ip dhcp server statistics** - Displays the DHCP server statistics

## 16.3.8 excluded-address

This command creates an excluded pool to prevent DHCP Server from assigning certain addresses. The no form of the command deletes the excluded pool.

```
excluded-address <low-address> <high-address>
```

```
no excluded-address <low-address> [<high-address>]
```

### Syntax Description

**low-address** - The excluded IP address, or first IP address in an excluded address range

**high-address** - The last IP address in the excluded address range

### Mode

DHCP Pool Configuration Mode

### Example:

```
SMIS(dhcp-config)# excluded-address 20.0.0.1 20.0.0.30
```

- ➡ The DHCP server assumes that all pool addresses may be assigned to clients. This command is used to exclude a single IP address or a range of IP addresses.

### Related Commands

**network** - Sets the network IP and mask in DHCP server configuration parameters

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the server information

**show ip dhcp server pools** - Displays the DHCP server pools

**show ip dhcp server binding** - Displays the DHCP server binding information

**show ip dhcp server statistics** - Displays the DHCP server statistics

### 16.3.9 domain-name

This command sets the domain name in the DHCP server configuration parameters. The no form of the command deletes the domain name from the DHCP server configuration parameters.

```
domain-name <domain (63)>
```

```
no domain-name
```

#### Syntax Description

**domain** - Client's domain name string

#### Mode

DHCP Pool Configuration Mode

#### Example:

```
SMIS(dhcp-config)# domain-name supermicro
```

The configuration of this command will take effect only after configuring the network address pool using network command.

#### Related Commands

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the server information

**show ip dhcp server pools** - Displays the DHCP server pools

**show ip dhcp server binding** - Displays the DHCP server binding information

**show ip dhcp server statistics** - Displays the DHCP server statistics

**network** - Configures the network IP address of the DHCP Address Pool

### 16.3.10 dns-server

This command is used to specify the IP address of a DNS server that is available to a DHCP client. The no form of the command deletes the DNS server from the DHCP server configuration parameters.

**dns-server** <ip address>

**no dns-server**

#### Mode

DHCP Pool Configuration Mode

#### Example:

```
SMIS(dhcp-config)# dns-server 20.0.0.1
```

- ➔ If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.
- ➔ The configuration of this command will take effect only after configuring the network address pool using network command.

#### Related Commands

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the server information

**show ip dhcp server pools** - Displays the DHCP server pools

**show ip dhcp server binding** - Displays the DHCP server binding information

**show ip dhcp server statistics** - Displays the DHCP server statistics

**network** - Configures the Network IP for the DHCP Pool

### 16.3.11 netbios-name-server

This command sets the NetBIOS (WINS) name servers in the DHCP server configuration parameters.

The no form of the command deletes the NetBIOS name server from the DHCP configuration parameters.

```
netbios-name-server <ip address>
```

```
no netbios-name-server
```

#### Mode

DHCP Pool Configuration Mode

#### Example:

```
SMIS(dhcp-config)# netbios-name-server 20.0.0.3
```

- ➔ The configuration of this command will take effect only after configuring the network address pool using network command.

#### Related Commands

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the server information

**show ip dhcp server pools** - Displays the DHCP server pools

**show ip dhcp server binding** - Displays the DHCP server binding information

**show ip dhcp server statistics** - Displays the DHCP server statistics

**network** - Configures the Network IP of the address pool

## 16.3.12 netbios-node-type

This command is used to set the NetBios node type in the DHCP server configuration parameters. The no form of this command is used to delete the NetBios node type from the DHCP server configuration parameters.

The NetBIOS node type for Microsoft DHCP clients can be one of the four settings: broadcast, peer-to-peer, mixed, or hybrid.

```
netbios-node-type { <0-FF> | b-node | h-node | m-node | p-node }
```

```
no netbios-node-type
```

### Syntax Description

**0-FF** - Node type value

**b-node** - Broadcast node

**h-node** - Hybrid node

**m-node** - Mixed node

**p-node** - Peer-to-peer node

### Mode

DHCP Pool Configuration Mode

### Example:

```
SMIS(dhcp-config)# netbios-node-type h-node
```

The recommended type is hybrid node.

The configuration of this command will take effect only after configuring the network address pool using network command.

### Related Commands

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the server information

**show ip dhcp server pools** - Displays the DHCP server pools

**show ip dhcp server binding** - Displays the DHCP server binding information

**show ip dhcp server statistics** - Displays the DHCP server statistics

**network** - Configures the Network IP of the address pool

### 16.3.13 default-router

This command sets the default router in the DHCP server configuration parameters. The no form of the command deletes the default router from the DHCP server configuration parameters.

```
default-router <ip address>
```

```
no default-router
```

#### Mode

DHCP Pool Configuration Mode

#### Example:

```
SMIS(dhcp-config)# default-router 10.23.2.99
```

- ➔ The configuration of this command will take effect only after configuring the network address pool using network command.

#### Related Commands

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the server information

**show ip dhcp server pools** - Displays the DHCP server pools

**show ip dhcp server binding** - Displays the DHCP server binding information

**show ip dhcp server statistics** - Displays the DHCP server statistics

**network** - Configures the Network IP of the address pool



## 16.3.14 option

This command sets the pool specific DHCP server option. The no form of the command deletes the pool specific DHCP server option.

```
option <code (1-2147483647)> { ascii <string> | hex <Hex String> | ip  
<address> }
```

```
no option <code (1-2147483647)>
```

### Syntax Description

**code** - Option Code

**ascii** - ASCII string

**hex** - Hexadecimal string

**ip** - IP address

### Mode

DHCP Pool Configuration Mode

### Example:

```
SMIS(dhcp-config) # option 19 hex f
```

RFC 2132 provides details about option code to option name mapping and the option length information.

The following is the list of supported/configurable DHCP options with their corresponding option length values

- Options 19, 20, 27, 29, 30, 31, 34, 36, 39, 46 must have length 1
- Options 12, 14, 15, 17, 18, 40, 43, 47, 64, 66, 67 must have length>=1
- Option 16 must have minimum length 4 and the value for this option must be an IP address and Option 25 can have a length of 2 and 2\*n
- Option 68 must have length 4 and the value for this option must be an IP address
- Options 1-11, 41, 42, 44, 45, 48, 49, 65, 69, 70-76 must have a length of 4 . Value for these options must be an IP address
- Options 21, 33 must have minimum length as 8 and 8\*n
- Options 0, 255, 50-60 are non-configurable options

- ▶ Network pool must be configured prior to the execution of this command. Only then the configured option will be visible to the user in the show command output. If the network pool is deleted, then the option configured for that network pool will also get deleted.

### Related Commands

**service dhcp-server** - Enables the DHCP server

**ip dhcp pool** - Creates a DHCP server address pool and places the user in the DHCP pool configuration mode

**ip dhcp option** - Sets the DHCP server options

**network** - Sets the network IP and mask in DHCP server configuration parameters

**show ip dhcp server pools** - Displays the DHCP server pools

### 16.3.15 lease

This command configures the duration of the lease for an IP address that is assigned from ISS Dynamic

Host Configuration Protocol (DHCP) Server to a DHCP client. The no form of this command restores the default value of 3600 seconds.

```
lease { <days (0-365)> [<hours (0-23)> [<minutes (0-59)>]] | infinite }
```

```
no lease
```

#### Syntax Description

**days** - Duration of the lease in number of days

**hours** - Number of hours in lease

**minutes** - Number of minutes in lease

**infinite** - Duration of the lease is unlimited

#### Mode

DHCP Pool Configuration Mode

#### Defaults

3600 seconds

#### Example:

```
SMIS(dhcp-config)# lease 1
```

#### Related Commands

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the server information

**show ip dhcp server pools** - Displays the DHCP server pools

**show ip dhcp server binding** - Displays the DHCP server binding information

**show ip dhcp server statistics** - Displays the DHCP server statistics

### 16.3.16 utilization threshold

This command sets the pool utilization threshold value in percentage. If the pool utilization reaches this threshold level, a syslog event and an SNMP trap message will be generated. The no form of this command sets pool utilization threshold to its default value.

```
utilization threshold { <integer (0-100)> }
```

```
no utilization threshold
```

#### Mode

DHCP Pool Configuration Mode

#### Defaults

75

#### Example:

```
SMIS(dhcp-config)# utilization threshold 76
```

#### Related Commands

**show ip dhcp server pools** - Displays the DHCP server pools

**logging** - Enables Syslog server and configures the Syslog Server IP address, the log-level and other Syslog related parameters

### 16.3.17 host hardware-type

This command specifies the hardware address of a Dynamic Host Configuration Protocol (DHCP) client and host specific DHCP options. The no form of the command deletes the host option.

```
host hardware-type <type (1-2147483647)> client-identifier <mac-address> option <code (1-2147483647)> { ascii <string> | hex <Hex String> | ip <address> }
```

```
no host hardware-type <host-hardware-type (1-2147483647)> client-identifier <client-mac-address> option <code (1-2147483647)>
```

#### Syntax Description

**type**- Host hardware address type

**client identifier** - Host MAC address

**option** - The tag octet of the DHCP option

**ascii** - ASCII String

**hex** - Hex String

**ip** - Host IP address

#### Mode

DHCP Pool Configuration Mode

#### Example:

```
SMIS(dhcp-config)# host hardware-type 1 client-identifier  
00:11:22:33:44:55 option 254 ip 10.0.0.1
```

The current valid values are only 0 and 1.

#### Related Commands

**service dhcp-server** - Enables the DHCP server

**ip dhcp pool** - Creates a DHCP server address pool and places the user in the DHCP pool configuration mode

### 16.3.18 host hardware-type mac binding

This command configures a fixed IP address to specific client devices based on their MAC address. The “no” form of this command removes the fixed IP address configured for the given client MAC.

```
host hardware-type <type> client-identifier <mac-address> ip <ip-  
address>
```

```
no host hardware-type <type> client-identifier <mac-address> ip <ip-  
address>
```

#### Syntax Description

**type**- Host hardware address type – Currently supported type is 1 (MAC address)

**client identifier** – Client host MAC address

**ip-address** - Fixed IP address to be assigned to this client host. This IP address must be part of the pool network and also not configured as exclude IP.

#### Mode

DHCP Pool Configuration Mode

#### Example:

```
SMIS(dhcp-config)# host hardware-type 1 client-identifier  
00:11:22:33:44:55 ip 1.2.3.4
```

#### Related Commands

**show ip dhcp server pools** - Displays the DHCP server pools configuration

**ip dhcp pool** - Creates a DHCP server address pool and places the user in the DHCP pool configuration mode

## 16.3.19 interface ip binding

This command configures a fixed IP address to the client devices connected to the given specific ports. The “no” form of this command removes the fixed IP address configured for the given port.

```
interface <interface-type> <interface-id> ip <ip-address>
```

```
no interface <interface-type> <interface-id> ip <ip-address>
```

### Syntax Description

**interface-type** - Interface type, e.g: ex.

**interface-id** - Physical interface ID including slot and port number.

**ip-address** - Fixed IP address to be assigned to this client host. This IP address must be part of the pool network and also not configured as exclude IP.

### Mode

DHCP Pool Configuration Mode

### Example:

```
SMIS(dhcp-config)# interface gi 0/1 ip 192.168.1.1
```

### Related Commands

**show ip dhcp server pools** - Displays the DHCP server pools configuration

**ip dhcp pool** - Creates a DHCP server address pool and places the user in the DHCP pool configuration mode

### Note:

This command is suitable mainly for the cases where only one device is connected to a port. If multiple devices are connected to the same port (through another switch), the configured IP address will be assigned to the first DHCP DISCOVER sent by the client host.

## 16.3.20 debug ip dhcp server

This command enables the debug level for tracing the DHCP server Module. The “no” form of this command disables the debug level for tracing the DHCP server Module.

```
debug ip dhcp server { all | events | packets | errors | bind }
```

```
no debug ip dhcp server { all | events | packets | errors | bind }
```

### Syntax Description

**all** - All trace messages

**events** - Trace management messages

**packets** - Packet related messages

**errors** - Trace error code debug messages

**bind** - Trace bind messages

### Mode

Privileged EXEC Mode

### Defaults

Debugging is disabled

### Example:

```
SMIS# debug ip dhcp server all
```

### Related Commands

**service dhcp-server** - Enables the DHCP server

**show ip dhcp server information** - Displays the server information

**show ip dhcp server binding** - Displays the DHCP server binding information



## 16.3.21 show ip dhcp server information

This command displays the DHCP server information.

**show ip dhcp server information**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip dhcp server information
DHCP server status : Enable
Send Ping Packets : Disable
Debug level : None
Server Address Reuse Timeout : 5 secs
Next Server Address : 0.0.0.0
Boot file name : None
```

### Related Commands

**service dhcp-server** - Enables the DHCP server

**ip dhcp next-server** - Sets the next boot server in the DHCP server configuration parameters

**ip dhcp bootfile** - Sets the boot file name in the DHCP server configuration parameters

**ip dhcp** - Sets the DHCP server parameters such as enabling ICMP echo mechanism or offer-reuse timeout

## 16.3.22 show ip dhcp server pools

This command displays the DHCP server pools.

**show ip dhcp server pools**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip dhcp server pools
```

```
Pool Id : 1
```

```
-----
```

```
Subnet : 12.0.0.0
```

```
Subnet Mask : 255.0.0.0
```

```
Lease time : 180 secs
```

```
Start Ip : 12.0.0.1
```

```
End Ip : 12.255.255.255
```

```
Exclude Address Start IP : 12.0.0.1
```

```
Exclude Address End IP : 12.0.0.10
```

```
Pool Id : 2
```

```
-----
```

```
Subnet : 20.0.0.0
```

```
Subnet Mask : 255.0.0.0
```

```
Lease time : 7200 secs
```

```
Start Ip : 20.0.0.1
```

```
End Ip : 20.255.255.255
```

### Related Commands

**service dhcp-server** - Enables the DHCP server

**ip dhcp pool** - Creates a DHCP server address pool and places the user in the DHCP pool configuration mode

**lease** - Configures the duration of the lease for an IP address that is assigned from ISS Dynamic Host Configuration Protocol (DHCP) Server to a DHCP client

**network** - Sets the network IP and mask in DHCP server configuration parameters

### 16.3.23 show ip dhcp server binding

This command displays the DHCP server binding information.

**show ip dhcp server binding**

**Mode**

Privileged EXEC Mode

**Example:**

```
SMIS# show ip dhcp server binding
Ip Hw Hw Alloc Expire Binding
Address Type Address Method Time State
(SeCs)
-----
12.0.0.11 Ethernet 00:01:02:03:04:41 Dynamic 161 Assigned
20.0.0.1 Ethernet 00:01:02:03:04:31 Dynamic 7152 Assigned
```

Binding refers to the state of binding. This can be “offered”, “assigned” or “probing”. In the “offered” state an offer is sent, but no “req” has been received from the client. In the “assigned” state the address is assigned to the client. In the “probing” state the address is currently being probed by the DHCP server.

**Related Commands**

- service dhcp-server** - Enables the DHCP server
- host hardware-type** - Specifies the hardware address of a Dynamic Host Configuration Protocol (DHCP) client
- ip dhcp option** - Sets the DHCP server options

## 16.3.24 show ip dhcp server statistics

This command displays the DHCP server statistics.

**show ip dhcp server statistics**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip dhcp server statistics
```

```
Address pools : 2
```

```
Message Received
```

```
-----
```

```
DHCPDISCOVER 6
```

```
DHCPREQUEST 2
```

```
DHCPDECLINE 0
```

```
DHCPRELEASE 0
```

```
DHCPINFORM 0
```

```
Message Sent
```

```
-----
```

```
DHCPOFFER 6
```

```
DHCPACK 2
```

```
DHCPNAK 0
```

### Related Commands

**service dhcp-server** - Enables the DHCP server

**ip dhcp pool** - Creates a DHCP server address pool and places the user in the DHCP pool configuration mode

**ip dhcp** - Sets the DHCP server parameters such as enabling ICMP echo mechanism or offer-reuse

timeout

**show ip dhcp server pools** - Displays the DHCP server pools

## 17 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 Mode ) and VACM (View based Access Control Model) are the main features added as part of the SNMPv3 specification. USM provides for 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 Modes, Access Control Models, etc. 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 **SMIS 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. **SMIS SNMP** is provided as source code available for licensing to OEMs and VARs who wish to incorporate the multilingual SNMP functionality into their products.

The list of CLI commands for the configuration of SNMPv3 is as follows:

[snmp community index](#)

[snmp group](#)

[snmp access](#)

[snmp engineid](#)

[snmp view](#)

[snmp targetaddr](#)

[snmp targetparams](#)

[snmp user](#)

[snmp notify](#)

[snmp-server enable traps snmp authentication](#)

[snmp-server trap udp-port](#)

[enable snmpagent](#)

[disable snmpagent](#)

[enable snmpsubagent](#)

[disable snmpsubagent](#)

[show snmp agentx information](#)

[show snmp agentx statistics](#)

[show snmp](#)

[show snmp community](#)

[show snmp group](#)

[show snmp group access](#)

[show snmp engineID](#)

[show snmp viewtree](#)

[show snmp targetaddr](#)

[show snmp targetparam](#)

[show snmp user](#)

[show snmp notif](#)

[show snmp inform statistics](#)

[show snmp-server traps](#)

## 17.1 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 <ContextName | none>] [{volatile |
nonvolatile}] [transporttag <TransportTagIdentifier | none>]
```

```
no snmp community index <CommunityIndex>
```

### Syntax Description

**CommunityIndex** - Community index identifier

**Name** - Community name

**Security** - User Name

**Context** - Context name through which the management information is accessed when using the community string specified by the corresponding instance of SNMP community name

**volatile | nonvolatile** - Storage type

**transporttag** - Transport tag identifier

### Mode

Global Configuration Mode

### Defaults

Community Index - NETMAN/PUBLIC

CommunityName - NETMAN/PUBLIC

Security Name - None

ContextName - Null

Transport Tag - Null

Storage type - Volatile

### Example:

```
SMIS(config)# snmp community index myv3com name myv3com security
xyz context myinst nonvolatile transporttag myv3tag
```

➔ The community index identifier must be unique for every community name entry.

## Related Commands

**show snmp** - Displays the status information of SNMP communications

**show snmp community** - Displays the configured SNMP community details



## 17.2 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-mode {v1 | v2c | v3 }  
[ {volatile | nonvolatile} ]
```

```
no snmp group <GroupName> user <UserName> security-mode {v1 | v2c | v3 }  
}
```

### Syntax Description

**GroupName** - Name of the SNMP group

**User** - User Name

**security-mode** - Security Model

**volatile | nonvolatile** - Storage Type

### Mode

Global Configuration Mode

### Defaults

Group Name - iso/initial

### Example:

```
SMIS(config)# snmp group myv3group user myv3user securitymode v1  
volatile
```

### Related Commands

**show snmp group** - Displays the configured SNMP groups

**show snmp user** - Displays the configured SNMP users

## 17.3 snmp access

This command configures the SNMP group access details. 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}]
```

```
no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}
```

**GroupName** - Name of the group

**v1 | v2c | v3** - Version of the SNMP

### Syntax Description

**auth** - Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication

**noauth** - no-authentication

**priv** - Specifies both authentication and privacy

**read** - A read view identifier

**write** - A write view identifier

**notify** - A notification view identifier

**volatile | nonvolatile** - Storage type

### Mode

Global Configuration Mode

### Defaults

Group Name - iso

Read/Write/Notify view - iso

Storage Type - volatile

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:**

```
SMIS(config)# snmp access myv2group v2 read v2readview write  
v2writeview notify v2notifyview nonvolatile
```

- ➡ To configure an SNMP access along with the group, a group must have already been created using the `snmp group` command.
- ➡ Version 3 is the most secure mode as it allows packet encryption with the `priv` key word.

**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

## 17.4 snmp engineid

This command configures the engine identifier. The no form of the command removes the configured engine identifier.

```
snmp engineid <EngineIdentifier>
```

```
no snmp engineid
```

### Syntax Description

**EngineIdentifier** - Engine Id

### Mode

Global Configuration Mode

### Defaults

80.00.08.1c.04.46.53

### Example:

```
SMIS(config)# snmp engineid 80.0.08.1c.04.5f.a9
```

- 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

### Related Commands

**show snmp engineID** - Displays the Engine Identifier

**show snmp user** - Displays the configured SNMP users

## 17.5 snmp view

This command configures the SNMP view. 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 Description

**ViewName** - View Name

**OIDTree** - Object Identifier

**OIDMask** | **none** - Defines views' subtrees

**included** | **excluded** - Type of view

**volatile** | **nonvolatile** - Type of storage

### Mode

Global Configuration Mode

View Name - iso/restricted

OIDTree - 1

OIDMask - None

View type – included

### Defaults

Storage type - non-volatile

### Example:

```
SMIS(config)# snmp view v2readview 1.3.6.1 mask 1.1.1.1 included
nonvolatile
```

- ▶ 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.

### 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

## 17.6 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 <TimeoutValue(1-1500)>] [retries <RetryCount(1-
3)>] [taglist <TagIdentifier | none>] [{volatile | nonvolatile}]
```

```
no snmp targetaddr <TargetAddressName>
```

### Syntax Description

**TargetAddressName** - Name of the Target address (host)

**Param** - SNMP parameter Name

**IPAddress/ IP6Address** - IP/IP6 Address of the host

**Timeout** - The time the SNMP agent waits for a response from the SNMP Manager before retransmitting the Inform Request Message

**retries** - The Maximum number of times the agent can retransmit the Inform Request Message

**taglist** - Tag Identifier

**volatile | nonvolatile** - Storage type

### Mode

Global Configuration Mode

### Defaults

ParamName - Internet

IPAddress - 10.0.0.10

Taglist - snmp

Storage type - volatile

### Example:

```
SMIS(config)# snmp targetaddr issmgr param issd 10.0.0.10 taglist
mytag nonvolatile
```

Target param must have been configured.

## Related Commands

**show snmp targetaddr** - Displays the configured SNMP target Addresses

**snmp targetparams** - Configures the SNMP target parameters

**show snmp targetparam** - Displays the configured SNMP Target Address Params



## 17.7 snmp targetparams

This command configures the SNMP target parameters. The no form of the command removes the SNMP target Params

```
snmp targetparams <ParamName> user <UserName> security-mode {v1 | v2c
| v3 {auth | noauth | priv}} message-processing {v1 | v2c | v3}
[{{volatile | nonvolatile}}
```

```
no snmp targetparams <ParamName>
```

### Syntax Description

**ParamName** - SNMP Parameter Name

**User** - User Name

**security-mode** - Security Mode

**auth** - Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication

**noauth** - no-authentication

**priv** - Specifies both authentication and privacy

**messageprocessing** - Message processing mode

**volatile | nonvolatile** - Storage type

### Mode

Global Configuration Mode

### Defaults

ParamName - internet

User/Security Name - None

Security Mode - v2c

Security Level - NoauthNoPriv

Message Processing Mode - v2c

Storage Type - Non-volatile

ParamName - test1

User/Security Name - None

Security Mode - v1

Security Level - NoauthNoPriv

Message Processing Mode - v1

Storage Type - Non-volatile

**Example:**

```
SMIS(config)# snmp targetparams param1 user user1 securitymode 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

**show snmp targetparam** - Displays the configured SNMP Target Address Params

**show snmp user** - Displays the configured SNMP users.

## 17.8 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]]
```

```
no snmp user <UserName>
```

### Syntax Description

**UserName** - Name of the User

**Auth** - Authentication Algorithm - can be Message Digest 5 or Secure Hash Algorithm

**Passwd** - Password associated with the Authentication type

**priv DES** - Private encryption password

**volatile | nonvolatile** - Storage type - can be either volatile or non-volatile

### Mode

Global Configuration Mode

### Defaults

UserName - Initial

Authentication Protocol - None

Privacy Protocol - None

Storage type - Non-volatile

Storage type - Non-volatile

### Example:

```
SMIS(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

## 17.9 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 Description

**NotifyName** - Notification Name

**tag** - Tag Name

**type** - Type of Notification

**volatile | nonvolatile** - Storage type of the notification details

### Mode

Global Configuration Mode

### Defaults

Notify Name - iss/iss1

Notify Tag - iss/iss1

Storage type - volatile

### Example:

```
SMIS(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

## 17.10 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

### Defaults

Generation of authentication traps is disabled by default.

### Example:

```
SMIS(config)# snmp-server enable traps snmp authentication
```

## 17.11 snmp-server trap udp-port

This command configures UDP port number to be used to send SNMP traps.

The “no” form of this command resets the UDP port number to the default value 162.

```
snmp-server trap udp-port <port>
```

```
no snmp-server trap udp-port
```

### Mode

Global Configuration Mode

### Defaults

UDP port 162

### Example:

```
SMIS(config)# snmp-server trap udp-port 165
```

### Related Commands

**show snmp-server traps** - Displays the SNMP server trap configuration details

## 17.12 enable snmpagent

This command enables the SNMP agent on the switch.  
SNMP agent feature is enabled by default.

**enable snmpagent**

### Mode

Global Configuration Mode

### Defaults

Enabled

### Example:

```
SMIS(config)# enable snmpagent
```

### Related Commands

**show snmp** - Displays the SNMP details

- ▶ If SNMP sub agent feature is enabled, disable the sub agent first before enabling the SNMP agent feature.

## 17.13 disable snmpagent

This command disables the SNMP agent on the switch.  
SNMP agent feature is enabled by default.

**disable snmpagent**

### **Mode**

Global Configuration Mode

### **Defaults**

SNMP feature is enabled.

### **Example:**

```
SMIS(config)# disable snmpagent
```

### **Related Commands**

**show snmp** - Displays the SNMP details



## 17.14 enable snmpsubagent

This command enables the SNMP sub agent on the switch.

The Switch can either operate as a SNMP agent or sub agent. Hence, to enable an SNMP sub agent the SNMP agent feature needs to be disabled. Use the command “disable snmpagent” to disable the SNMP agent feature before enabling the SNMP sub agent feature.

The SNMP sub agent feature is disabled by default.

```
enable snmpsubagent { master { ip4 <ipv4_address> | ip6 <ipv6_address>
} [port <number>] }
```

### Syntax Description

**ipv4\_address** – IP address of the master agent

**ip6\_address** – Ipv6 address of the master agent

**<number>** - TCP port number to be used to reach master agent

### Mode

Global Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config)# enable snmpsubagent
```

### Related Commands

**show snmp agentx information** - Displays the SNMP sub agent details

- ➡ Disable SNMP agent feature before enabling the SNMP sub agent feature.

## 17.15 disable snmpsubagent

This command disables the SNMP sub agent on the switch.

SNMP sub agent feature is disabled by default.

**disable snmpsubagent**

### **Mode**

Global Configuration Mode

### **Defaults**

SNMP sub agent feature is disabled.

### **Example:**

```
SMIS(config)# disable snmpsubagent
```

### **Related Commands**

**show snmp agentx information** - Displays the SNMP sub agent details

## 17.16 show snmp agentx information

This command displays the information about SNMP sub agent configuraiton.

```
show snmp agentx information
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show snmp agentx information
Agentx Subagent is enabled
TransportDomain :TCP
Master IP Address :192.168.5.89
Master PortNo :705
SMIS#
```

## 17.17 show snmp agentx statistics

This command displays the SNMP sub agent related counters.

**show snmp agentx statistics**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show snmp agentx statistics
```

#### Tx Statistics

Transmitted Packets	:1
Open PDU	:1
Index Allocate PDU	:0
Index DeAllocate PDU	:0
Register PDU	:0
Add Agent Capabilities PDU	:0
Notify PDU	:0
Ping PDU	:0
Remove Agent Capabilities PDU	:0
UnRegister PDU	:0
Close PDU	:0
Response PDU	:0

#### Rx Statistics

Rx Packets	:0
Get PDU	:0
GetNext PDU	:0
GetBulk PDU	:0
TestSet PDU	:0
Commit PDU	:0
Cleanup PDU	:0
Undo PDU	:0
Dropped Packets	:0
Parse Drop Errors	:0
Open Fail Errors	:0
Close PDU	:0

Response PDU

:0

## 17.18 show snmp

This command displays the status information of SNMP communications.

**show snmp**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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

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
```

## 17.19 show snmp community

This command displays the configured SNMP community details.

**show snmp community**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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

## 17.20 show snmp group

This command displays the configured SNMP groups.

**show snmp group**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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  : Non-volatile
Row Status    : Active
-----
Security Model : v3
Security Name  : templateMD5
Group Name    : initial
Storage Type  : Non-volatile
Row Status    : Active
-----
Security Model : v3
Security Name  : templateSHA
```



Group Name : initial  
Storage Type : Non-volatile  
Row Status : Active

---

## Related Commands

**snmp group** - Configures the SNMP group details

**snmp user** - Configures the SNMP user details

## 17.21 show snmp group access

This command displays the configured SNMP group access details.

**show snmp group access**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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 : Non-volatile
Row Status   : Active
```

-----

```
Group Name   : initial
Read View    : iso
Write View   : iso
Notify View  : iso
Storage Type : Non-volatile
```

Row Status : Active

-----

Group Name : initial

Read View : iso

Write View : iso

Notify View : iso

Storage Type : Non-volatile

Row Status : Active

-----

## Related Commands

**snmp access** - Configures the SNMP group access details

**snmp view** - Configures the SNMP view

## 17.22 show snmp engineID

This command displays the Engine Identifier.

**show snmp engineID**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show snmp engineID
```

```
EngineId: 80.00.08.1c.04.46.53
```

### Related Command

**snmp engineid** - Configures the engine identifier

## 17.23 show snmp viewtree

This command displays the configured SNMP Tree views.

**show snmp viewtree**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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 view** - Configures the SNMP view

## 17.24 show snmp targetaddr

This command displays the configured SNMP target Addresses.

```
show snmp targetaddr
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show snmp targetaddr
Target Address Name: issmanager
IP Address: 10.0.0.10
Tag List: snmp
Parameters: internet
Storage Type: 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

## 17.25 show snmp targetparam

This command displays the configured SNMP Target Address Params.

**show snmp targetparam**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show snmp targetparam
```

```
Target Parameter Name      : internet
Message Processing Model   : v2c
Security Model             : v2c
Security Name              : none
Security Level             : No Authentitcation, No Privacy
Storage Type               : Volatile
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               : Volatile
Row Status                  : Active
```

### Related Commands

**snmp targetparams** - Configures the SNMP target parameters

**snmp user** - Configures the SNMP user details

## 17.26 show snmp user

This command displays the configured SNMP users.

**show snmp user**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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 user** - Configures the SNMP user details

**show snmp community** - Displays the configured SNMP community details



## 17.27 show snmp notif

This command displays the configured SNMP Notification types.

```
show snmp notif
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# 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

## 17.28 show snmp inform statistics

This command displays the inform message statistics.

```
show snmp inform statistics
```

### **Mode**

Privileged EXEC Mode

### **Example:**

```
SMIS# 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.
```

## 17.29 show snmp-server traps

This command displays the SNMP trap information.

**show snmp-server traps**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show snmp-server traps
```

```
SNMP Trap Listen Port is 162
```

```
Currently enabled traps:
```

```
-----
```

```
linkup,linkdown,
```

```
Login Authentication Traps DISABLED.
```

## 17.30 debug ip snmp

This command enables the display of SNMP module debug messages on the console.

The no form of this command disables the SNMP debug messages display.

```
debug ip snmp
```

```
no debug ip snmp
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# debug ip snmp
```

## 18 IP

IP (Internet Protocol) is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. Example:: 10.5.25.180.

Every computer that communicates over the Internet is assigned an IP address that uniquely identifies the device and distinguishes it from other computers on the Internet. Within an isolated network, IP addresses can be assigned at random as long as each one is unique. However, to connect a private network to the Internet, the registered IP addresses must be used (called Internet addresses) to avoid duplicates. The four numbers in an IP address are used in different ways to identify a particular network and a host on that network.

Four regional Internet registries -- ARIN, RIPE NCC, LACNIC and APNIC -- assign Internet addresses from the following three classes.

Class A - supports 16 million hosts on each of 126 networks

Class B - supports 65,000 hosts on each of 16,000 networks

Class C - supports 254 hosts on each of 2 million networks

The number of unassigned Internet addresses is running out, so a new classless scheme called CIDR (Classless Inter-Domain Routing) is gradually replacing the system based on classes A, B, and C and is tied to adoption of IPv6.

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

ping

ip route

ip routing

ip default-ttl

arp timeout

arp – ip address

ip arp max-retries

show ip traffic

show ip route

show ip arp

## 18.1 show ip information

This command displays IP configuration information.

**show ip information**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip information
Global IP Configuration:
-----
IP routing is enabled
Default TTL is 64
IGMP is globally disabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP echo replies are always sent
ICMP mask replies are always sent
Number of aggregate routes is 10
Number of multi-paths is 2
Load sharing is disabled
Path MTU discovery is disabled
```

### 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

**ip aggregate-route** – Sets the maximum number of aggregate routes

**ip path mtu discover** – Enables path mtu discovery

**traffic-share** - Enables traffic sharing

## 18.2 ping

This command sends echo messages.

```
ping [ip] destination-address [size packet_size (0-2080)] [count  
packet_count (1-10)] [timeout time_out (1-100)]
```

### Syntax Description

**ip** - IP address of the node to be pinged

**size packet\_size** - Size of the data portion of the PING PDU

**count packet\_count** - Number of times the given node address is to be pinged

**timeout** - Time in seconds after which the entity waiting for the ping response times out

### Mode

User EXEC Mode

### Defaults

size packet\_size - 500

count packet\_count - 3

timeout time\_out - 5

### Example:

```
SMIS# ping 10.0.0.2  
Reply Received From :10.0.0.2, TimeTaken : 20 msec  
Reply Received From :10.0.0.2, TimeTaken : 10 msec  
Reply Received From :10.0.0.2, TimeTaken : 10 msec  
--- 10.0.0.2 Ping Statistics ---  
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
```

## 18.3 ip route

This command adds a static route and the no form of the command deletes a static route.

```
ip route <prefix> <mask> {<next-hop> | Vlan <vlan-id (1-4069)> |  
<interface-type> <interface-id> | null0 } [<distance (1-255)>] [  
private ]
```

```
no ip route <prefix> <mask> { <next-hop> | Vlan <vlan-id(1-4069)> |  
<interface-type> <interface-id> | null0 } [private]
```

### Syntax Description

**prefix** - IP route prefix for the destination. (Destination IP address)

**mask** - Subnet mask for the destination

**next-hop** - IP address or IP alias of the next hop that can be used to reach that network

**Vlan** - VLAN ID

**interface-type** - Interface type, can either be a gi, ex or qx ethernet interfaces

**interface-id** - Physical interface ID including slot and port number

**null0** - Null0 routes make the switch drop all the packets matching this route entry

**distance** - Administrative distance

**private** - Private routes are not distributed to other routers through routing protocols

### Mode

Global Configuration Mode

### Defaults

distance - 1

### Example:

```
SMIS(config)# ip route 30.0.0.2 255.255.255.255 Vlan 1
```

When the next-hop object is unknown or not relevant its value must be set to zero.

Physical Interface must be a router port.

### Related Commands

**show ip route** - Displays the IP routing table

**no switchport** - Configures the port as a router port





## 18.4 ip routing

This command enables IP routing and the no form of the command disables IP routing.

`ip routing`

`no ip routing`

### Mode

Global Configuration Mode

### Defaults

Enabled

### Example:

```
SMIS(config)# ip routing
```

A static route is appropriate when **SMIS** cannot dynamically build a route to the destination.

### Related Commands

`show ip information` – Displays IP configuration information

`show ip route` – Displays the IP routing table

## 18.5

## 18.6 ip default-ttl

This command sets the Time-To-Live (TTL) value and the no form of the command sets the TTL to the default value.

```
ip default-ttl <value (1-255)>
```

```
no ip default-ttl
```

### Mode

Global Configuration Mode

### Defaults

64 seconds

### Example:

```
SMIS(config)# ip default-ttl 1
```

- ▶ Time-to-live (TTL) is a value in an Internet Protocol (IP) packet that tells a network router whether or not the packet has been in the network too long and must be discarded
- ▶ The default Windows 95/98 TTL value is 32 seconds.

### Related Command

`show ip information` – Displays IP configuration information

## 18.7 arp timeout

This command sets the ARP (Address Resolution Protocol) cache timeout and the no form of the command sets the ARP cache timeout to its default value.

```
arp timeout <seconds (30-86400)>
```

```
no arp timeout
```

### Mode

Global Configuration Mode

### Defaults

7200

### Example:

```
SMIS(config)# arp timeout 35
```

### Related Command

**show ip arp** – Displays IP ARP table for the given VLAN ID/IP Address of ARP entry/MAC Address of ARP entry/IP ARP summary table/ARP configuration information

## 18.8 arp – ip address

This command adds a static entry in the ARP cache and the “no” form of the command deletes a static entry from the ARP cache.

```
arp <ip address> <hardware address> {Vlan <vlan-id(1-4069)> |
<interface-type> <interface-id>}
```

```
no arp <ip address>
```

### Syntax Description

**ip address** - IP address or IP alias to map to the specified MAC address

**hardware address** - MAC address to map to the specified IP address or IP alias

**Vlan** - VLAN ID

**interface-type** – Physical interface type like gi,ex which are configured as routed port using “no switchport” command.

**Interface-id** – Physical interface port number like 0/1 which are configured as routed port using “no switchport” command.

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# arp 10.203.120.21 00:11:22:33:44:55 Vlan 1
```

The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The term address resolution refers to the process of finding an address of a computer in a network. Interface must be a router port.

### Related Commands

**show ip arp** – Displays IP ARP table for the given VLAN ID/IP Address of ARP entry/MAC Address of

ARP entry/IP ARP summary table/ARP configuration information

**no switchport** - Configures the port as a router port

## 18.9 ip arp max-retries

This command sets the maximum number of ARP request retries. The “no” form of the command sets the maximum number of ARP request retries to its default value.

```
ip arp max-retries <value (2-10)>
```

```
no ip arp max-retries
```

### Mode

Global Configuration Mode

### Defaults

3

### Example:

```
SMIS(config)# ip arp max-retries 2
```

The command configures the maximum number of ARP requests that the switch will generate before deleting an un-resolved ARP entry.

### Related Command

**show ip arp** – Displays IP ARP table for the given VLAN ID/IP Address of ARP entry/MAC Address of ARP entry/IP ARP summary table/ARP configuration information

## 18.10 show ip traffic

This command displays the IP protocol statistics.

**show ip traffic**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip traffic
```

```
IP Statistics:
```

```
-----
```

```
Rcvd: 0 total, 0 header error discards
```

```
0 bad ip address discards, 0 unsupported protocol  
discards
```

```
Frag: 0 reassembled, 30 timeouts, 0 needs reassembly
```

```
0 fragmented, 0 couldn't fragment
```

```
Bcast: Sent: 0 forwarded, 0 generated requests
```

```
Drop:
```

```
ICMP Statistics:
```

```
-----
```

```
Rcvd: 0 total, 0 checksum errors, 0 unreachable, 0  
redirects
```

```
0 time exceeded, 0 param problems, 0 quench
```

```
0 echo, 0 echo reply, 0 mask requests, 0 mask  
replies,
```

```
0 timestamp , 0 time stamp reply,
```

```
Sent: 0 total, 0 checksum errors, 0 unreachable, 0  
redirects
```

```
0 time exceeded, 0 param problems, 0 quench
```

```
0 echo, 0 echo reply, 0 mask requests, 0 mask  
replies,
```

```
0 timestamp , 0 time stamp reply,
```

## 18.11 show ip route

This command displays the IP routing table.

```
show ip route [ { <ip-address> [<mask>] | bgp | connected | ospf | rip
| static | summary } ]
```

### Syntax Description

**ip-address** - Destination IP Address  
**mask** - Prefix Mask for the destination  
**bgp** - Border Gateway Protocol  
**connected** - Directly Connected Network Routes  
**ospf** - Open Shortest Path First (OSPF)  
**rip** - Routing Information Protocol (RIP)  
**static** - Static Routes  
**summary** - Summary of all routes

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip route
S 20.0.0.0/8 [1] via 100.20.6.20
S 30.0.0.0/8 [4] via 120.20.6.20
S 40.0.0.0/8 is directly connected, vlan1
S 50.0.0.0/8 [1] via 100.20.6.21
C 100.0.0.0/8 is directly connected, vlan1
C 110.0.0.0/8 is directly connected, vlan2
C 120.0.0.0/8 is directly connected, vlan3
```

```
SMIS# show ip route 20.0.0.0
Codes: C - connected, S - static, R - RIP, B - BGP, O - OSPF
S 20.0.0.0/8 [1] via 100.20.6.20
```

```
SMIS# show ip route 30.0.0.0 255.0.0.0
Codes: C - connected, S - static, R - RIP, B - BGP, O - OSPF
S 30.0.0.0/8 [4] via 120.20.6.20
```



**Related Commands**

**ip route** – Adds a static route

**ip routing** – Enables IP routing

## 18.12 show ip arp

This command displays IP ARP table.

```
show ip arp [ { Vlan <vlan-id(1-4069)> | <ip-address> | <mac-address> |
summary | information }]
```

### Syntax Description

**Vlan** - VLAN ID

**ip-address** - IP Address of ARP Entry

**mac-address** - MAC Address of ARP Entry

**summary** - IP ARP Table summary

**information** - ARP Configuration information

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip arp
```

```
Address Hardware Address Type Interface Mapping
-----
110.20.6.99 00:11:22:44:55:66 ARPA vlan1 Static
100.20.6.99 00:11:22:33:44:55 ARPA vlan2 Static
110.20.6.101 00:5e:01:00:11:55 ARPA vlan2 Static
```

```
SMIS# show ip arp vlan 1
```

```
Address Hardware Address Type Interface Mapping
-----
110.20.6.99 00:11:22:44:55:66 ARPA vlan1 Static
```

```
SMIS# show ip arp 00:10:b5:66:a7:0e
```

```
Address Hardware Address Type Interface Mapping
-----
100.20.6.20 00:10:b5:66:a7:0e ARPA vlan1 Dynamic
```

```
SMIS# show ip arp 100.20.6.99
```

```
Address Hardware Address Type Interface Mapping
-----
```

```
100.20.6.99 00:11:22:33:44:55 ARPA vlan2 Static
```

```
SMIS# show ip arp summary
```

```
3 IP ARP entries, with 0 of them incomplete
```

```
SMIS# show ip arp information
```

```
ARP Configurations:
```

```
-----
```

```
Maximum number of ARP request retries is 10
```

```
ARP cache timeout is 7200 seconds
```

### Related Commands

**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

## 19 IGMP

**SMIS IGMP** (Internet Group Management Protocol) is a portable implementation of the Internet Group Management Protocol Version 3. It implements the IGMP router functionalities required by the Multicast Routing Protocol.

**SMIS IGMP conforms with RFC 3376 for IGMP v3 router functionality.** **SMIS IGMP** supports the MIB defined in draft-ietf-magma-rfc2933-update-00.txt.

The deployment of the **SMIS IGMP** router can be within a routing domain that uses any Multicast Routing Protocol. **SMIS IGMP** informs MRPs about group membership messages and leave messages.

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

[set ip igmp](#)

[set ip igmp](#)

[ip igmp immediate-leave](#)

[ip igmp version](#)

[ip igmp query-interval](#)

[ip igmp query-max-response-time](#)

[ip igmp robustness](#)

[ip igmp last-member-query-interval](#)

[ip igmp static-group](#)

[no ip igmp](#)

[debug ip igmp](#)

[show ip igmp global-config](#)

[show ip igmp interface](#)

[show ip igmp groups](#)

[show ip igmp sources](#)

[show ip igmp statistics](#)

## 19.1 set ip igmp

This command enables or disables IGMP.

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

### Syntax Description

**enable** - Enables IGMP

**disable** - Disables IGMP

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config)# set ip igmp enable
```

### Related Commands

**show ip igmp global-config** - Displays the global configuration of IGMP

## 19.2 set ip igmp

This command enables or disables IGMP on the interface.

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

### Syntax Description

**enable** - Enables IGMP

**disable** - Disables IGMP

### Mode

Interface Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config-if)# set ip igmp enable
```

### Related Commands

**show ip igmp interface** - Displays the interface configuration of IGMP

## 19.3 ip igmp immediate-leave

This command enables immediate leave processing on the interface and the “no” form of the command disables immediate-leave processing.

```
ip igmp immediate-leave
```

```
no ip igmp immediate-leave
```

### Mode

Interface Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config-if)# ip igmp immediate-leave
```

### Related Commands

**show ip igmp interface** - Displays the interface configuration of IGMP

## 19.4 ip igmp version

This command sets the IGMP version on the interface and the “no” form of the command sets the default IGMP version on the interface.

```
ip igmp version { 1 | 2 | 3 }
```

```
no ip igmp version
```

### Syntax Description

1 | 2 | 3 - IGMP versions

### Mode

Interface Configuration Mode

### Defaults

2

### Example:

```
SMIS(config-if)# ip igmp version 1
```

### Related Commands

**show ip igmp interface** - Displays the interface configuration of IGMP



## 19.5 ip igmp query-interval

This command sets the IGMP query interval for the interface and the “no” form of the command sets the query interval to the default value.

```
ip igmp query-interval <value (1-65535) seconds>
```

```
no ip igmp query-interval
```

### Mode

Interface Configuration Mode

### Defaults

125

### Example:

```
SMIS(config-if)# ip igmp query-interval 30
```

### Related Commands

**show ip igmp interface** - Displays the interface configuration of IGMP

## 19.6 ip igmp query-max-response-time

This command sets the IGMP max query response value for the interface and the “no” form of the command sets the max query response to the default value.

```
ip igmp query-max-response-time <value (1-255) seconds>
```

```
no ip igmp query-max-response-time
```

### Mode

Interface Configuration Mode

### Defaults

100

### Example:

```
SMIS(config-if)# ip igmp query-max-response-time 20
```

### Related Commands

**show ip igmp interface** - Displays the interface configuration of IGMP

## 19.7 ip igmp robustness

This command sets the IGMP robustness value for the interface and the “no” form of the command sets the robustness value to default value.

```
ip igmp robustness <value(1-255)>
```

```
no ip igmp robustness
```

### Mode

Interface Configuration Mode

### Defaults

2

### Example:

```
SMIS(config-if)# ip igmp robustness 100
```

### Related Commands

**show ip igmp interface** - Displays the interface configuration of IGMP

## 19.8 ip igmp last-member-query-interval

This command sets the IGMP last member query interval for the interface and the “no” form of the command sets the last member query interval to the default value.

```
ip igmp last-member-query-interval <value (1-255)>
```

```
no ip igmp last-member-query-interval
```

### Mode

Interface Configuration Mode

### Defaults

10

### Example:

```
SMIS(config-if)# ip igmp last-member-query-interval 100
```

The `igmp version` on this interface must be set to 2.

### Related Commands

`show ip igmp interface` - Displays the interface configuration of IGMP

## 19.9 ip igmp static-group

This command adds the static group membership on the interface and the “no” form of the command deletes the static group membership on the interface.

```
ip igmp static-group <Group Address> [source <Source Address>]
```

```
no ip igmp static-group <Group Address> [source <Source Address>]
```

### Syntax Description

**Group Address** - Group IP address

**source** - Source IP address

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ip igmp static-group 224.1.2.3 source 12.0.0.1
```

The **igmp version** on this interface must be set to 3 for configuring static group along with source information.

### Related Commands

**show ip igmp groups** - Displays the IGMP groups information

**show ip igmp sources** - Displays the IGMP sources information

**show ip igmp interface** - Displays the interface configuration of IGMP

## 19.10 no ip igmp interface

This command deletes the IGMP capable interface.

```
no ip igmp interface
```

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# no ip igmp interface
```

### Related Commands

**show ip igmp interface** - Displays the interface configuration of IGMP

## 19.11 debug ip igmp

This command enables the IGMP trace and the “no” form of the command disables the IGMP trace.

```
debug ip igmp { [i/o][grp][qry][tmr][mgmt] | [all] }
```

```
no debug ip igmp { [i/o][grp][qry][tmr][mgmt] | [all] }
```

### Syntax Description

**i/o** - Input/Output messages

**grp** - Group Related messages

**qry** - Query Related messages

**tmr** - Timer Related messages

**mgmt** - Management Configuration messages

**all** - All Traces

### Mode

Privileged EXEC Mode

### Defaults

Debugging is disabled by default.

### Example:

```
SMIS# debug ip igmp all
```

## 19.12 show ip igmp global-config

This command displays the global configuration of IGMP.

```
show ip igmp global-config
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip igmp global-config  
IGMP is globally enabled
```

### Related Commands

**set ip igmp** - Enables or disables IGMP

**ip igmp proxy-service** - Enables IGMP Proxy service in the system



## 19.13 show ip igmp interface

This command displays the interface configuration of IGMP.

```
show ip igmp interface [Vlan <vlan-id> | <iftype> <ifnum>]
```

### Syntax Description

**Vlan** - VLAN ID

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip igmp interface
vlan1, line protocol is up
Internet Address is 10.0.0.1/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 10 seconds
IGMP querying router is 10.0.0.1 (this system)
Fast leave is disabled on this interface
No multicast groups joined
vlan2, line protocol is up
Internet Address is 20.0.0.1/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 10 seconds
IGMP querying router is 20.0.0.1 (this system)
Fast leave is disabled on this interface
No multicast groups joined
```

### Related Commands

**set ip igmp** - Enables or disables IGMP on the interface

**ip igmp immediate-leave** - Enables immediate leave processing on the interface

**ip igmp version** - Sets the IGMP version on the interface

**ip igmp query-interval** - Sets the IGMP query interval for the interface

**ip igmp query-max-response-time** - Sets the IGMP max query response value for the interface

**ip igmp robustness** - Sets the IGMP robustness value for the interface

**ip igmp last-member-query-interval** - Sets the IGMP last member query interval for the interface

**no ip igmp** - Deletes the IGMP capable interface

## 19.14 show ip igmp groups

This command displays the IGMP groups information.

```
show ip igmp groups
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip igmp groups
```

```
I - Include Mode
```

```
E - Exclude Mode
```

```
S - Static Mbr, D - Dynamic Mbr
```

```
GroupAddress Flg Iface UpTime ExpiryTime LastReporter
```

```
-----
```

```
224.5.5.5 S vlan2 [0d 00:00:22.28] [0d 00:00:00.00] 20.0.0.1
```

```
226.7.7.7 IS vlan3 [0d 00:00:04.59] [0d 00:00:00.00] 30.0.0.1
```

### Related Commands

**ip igmp static-group** - Adds the static group membership on the interface

## 19.15 show ip igmp sources

This command displays the IGMP source information.

```
show ip igmp sources
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip igmp sources
```

```
I - Include Mode
```

```
E - Exclude Mode
```

```
S - Static Mbr, D - Dynamic Mbr
```

```
F - Forward List, N - Non-Forward List
```

```
GroupAddress Iface SrcAddress Flg ExpiryTime LastReporter
```

```
-----  
226.7.7.7 vlan3 12.0.0.1 ISF [0d 00:00:00.00] 30.0.0.1
```

### Related Commands

**ip igmp static-group** - Adds the static group membership on the interface

## 19.16 show ip igmp statistics

This command displays the IGMP statistics information.

```
show ip igmp statistics [Vlan <vlan-id> | <iftype> <ifnum>]
```

### Syntax Description

**Vlan** - VLAN ID

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip igmp statistics
IGMP Statistics for vlan1
Number of General queries received 1
Number of Group Specific queries received 0
Number of Group and Source Specific queries received 0
Number of v1/v2 reports received 0
Number of v3 reports received 8
Number of v2 leaves received 0
Number of General queries transmitted 1
Number of Group Specific queries transmitted 1
Number of Group and Source Specific queries transmitted 2
Number of v1/v2 reports transmitted 0
Number of v3 reports transmitted 0
Number of v2 leaves transmitted 0
IGMP Statistics for vlan3
Number of General queries received 0
Number of Group Specific queries received 0
Number of Group and Source Specific queries received 0
Number of v1/v2 reports received 0
Number of v3 reports received 6
Number of v2 leaves received 0
Number of General queries transmitted 1
```

Number of Group Specific queries transmitted 0  
Number of Group and Source Specific queries transmitted 0  
Number of v1/v2 reports transmitted 0  
Number of v3 reports transmitted 0  
Number of v2 leaves transmitted 0

## 20 RRD

RRD (Route Redistribution) allows different routing protocols to exchange routing information. Using a routing protocol to advertise routes that are learnt by other means, such as another routing protocol, static routes, or directly connected routes, is called redistribution. While running a single routing protocol throughout an entire IP internetwork is desirable, multi-protocol routing is widespread for a number of reasons, for example, company mergers, multiple departments managed by multiple network administrators, and multi-vendor environments. If a single routing protocol cannot be used, route redistribution is the only solution. Running different routing protocols is often part of a network design. In any case, having a multiple protocol environment makes redistribution a necessity.

Each routing protocol on a network is separated into an autonomous system (AS). All routers in the same autonomous system (running the same routing protocol) have complete knowledge of the entire AS. A router that connects two (or more) autonomous systems is known as a border router. A border router advertises routing information from one AS to the other AS(s). It is only possible to redistribute routing information for like routed protocols. Different routing protocols have different, and often incompatible algorithms and metrics.

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

[as-num](#)

[router-id](#)

[export ospf](#)

[redistribute-policy](#)

[default redistribute-policy](#)

[show ip protocols](#)

[show redistribute-policy](#)

[show redistribute information](#)

## 20.1 as-num

This command sets the AS (Autonomous System) number for the router.

**as-num** <value (1-65535)>

### Mode

Global Configuration Mode

### Defaults

0

### Example:

```
iss (config)# as-num 5
```

The RRD Module must be enabled before any routing protocol module is configured.

### Related Command

**show redistribute information** – Displays RTM RRD status for registered protocols



## 20.2 router-id

This command sets the router ID's address for the router.

**router-id** <addr>

### Mode

Global Configuration Mode

### Example:

```
iss (config)# router-id 12.0.0.1
```

The router-id must be one of the IP addresses of the IP interfaces configured in the switch.

### Related Command

**show redistribute information** – Displays RTM RRD status for registered protocols

## 20.3 export ospf

This command enables redistribution of OSPF (Open Shortest Path First) area / External routes to the protocol and the “no” form of the command disables redistribution of OSPF area / External routes to the protocol.

```
export ospf {area-route|external-route} {rip|bgp}
```

```
no export ospf {area-route|external-route} {rip|bgp}
```

### Syntax Description

**area-route** - OSPF inter-area and intra-area address/mask pairs to be exported into the routing protocol

**external-route** - OSPF Type 1 and Type 2 External address/mask pairs to be exported into the routing protocol

**rip** - Routing Information Protocol

**bgp** - Border Gateway Protocol

### Mode

Global Configuration Mode

### Example:

```
iss (config)# export ospf area-route rip
```

### Related Command

**show ip protocols** – Displays information about the active routing protocol process

## 20.4 redistribute-policy

This command adds the permit/deny Redistribution Policy and the “no” form of the command removes the permit/deny Redistribution Policy

```
redistribute-policy {permit|deny} <DestIp> <DestRange>
{connected|static|rip|ospf|bgp} {rip|bgp|ospf|all}

no redistribute-policy <DestIp> <DestRange>
```

### Syntax Description

**permit** - Sets the default rule for all prefixes to 'permit'

**deny** - Sets the default rule for all prefixes to 'deny'

**DestIp** - Destination IP address

**DestRange** - Destination range

**connected** Connected routes

**static** - Static routes

**rip** - Routing Information Protocol

**ospf** - Open Shortest Path First

**bgp** - Border Gateway Protocol

**all** - All

### Mode

Global Configuration Mode

### Defaults

permit all

### Example:

```
iss (config)# redistribute-policy permit 10.0.0.0 0.0.0.255
connected ospf
```

The addresses learnt within the specified range through the specified routing protocol will be redistributed to other routing protocols, if **permit** is used and will not be redistributed to other routing protocols, if **deny** is used.

### **Related Command**

**show redistribute-policy** – Displays route redistribution filters

## 20.5 default redistribute-policy

This command sets the default behavior of RRD Control Table.

```
default redistribute-policy {permit | deny}
```

### Syntax Description

**permit** - Sets the default rule for all prefixes to 'permit'

**deny** - Sets the default rule for all prefixes to 'deny'

### Mode

Global Configuration Mode

### Example:

```
iss (config)# default redistribute-policy permit
```

### Related Command

**show redistribute-policy** – Displays route redistribution filters

## 20.6 show ip protocols

This command displays information about the active routing protocol process.

**show ip protocols**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip protocols
Routing Protocol is rip
RIP2 security level is Maximum
Redistributing : rip
Output Delay is disabled
Retransmission timeout interval is 5 seconds
Number of retransmission retries is 36
Default metric is 3
Auto-Summarisation of routes is enabled
Routing for Networks :
10.0.0.0
30.2.0.0
Routing Information Sources :
Interface Specific Address Summarisation :
Interface vlan1
Sending updates every 30 seconds
Invalid after 180 seconds
Flushed after 120 seconds
Send version is 1 2, receive version is 1 2
Authentication type is none
Split Horizon with poisoned reverse is enabled
Installs default route received
Originate default route
Interface vlan2
Sending updates every 30 seconds
Invalid after 180 seconds
Flushed after 120 seconds
```

```
Send version is 2, receive version is 2
Authentication type is none
Split Horizon with poisoned reverse is enabled
Restricts default route installation
Restricts default route origination
Routing Protocol is "ospf" Router ID 0.0.0.0
Number of areas in this router is 0 . 0 normal 0 stub 0 nssa
Routing for Networks:
Passive Interface(s):
Routing Information Sources:
Gateway Distance Last Update(secs)
Distance: (default is 121)
Routing Protocol is "bgp 0"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
IGP synchronization is disabled
Neighbor(s):
Address
Routing Information sources:
Gateway Last Update
```

The information displayed by this command is useful in debugging routing operations.

### Related Command

**export ospf** – Enables redistribution of Ospf area/External routes to protocol

## 20.7 show redistribute-policy

This command displays route redistribution filters.

**show redistribute-policy**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show redistribute-policy
Destination Range SrcProto DestProto Flag
-----
0.0.0.0 255.255.255.255 none others Deny
10.0.0.0 255.0.0.0 rip all Allow
```

### Related Commands

**redistribute-policy** – Adds the permit/Deny Redistribution Policy

**default redistribute-policy** – Sets the default behavior of RRD Control Table



## 20.8 show redistribute information

This command displays RTM (Route Table Manager) RRD status for registered protocols.

**show redistribute information**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show redistribute information
Router ID is 0.0.0.0
AS Number is 0
Current State is disabled
ProtoName OspfAreaRoutes OspfExtRoutes
-----
other Disable Disable
local Disable Disable
static Disable Disable
rip Disable Disable
bgp Disable Disable
```

### Related Commands

**as-num** – Sets the AS (Autonomous System) number for the router

**router-id** – Sets the router-id for the router

## 21 DVMRP

DVMRP (Distance Vector Multicast Routing Protocol) is an Internet Routing Protocol that provides an efficient mechanism for connectionless message multicasting to a group of hosts across an internetwork.

Distance Vector Multicast Routing Protocol is an interior gateway protocol (IGP) suitable for use within an autonomous system, but not between different autonomous systems.

DVMRP is based on RIP. DVMRP combines many of the features of RIP with the Truncated Reverse Path Broadcasting (TRPB) algorithm. To allow experiments to traverse networks that do not support multicasting a mechanism called tunneling was developed. DVMRP tunnels multicast transmission within unicast packets that are reassembled into multicast data when they arrive at their destination.

A key difference between DVMRP and RIP is that RIP routes and forwards datagrams to a particular destination. The purpose of DVMRP is to keep track of the return paths to the source of the multicast datagrams.

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

[set ip dvmrp](#)

[ip dvmrp prune-life-time](#)

[set ip dvmrp - interface](#)

[debug ip dvmrp](#)

[show ip dvmrp](#)

## 21.1 set ip dvmrp

This command enables / disables DVMRP in the switch.

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

### Syntax Description

**enable** - Enables DVMRP in the switch

**disable** - Disables DVMRP in the switch

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config)# set ip dvmrp enable
```

If DVMRP is disabled on an interface, the DVMRP parameters return to their default values.

### Related Commands

**set ip dvmrp - interface** – Enables/disables DVMRP on the interface

**show ip dvmrp** – Displays the DVMRP details

## 21.2 ip dvmrp prune-life-time

This command sets the prune life time value. The “no” form of the command sets the prune life time to the default value (50 seconds).

```
ip dvmrp prune-life-time <time(1-7200secs)>
```

```
no ip dvmrp prune-life-time
```

### Mode

Global Configuration Mode

### Defaults

time - 50 seconds

### Example:

```
SMIS(config)# ip dvmrp prune-life-time 100
```

DVMRP must be enabled globally prior to the execution of this command.

### Related Commands

**set ip dvmrp** – Enables / disables DVMRP in the switch

**show ip dvmrp** – Displays the DVMRP details

## 21.3 set ip dvmrp - interface

This command enables/disables DVMRP on the interface.

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

### Syntax Description

**enable** - Enables DVMRP on the interface

**disable** - Disables DVMRP on the interface

### Mode

Interface Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config-if)# set ip dvmrp enable
```

DVMRP must be enabled globally prior to the execution of this command.

### Related Commands

**set ip dvmrp** – Enables / disables DVMRP in the switch

**show ip dvmrp** – Displays the DVMRP details

## 21.4 debug ip dvmrp

This command enables debugging support for DVMRP. The “no” form of the command disables debugging support for DVMRP.

```
debug ip dvmrp { [neighbor] [group] [join-prune] [i/o] [mrt] [mdh] [mgmt] |  
all }
```

```
no debug ip dvmrp { [neighbor] [group] [join-prune] [i/o] [mrt] [mdh] [mgmt]  
| all }
```

### Syntax Description

**neighbor** - Neighbor Discovery messages

**group** - Group Membership messages

**join-prune** - Join or Prune messages

**i/o** - Input/Output messages

**mrt** - Multicast Route table update messages

**mdh** - Multicast Data Handling messages

**mgmt** - Management Configuration messages

**all** - All traces

### Mode

Privileged EXEC Mode

### Defaults

Debugging is disabled by default.

### Example:

```
SMIS# debug ip dvmrp all
```

DVMRP must be enabled in the device prior to the execution of this command.

### Related Commands

**set ip dvmrp** – Enables / disables DVMRP in the switch

**set ip dvmrp - interface** – Enables DVMRP in the interface

**show ip dvmrp** – Displays the DVMRP details



## 21.5 show ip dvmrp

This command displays the DVMRP details.

```
show ip dvmrp { routes [ vlan <vlan-id(1-4069)> ] | mroutes | nexthop |
neighbor | info | prune }
```

### Syntax Description

**routes** - Unicast Routes for VLAN ID

**mroutes** - Multicast Routes

**nexthop** - Nexthop Routes

**neighbor** - DVMRP neighbors

**info** - Information

**prune** - Prune

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip dvmrp routes
```

```
Dvmrp Routing Table
```

```
-----
```

```
2.0.0.0/8[2] uptime [0d 20:49:41.00], expires [0d 00:01:50.00]
```

```
Status: Active
```

```
via 10.0.0.2, vlan1
```

```
10.0.0.0/8[1] uptime [0d 22:20:00.00], expires [0d 00:02:00.00]
```

```
Status: Local/NeverExpire
```

```
via 10.0.0.1, vlan1
```

```
SMIS# show ip dvmrp mroutes
```

```
Dvmrp Forward Information
```

```
-----
```

```
(2.0.0.0, 227.1.1.1)
```

```
Reverse Path Forwarding Neighbor/Interface : 10.0.0.2/(vlan1)
```

```
Interface State of Upstream neighbor : PRUNED Expiry Time :
```

```
6000
```



```
SMIS# show ip dvmrp nexthop
Dvmrp NextHop Information
-----
SrcAddress/Mask : 2.0.0.0/255.0.0.0
NextHopIndex : 160 (vlan1), IfType : Branch, DF: True
Dependent Nbrs :10.0.0.1
```

```
SMIS# show ip dvmrp neighbor
Neighbour Information
-----
Neighbor Interface Up Exp GenId Adjacency
Address Time Time
-----
10.0.0.2 vlan1 [0d 22:31:48.00] 3400 133 ESTABLISHED
```

```
SMIS# show ip dvmrp info
DVMRP is enabled in the switch
Dvmrp Version:0x3 (major) 0xff (minor)
GenerationId: 0, Total Routes: 0, Reachable Routes: 0
Prune Life Time: 50
Interface Information
-----
IfaceName/Id Address Metric AdminStatus
-----
vlan1/160 10.0.0.1 1 DVMRP_ENABLED
```

```
SMIS# show ip dvmrp prune
Prune List :
NbrAddress/PruneTime : 20.0.0.20/28
NbrAddress/PruneTime : 20.0.0.10/38
```

## Related Commands

- set ip dvmrp** – Enables / disables DVMRP in the switch
- ip dvmrp prune-life-time** – Sets the prune life time value
- set ip dvmrp - interface** – Enables DVMRP in the interface
- debug ip dvmrp** – Enables debugging support for DVMRP

## 22 PIM

PIM (Protocol Independent Multicast) is a multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. Multicast IP Routing protocols are used to distribute data to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients. A multicast group identifies a set of recipients that are interested in a particular data stream, and is represented by an IP address from a well-defined range. Data sent to this IP address is forwarded to all members of the multicast group.

PIM is unicast routing protocol independent and can be operated in two modes : dense and sparse. It is designed to provide scalable inter-domain multicast routing across the Internet. PIM provides multicast routing and forwarding capability to the switch. It maintains the integrity of the hardware based multicast forwarding table with respect to the forwarding table existing in the software. It is independent of the underlying unicast routing protocol and uses the information from the Unicast Routing protocol.

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

[set ip pim](#)

[set ip pim threshold](#)

[set ip pim spt-switchperiod](#)

[set ip pim rp-threshold](#)

[set ip pim rp-switchperiod](#)

[set ip pim regstop-ratelimit-period](#)

[set ip pim pmbr](#)

[ip pim component](#)

[set ip pim static-rp](#)

[set mode](#)

[rp-candidate rp-address](#)

[rp-candidate holdtime](#)

[rp-static rp-address](#)

[ip pim query-interval](#)

[ip pim message-interval](#)

[ip pim bsr-candidate](#)

[ip pim componentId](#)

[ip pim hello-holdtime](#)

[ip pim dr-priority](#)

[ip pim override-interval](#)

[ip pim lan-delay](#)

[set ip pim lan-prune-delay](#)

[no ip pim interface](#)

[debug ip pim](#)

[show ip pim interface](#)

[show ip pim neighbor](#)

[show ip pim rp-candidate](#)

[show ip pim rp-set](#)

[show ip pim bsr](#)

[show ip pim rp-static](#)

[show ip pim component](#)

[show ip pim thresholds](#)

[show ip pim mroute](#)

## 22.1 set ip pim

This command enables or disables PIM globally.

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

### Syntax Description

**enable** - Enables PIM

**disable** - Disables PIM

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
iss (config)# set ip pim enable
```

➔ When PIM is enabled globally mode will be sparse.

### Related Command

**show ip pim interface** - Displays the routers PIM interfaces

## 22.2 set ip pim threshold

This command specifies the SPT group or source threshold when exceeded, switching to shortest path tree is initiated. To switch to SPT, the threshold MUST be configured.

```
set ip pim threshold { spt-grp | spt-src } < number of packets (0-2147483647) >
```

### Syntax Description

**spt-grp** - The threshold of data rate for any group when exceeded, source specific counters are initiated for that particular group. It is based on number of bits per second.

**spt-src** - The switching to Shortest Path Tree is initiated, when the threshold of data rate for any source is exceeded. It is based on number of bits per second.

**number of packets** - Number of packets

### Mode

Global Configuration Mode

### Defaults

0

### Example:

```
iss (config)# set ip pim threshold spt-grp 50
```

### Related Command

**show ip pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM

## 22.3 set ip pim spt-switchperiod

This command specifies the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.

```
set ip pim spt-switchperiod <0-2147483647(in secs)>
```

### Mode

Global Configuration Mode

### Defaults

0

### Example:

```
iss (config)# set ip pim spt-switchperiod 60
```

- ▶ The same period is used for monitoring the data rate for both source and group. To switch to SPT, this period must be configured.

The SPT (Shortest Path Tree) is used for multicast transmission of packets with the shortest path from sender to recipients

### Related Command

**show ip pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

## 22.4 set ip pim rp-threshold

This command specifies the threshold at which the RP (Rendezvous Point) initiates switching to source specific shortest path tree.

```
set ip pim rp-threshold <0-2147483647(number of reg packets)>
```

### Mode

Global Configuration Mode

### Defaults

0

### Example:

```
iss (config)# set ip pim rp-threshold 50
```

- ➡ To switch to SPT, this threshold must be configured and this switching is based on the number of registered packets received.

### Related Command

**show ip pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

## 22.5 set ip pim rp-switchperiod

This command specifies the period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.

```
set ip pim rp-switchperiod <0-2147483647(in secs)>
```

### Mode

Global Configuration Mode

### Defaults

0

### Example:

```
iss (config)# set ip pim rp- switchperiod 100
```

- ➡ To switch to SPT, this period must be configured RP-tree is a pattern that multicast packets are sent to a PIM-SM router by unicast and then forwarded to actual recipients from RP

### Related Command

**show ip pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM



## 22.6 set ip pim regstop-ratelimit-period

This command specifies the period over which RP monitors the number of register packets after sending the register stop message.

```
set ip pim regstop-ratelimit-period <0-2147483647 (in secs)>
```

### Mode

Global Configuration Mode

### Defaults

5

### Example:

```
iss (config)# set ip pim regstop-ratelimit-period 100
```

- ➔ Register stop message is used to avoid encapsulation of multicast data packets from the first hop router to the RP.

### Related Command

**show ip pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM

## 22.7 set ip pim pmbr

This command enables or disables the PMBR (PIM Multicast Border Router) Status.

```
set ip pim pmbr { enable | disable }
```

### Syntax Description

**enable** - Enables the PMBR Status

**disable** - Disables the PMBR Status

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
iss (config)# set ip pim pmbr enable
```

- ➔ A PMBR integrates two different PIM domains (either PIM -SM or PIM -DM).
- ➔ A PMBR connects a PIM domain to other multicast routing domain(s).

### Related Command

**show ip pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM

## 22.8 ip pim component

This command configures the PIM component in the router and the no form of the command destroys the PIM component.

```
ip pim component <ComponentId (1-255)>
```

```
no ip pim component <ComponentId (2-255)>
```

### Mode

Global Configuration Mode

### Example:

```
iss (config)# ip pim component 1
```

- The PIM Component 1 cannot be deleted as it is the default component.
- The PIM Component corresponds to each instance of a PIM domain and classifies it as Sparse or Dense mode

### Related Command

**show ip pim component** - Displays the component information

## 22.9 set ip pim static-rp

This command enables or disables the Static RP configuration Status. This command specifies whether to use the configured static- RP.

```
set ip pim static-rp { enable | disable }
```

### Syntax Description

**enable** - Enables the Static RP configuration Status

**disable** - Disables the Static RP configuration Status

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
iss (config)# set ip pim static-rp enable
```

### Related Commands

**show ip pim rp-set** – Displays the RP-set information

**show ip pim rp-static** – Displays the RP-static information

## 22.10 set mode

This command sets the component mode to sparse or dense.

```
set mode {sparse | dense}
```

### Syntax Description

**sparse** - Sparse mode

**dense** - Dense mode

### Mode

PIM Component Mode

### Defaults

sparse

### Example:

```
SMIS(pim-comp)# set mode dense
```

- ➔ Sparse-mode routing protocols use shared trees. In a shared tree, sources forward multicast datagrams to a directly connected router, the designated router. The designated router encapsulates the datagram and unicasts it to an assigned RP router, which then forwards the datagram to members of multicast groups.
- ➔ Dense mode protocols are data driven, where multicast sources starts sending multicast data packets and receivers join if they want data packets or prune themselves

### Related Command

**show ip pim component** – Displays the component information

## 22.11 rp-candidate rp-address

This command sets the address of the interface, which will be advertised as a Candidate-RP and the “no” form of the command disables the address of the interface, which will be advertised as a Candidate-RP.

```
rp-candidate rp-address <Group Address> <Group Mask> <IP address>
```

```
no rp-candidate rp-address <Group Address> <Group Mask> <RP address>
```

### Syntax Description

**Group Address** - The IP multicast group address for which this entry contains multicast routing information

**Group Mask** - The IP multicast group address mask that, gives the group prefix for which this entry contains information about the RP

**IP address** - IP address

### Mode

PIM Component Mode

### Example:

```
SMIS(pim-comp)# rp-candidate rp-address 224.1.0.0 255.255.0.0  
20.0.0.2
```

- ➡ A Candidate-RP is a router configured to send periodic Candidate-RP-Advertisement messages to the BSR, and processes Join/Prune or Register messages for the advertised group prefix, when it is elected as a RP.

### Related Commands

**show ip pim rp-set** – Displays the RP-set information

**show ip pim rp-candidate** – Displays the RP-candidate information

## 22.12 rp-candidate holdtime

This command sets the holdtime of the component when it is a candidate RP in the local domain and the “no” form of the command sets the default holdtime (0) of the component.

```
rp-candidate holdtime <Holdtime value (0-255)>
```

```
no rp-candidate holdtime
```

### Mode

PIM Component Mode

### Defaults

0

### Example:

```
SMIS(pim-comp)# rp-candidate holdtime 25
```

- ➔ If its value is set to 0, it indicates that the local system is not a candidate RP Holdtime is the amount of time the candidate RP advertisement is valid. This field allows advertisements to be aged out.

### Related Command

**show ip pim rp-candidate** – Displays the RP-candidate information

## 22.13 rp-static rp-address

This command sets the address of the interface, which will be advertised as a Static-RP and the “no” form of the command disables the address of the interface, which will be advertised as a Static-RP.

```
rp-static rp-address <Group Address> <Group Mask> <IP address>
```

```
no rp-static rp-address <Group Address> <Group Mask>
```

### Syntax Description

**Group Address** - Indicates the PIM Sparse multicast group address using the listed RP.

**Group Mask** - The IP multicast group address mask that gives the group prefix for which this entry contains information about the RP

**IP address** - IP address

### Mode

PIM Component Mode

### Example:

```
SMIS(pim-comp)# rp-static rp-address 224.1.0.0 255.255.0.0 20.0.0.2
```

- ➡ Static configuration allows additional structuring of the multicast traffic by directing the multicast join/prune messages to statically configured RPs.

### Related Commands

**show ip pim rp-static** – Displays the RP-static information



## 22.14 ip pim query-interval

This command sets the frequency at which PIM hello messages are transmitted on this interface and the “no” form of the command sets the default hello timer interval for this interface.

```
ip pim query-interval <Interval (0-65535) secs>
```

```
no ip pim query-interval
```

### Mode

Interface Configuration Mode

### Defaults

30

### Example:

```
iss (config-if)# ip pim query-interval 60
```

- ➔ The query message informs the presence of a PIM router on the interface to the neighboring PIM routers.

### Related Command

**show ip pim interface** – Displays the routers PIM interfaces

## 22.15 ip pim message-interval

This command sets the frequency at which PIM Join/Prune messages are transmitted on this PIM interface and the “no” form of the command sets the default value for PIM Join/Prune message.

```
ip pim message-interval <Interval(0-65535)>
```

```
no ip pim message-interval
```

### Mode

Interface Configuration Mode

### Defaults

60

### Example:

```
iss (config-if)# ip pim message-interval 120
```

- ➔ The same Join/Prune message interval must be used on all the PIM routers in the PIM domain. If all the routers do not use the same timer interval, the performance of PIM Sparse can be adversely affected.

### Related Command

**show ip pim interface** – Displays the routers PIM interfaces

## 22.16 ip pim bsr-candidate

This command sets the preference value for the local interface as a candidate bootstrap router and the “no” form of the command sets the default preference value for the local interface as a candidate bootstrap router.

```
ip pim bsr-candidate <value (0-255)>
```

```
no ip pim bsr-candidate
```

### Mode

Interface Configuration Mode

### Defaults

0

### Example:

```
iss (config-if)# ip pim bsr-candidate 1
```

➡ A BSR is a dynamically elected router within a PIM domain.

### Related Command

**show ip pim bsr** – Displays the BSR information

## 22.17 ip pim componentId

This command adds the interface to the component.

```
ip pim componentId <value (1-255)>
```

### Mode

Interface Configuration Mode

### Defaults

1

### Example:

```
iss (config-if)# ip pim componentId 1
```

➡ This command adds the current VLAN into the specified PIM component.

### Related Commands

**ip pim component** – Configures the PIM component in the router

**show ip pim component** – Displays the component information

## 22.18 ip pim hello-holdtime

This command sets the holdtime for the hello message for that interface. The “no” form of the command sets the default holdtime (105) for the hello message for that interface.

```
ip pim hello-holdtime <holdtime(1-65535)>
```

```
no ip pim hello-holdtime
```

### Mode

Interface Configuration Mode

### Defaults

105

### Example:

```
iss (config-if)# ip pim hello-holdtime 180
```

➔ Holdtime is the amount of time a receiver must keep the neighbor reachable, in seconds.

### Related Commands

**show ip pim neighbor** – Displays the routers PIM neighbors information

**show ip pim interface** – Displays the routers PIM interfaces

## 22.19 ip pim dr-priority

This command sets the designated router priority value configured for the router interface and the “no” form of the command sets the default designated router priority value (0) for the router interface.

```
ip pim dr-priority <priority(1-65535)>
```

```
no ip pim dr-priority
```

### Mode

Interface Configuration Mode

### Defaults

1

### Example:

```
iss (config-if)# ip pim dr-priority 100
```

- ➔ The DR sets up multicast route entries and sends corresponding Join/Prune and Register messages on behalf of directly-connected receivers and sources, respectively.

### Related Command

**show ip pim interface** – Displays the routers PIM interfaces

## 22.20 ip pim override-interval

This command sets the override interval configured for router interface and the “no” form of the command sets the default override interval (0) for router interface.

```
ip pim override-interval <interval(0-65535)>
```

```
no ip pim override-interval
```

### Mode

Interface Configuration Mode

### Defaults

0

### Example:

```
iss (config-if)# ip pim override-interval 100
```

- ➔ Override interval is the random amount of time delayed for sending override messages to avoid synchronization of override messages when multiple downstream routers share a multi-access link.

### Related Command

**show ip pim interface** – Displays the routers PIM interfaces

## 22.21 ip pim lan-delay

This command sets the LanDelay configured for the router interface and the “no” form of the command sets the default LanDelay (0) for the router per interface.

```
ip pim lan-delay <value(0-65535)>
```

```
no ip pim lan-delay
```

### Mode

Interface Configuration Mode

### Defaults

0

### Example:

```
iss (config-if)# ip pim lan-delay 120
```

- ➔ The LAN Delay inserted by a router in the LAN Prune Delay option expresses the expected message propagation delay on the interface. It is used by upstream routers to find out the delayed time interval for a Join override message before pruning an interface.

### Related Command

**show ip pim interface** – Displays the routers PIM interfaces



## 22.22 set ip pim lan-prune-delay

This command sets the LanPruneDelay bit configured for the router interface to advertise the Lan delay.

```
set ip pim lan-prune-delay { enable | disable }
```

### Syntax Description

**enable** - Enables LAN-prune-delay

**disable** - Disables LAN-prune-delay

### Mode

Interface Configuration Mode

### Defaults

disable

### Example:

```
iss (config-if)# ip pim lan-prune-delay enable
```

The command specifies whether to use LAN prune delay or not.

### Related Command

**show ip pim interface** – Displays the routers PIM interfaces

## 22.23 no ip pim interface

This command deletes an interface at PIM level.

**no ip pim interface**

**Mode**

Interface Configuration Mode

**Example:**

```
iss (config-if)# no ip pim interface
```

This command is used to destroy the interface at PIM.

**Related Command**

**show ip pim interface** – Displays the routers PIM interfaces

## 22.24 debug ip pim

This command enables PIM trace and the “no” form of the command disables PIM trace.

```
debug ip pim {[nbr][grp][jp][ast][bsr][io][pibr][mrt][mdh][mgmt] |  
[all]}
```

```
no debug ip pim {[nbr][grp][jp][ast][bsr][io][pibr][mrt][mdh][mgmt] |  
[all]}
```

### Syntax Description

**nbr** - Neighbor Discovery traces

**grp** - Group Membership traces

**jp** - Join or Prune traces

**ast** - Assert state traces

**bsr** - Bootstrap/RP traces

**io** - Input Output traces

**pibr** - Interoperability traces

**mrt** - Multicast Route Table Update traces

**mdh** - Multicast Data Handling traces

**mgmt** - Configuration traces

**all** - All traces

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# debug ip pim all
```

A Four byte integer value is specified for enabling the level of debugging. Each bit in the four byte integer variable represents a level of debugging. The combinations of levels are also allowed.

The user has to enter the corresponding integer value for the bit set.

### Related Command

**show ip pim interface**— Displays the routers PIM interfaces



## 22.25 show ip pim interface

This command displays the routers PIM interfaces.

```
show ip pim interface [{ Vlan <vlan-id> | <iftype> <ifnum> | detail }]
```

### Syntax Description

**Vlan** - VLAN ID

**detail** - Detailed information of the interface

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip pim interface
Address IfName/IfId Ver/Mode
Nbr Qry DR-Address DR-Pr

Count Interval
10.0.0.1 vlan1/160 2/Sparse 0 45 10.0.0.1 5
20.0.0.1 vlan2/33 2/Sparse 0 30 20.0.0.1 1
30.0.0.1 vlan3/34 2/Sparse 0 60 30.0.0.1 1
```

```
SMIS# show ip pim interface vlan 1
Address IfName/IfId Ver/Mode
Nbr Qry DR-Address DR-Pr

Count Interval
10.0.0.1 vlan1/160 2/Sparse 0 45 10.0.0.1 5
```

```
SMIS# show ip pim interface detail
vlan1 160 is up
Internet Address is 10.0.0.1
Multicast Switching : Enabled
PIM: enabled
```

```
PIM version: 2, mode
  Sparse

PIM DR: 10.0.0.1
PIM DR Priority: 5
PIM Neighbour Count: 0
PIM Hello/Query Interval: 45
PIM Message Interval: 67
PIM Override Interval: 56
PIM Lan Delay: 66
PIM Lan-Prune-Delay: Disabled
PIM Component Id: 1
PIM domain border: disabled
```

It shows the list of Interface addresses, the mode of the interface, Designated Router on that interface, Hello Interval, Join/Prune Interval of the interface.

### Related Commands

```
set ip pim – Enables or disables PIM
ip pim query-interval – Sets the frequency at which PIM hello messages are transmitted
on this interface
ip pim message-interval – Sets the frequency at which PIM Join/Prune messages are
transmitted on this PIM interface
ip pim bsr-candidate – Sets the preference value for the local interface as a candidate
bootstrap router
ip pim hello-holdtime – Sets the holdtime for the hello message for that interface
ip pim dr-priority – Sets the designated router priority value configured for the router
interface
ip pim override-interval – Sets the override interval configured for router interface
ip pim lan-delay – Sets the LanDelay configured for the router interface
set ip pim lan-prune-delay – Sets the LanPruneDelay bit configured for the router
interface to advertise the lan delay
no ip pim interface – Deletes an interface at PIM level
debug ip pim – Enables PIM trace
```



## 22.26 show ip pim neighbor

This command displays the router's PIM neighbors' information.

```
show ip pim neighbor [ Vlan <vlan-id> | <iftype> <ifnum>]
```

### Syntax Description

**Vlan** - VLAN ID

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip pim neighbor vlan 1
```

```
Nbr IfName/Idx Uptime/Expiry Ver DRPri/Mode
CompId Override Lan
```

```
Address Interval Delay
```

```
-----
```

```
10.0.0.1 vlan1/160 00:03:41/92 v2 32/S 20 0 0
```

```
10.0.0.2 vlan1/160 00:04:13/97 v2 32/S 20 0 0
```

It shows the Neighbor Address, the interface used to reach the PIM Neighbor, the Up time (the time since this neighbor became the neighbor of the local router), Expiry Time (the min. time remaining before this PIM neighbor will be aged out), LAN delay and Override interval.

### Related Commands

**ip pim query-interval** – Sets the frequency at which PIM hello messages are transmitted on this interface

**ip pim message-interval** – Sets the frequency at which PIM Join/Prune messages are transmitted on this PIM interface

**ip pim bsr-candidate** – Sets the preference value for the local interface as a candidate bootstrap router

**ip pim hello-holdtime** – Sets the holdtime for the hello message for that interface





## 22.27 show ip pim rp-candidate

This command displays the candidate RP information.

```
show ip pim rp-candidate [ComponentId <1-255>]
```

### Syntax Description

**ComponentId** - Component ID

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip pim rp-candidate 2
CompId GroupAddress Group Mask RPAAddress/Priority
2 224.1.0.0 255.255.0.0 20.0.0.1/192
```

It shows the Group addresses, the Group Mask and the RP address that indicates the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.

### Related Commands

**rp-candidate rp-address** – Enables the address of the interface, which will be advertised as a Candidate-RP

**rp-candidate holdtime** – Sets the holdtime of the component when it is a candidate RP in the local domain

**rp-static rp-address** – Sets the address of the interface, which will be advertised as a Static- RP

## 22.28 show ip pim rp-set

This command displays the RP-set information.

```
show ip pim rp-set [rp-address]
```

### Syntax Description

**rp-address** - Indicates the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip pim rp-set
PIM Group-to-RP mappings
-----
Group Address: 224.1.0.0 Group Mask: 255.255.0.0
RP: 20.0.0.1
Component-Id: 2
Hold Time: 120, Expiry Time: 00:01:43
```

It shows details of the Group Prefix, RP address, Hold time and Expiry Time.

### Related Commands

**rp-candidate rp-address** – Enables the address of the interface, which will be advertised as a Candidate-RP

**set ip pim static-rp** – Enables or disables the Static RP configuration Status

## 22.29 show ip pim bsr

This command displays the BSR information.

```
show ip pim bsr [Component-Id (1-255)]
```

### Syntax Description

**Component-Id** - Component ID

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip pim bsr 1
PIMv2 Bootstrap Configuration For Component 1
```

```
-----
This system is the Bootstrap Router (BSR)
```

```
BSR Address: 10.0.0.1
```

```
BSR Priority: 6, Hash Mask Length: 30
```

### Related Command

**ip pim bsr-candidate** – Sets the preference value for the local interface as a candidate bootstrap router

## 22.30 show ip pim rp-static

This command displays the static RP information.

```
show ip pim rp-static [ComponentId <1-255>]
```

### Syntax Description

**ComponentId** - Component ID

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip pim rp-static 2
Static-RP Enabled
CompId GroupAddress Group Mask RPAAddress
2 225.1.0.0 255.255.0.0 20.0.0.1
```

### Related Command

**set ip pim static-rp** – Enables or disables the Static RP configuration Status

## 22.31 show ip pim component

This command displays the component information.

```
show ip pim component [ComponentId <1-255>]
```

### Syntax Description

**ComponentId** - Component ID

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip pim component 1
```

```
PIM Component Information
```

```
-----
```

```
Component-Id: 1
```

```
PIM Mode
```

```
  sparse, PIM Version: 2
```

```
Elected BSR: 10.0.0.1
```

```
Candidate RP Holdtime: 0
```

### Related Commands

**ip pim component** – Configures the PIM component in the router

**ip pim componentId** – Adds the interface to the component

## 22.32 show ip pim thresholds

This command displays threshold configured for SPT, RP thresholds, and rate limit values for both SM (Sparse mode

```
show ip pim thresholds
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip pim thresholds
PIM SPT Threshold Information
Group Threshold: 0
Source Threshold: 0
Switching Period: 0
PIM SPT-RP Threshold Information
Register Threshold: 0
RP Switching Period: 0
Register Stop rate limit: 5
```

### Related Commands

**set ip pim threshold** – Specifies the SPT group or source threshold when exceeded, switching to shortest path tree is initiated

**set ip pim spt-switchperiod** – Specifies the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree

**set ip pim rp-threshold** – Specifies the threshold at which the RP initiates switching to source specific shortest path tree

**set ip pim rp-switchperiod** – Specifies the period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree

**set ip pim regstop-ratelimit-period** – Specifies the period over which RP monitors number of register packets after sending the register stop message

**set ip pim pmbr** – Enables or disables the PMBR (PIM Multicast Border Router) Status

**ip pim dr-priority** – Sets the designated router priority value configured for the router interface

## 22.33 show ip pim mroute

This command displays the PIM multicast information.

```
show ip pim mroute [ {compid(1-255) | group-address | source-address }
summary]
```

### Syntax Description

**compid** - Component ID

**group-address** - Indicates the PIM multicast group address using the listed RP

**source-address** - The network address which identifies the sources for which this entry contains multicast routing information

**summary** - Summary of PIM mroute information

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip pim mroute
IP Multicast Routing Table
-----
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
Timers: Uptime/Expires

Interface State: Interface, State/Mode
PIM Multicast Routing Table for Component 1

(*, 224.1.0.0), 00:04:35/--- , RP:12.0.0.1
Incoming Interface: vlan1, RPF nbr: NULL, Route Flags: WR
Outgoing InterfaceList:
vlan2, Forwarding/Sparse, 00:04:35/---
(12.0.0.30,224.1.0.0), 00:00:04/00:03:26
Incoming Interface : vlan1, RPF nbr : NULL, Route Flags : S
Outgoing InterfaceList
vlan2, Forwarding/Sparse, 00:00:04/---
```

SMIS# show ip pim mroute 1 summary



## IP Multicast Routing Table

-----

Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit

Timers : Uptime/Expires

Interface State : Interface, State/Mode

PIM Multicast Routing Table For Component 1

(\* , 224,1,0.0) , 00:04:35/--- , RP : 12.0.0.1

Incoming Interface : vlan1, RPF nbr : NULL, Route Flags : WR

Outgoing InterfaceList:

vlan2, Forwarding/Sparse, 00:04:35/---

(12.0.0.30,224.1.0.0) , 00:00:04/00:03:26

Incoming Interface : vlan1, RPF nbr : NULL, Route Flages : S

Outgoing InterfaceList :

vlan2, Forwarding/Sparse , 00:00:04/---

It shows details of the (S ,G) ,(\*,G) and (\*,\*,RP) entries.

### Related Command

**ip pim bsr-candidate** – Sets the preference value for the local interface as a candidate bootstrap router

## 23 PIMv6

PIMv6 is a portable software implementation of the PIM (Sparse Mode and Dense Mode) specification, for IPv6 networks. **PIMv6** provides support for inter-domain routing between domains using PIMv6-SM or PIMv6-DM. It also avoids the performance problems of earlier multicast routing protocols.

This software provides multicast routing and forwarding capability to a router that runs the IPv6 protocol along with MLD (Multicast Listener Discovery). **PIMv6** routes multicast data packets independent of any unicast routing protocol.

The list of CLI commands for the configuration of PIMv6 is as follows:

- [set ipv6 pim](#)
- [set ip pim threshold](#)
- [set ip pim spt-switchperiod](#)
- [set ip pim rp-threshold](#)
- [set ip pim rp-switchperiod](#)
- [set ip pim regstop-ratelimit-period](#)
- [set ip pim pmbr](#)
- [set ip pim static-rp](#)
- [ip pim component](#)
- [ipv6 pim rp-candidate rp-address](#)
- [ipv6 pim rp-static rp-address](#)
- [ipv6 pim query-interval](#)
- [ipv6 pim message-interval](#)
- [ipv6 pim bsr-candidate](#)
- [ipv6 pim componentId](#)
- [ipv6 pim hello-holdtime](#)
- [ipv6 pim dr-priority](#)
- [ipv6 pim override-interval](#)
- [ipv6 pim lan-delay](#)
- [set ipv6 pim lan-prune-delay](#)
- [no ipv6 pim interface](#)
- [debug ipv6 pim](#)
- [show ipv6 pim interface](#)
- [show ipv6 pim neighbor](#)

[show ipv6 pim rp-candidate](#)

[show ipv6 pim rp-set](#)

[show ipv6 pim bsr](#)

[show ipv6 pim rp-static](#)

[show ipv6 pim component](#)

[show ipv6 pim thresholds](#)

[show ipv6 pim mroute](#)

## 23.1 set ipv6 pim

This command enables or disables PIMv6 globally.

```
set ipv6 pim { enable | disable }
```

### Syntax Description

**enable** - Enables PIMv6

**disable** - Disables PIMv6

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
iss (config)# set ipv6 pim enable
```

➔ When PIMv6 is globally enabled, the mode will be sparse.

### Related Command

**show ipv6 pim interface** – Displays the PIMv6 interfaces of the router

## 23.2 set ip pim threshold

This command configures the (Shortest Path Tree) SPT group or source threshold, when exceeded, switching to shortest path tree is initiated. To switch to SPT, the threshold MUST be configured.

```
set ip pim threshold { spt-grp | spt-src } < number of packets (0-2147483647) >
```

### Syntax Description

**spt-grp** - The threshold of data rate for any group. When exceeded, source specific counters are initiated for that particular group. It is based on number of bits per second

**spt-src** - The switching to Shortest Path Tree is initiated when the threshold of data rate for any source is exceeded. It is based on number of bits per second

**number of packets** - Number of packets

### Mode

Global Configuration Mode

### Defaults

0

### Example:

```
iss (config)# set ip pim threshold spt-grp 50
```

### Related Command

**show ipv6 pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

## 23.3 set ip pim spt-switchperiod

This command configures the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.

```
set ip pim spt-switchperiod <0-2147483647(in secs)>
```

### Mode

Global Configuration Mode

### Defaults

0

### Example:

```
iss (config)# set ip pim spt-switchperiod 60
```

- ▶ The same period is used for monitoring the data rate for both source and group. To switch to SPT, this period must be configured.

The SPT is used for multicast transmission of packets with the shortest path from sender to recipients.

### Related Command

**show ipv6 pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

## 23.4 set ip pim rp-threshold

This command sets the threshold at which RP (Rendezvous Point) initiates switching to source specific shortest path tree.

```
set ip pim rp-threshold <0-2147483647(number of reg packets)>
```

### Mode

Global Configuration Mode

### Defaults

0

### Example:

```
iss (config)# set ip pim rp-threshold 50
```

To switch to SPT, this threshold must be configured and this switching is based on the received number of registered packets.

### Related Command

**show ipv6 pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

## 23.5 set ip pim rp-switchperiod

This command sets the period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.

```
set ip pim rp-switchperiod <0-2147483647(in secs)>
```

### Mode

Global Configuration Mode

### Defaults

0

### Example:

```
iss (config)# set ip pim rp-switchperiod 100
```

To switch to SPT, this period must be configured RP-tree is a pattern that multicast packets are sent to a PIM-SM router by unicast and then forwarded to actual recipients from RP

### Related Command

**show ipv6 pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM



## 23.6 set ip pim regstop-ratelimit-period

This command sets the period over which RP monitors the number of register packets after sending the register stop message.

```
set ip pim regstop-ratelimit-period <0-2147483647(in secs)>
```

### Mode

Global Configuration Mode

### Defaults

5

### Example:

```
iss (config)# set ip pim regstop-ratelimit-period 100
```

The Register Stop Message is used to avoid encapsulation of multicast data packets from the first hop router to the RP.

### Related Command

**show ipv6 pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

## 23.7 set ip pim pmbr

This command enables or disables the PMBR (PIM Multicast Border Router) Status.

```
set ip pim pmbr { enable | disable }
```

### Syntax Description

**enable** - Enables the PMBR Status

**disable** - Disables the PMBR Status

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
iss (config)# set ip pim pmbr enable
```

A PMBR integrates two different PIM domains (either PIM -SM or PIM -DM).

A PMBR connects a PIM domain to other multicast routing domain(s).

### Related Command

**show ipv6 pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

## 23.8 set ip pim static-rp

This command enables or disables the Static RP configuration Status. This command specifies whether to use the configured static- RP.

```
set ip pim static-rp { enable | disable }
```

### Syntax Description

**enable** - Enables the Static RP configuration Status

**disable** - Disables the Static RP configuration Status

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
iss (config)# set ip pim static-rp enable
```

### Related Commands

**show ipv6 pim rp-set** – Displays the RP-set information

**show ipv6 pim rp-static** – Displays the RP-static information

## 23.9 ip pim component

This command configures the PIMv6 component in the router and the no form of the command destroys the PIMv6 component.

```
ip pim component <ComponentId (1-255)>
```

```
no ip pim component <ComponentId (2-255)>
```

### Mode

Global Configuration Mode

### Example:

```
iss (config)# ip pim component 1
```

- ➔ PIMv6 component 1 cannot be deleted as it is the default component.
- ➔ The PIMv6 Component corresponds to each instance of a PIMv6 domain and classifies it as Sparse or Dense mode.

### Related Command

**show ipv6 pim component-** Displays the component information

## 23.10 ipv6 pim rp-candidate rp-address

This command sets the address of the interface, which will be advertised as a Candidate-RP. The “no” form of the command disables the address of the interface, which will be advertised as a Candidate-RP.

```
ipv6 pim rp-candidate rp-address <Group Address> <Group Mask> <RP-  
address>
```

```
no ipv6 pim rp-candidate rp-address <Group Address> <Group Mask> <RP  
address>
```

**Group Address** - IPv6 multicast group address

**Group Mask** - IPv6 multicast group address mask that gives the group prefix for which the entry contains information about RP

### Syntax Description

**RP address** - IPv6 address of the Rendezvous Point

### Mode

PIM Component Mode

### Example:

```
SMIS(pim-comp)# ipv6 pim rp-candidate rp-address ff02::e001:0000  
112 3333::1111
```

- ➔ A Candidate-RP is a router configured to send periodic Candidate-RP-Advertisement messages to the BSR, and processes Join/Prune or Register messages for the advertised group prefix, when it is elected as a RP.

### Related Commands

**show ipv6 pim rp-set** – Displays the PIMv6 RP-set information

**show ipv6 pim rp-candidate** – Displays the PIMv6 RP-candidate information

## 23.11 ipv6 pim rp-static rp-address

This command sets the address of the IPv6 interface, which will be advertised as a Static-RP. The “no” form of the command disables the address of the IPv6 interface, which will be advertised as a Static-RP.

```
ipv6 pim rp-static rp-address <Group Address> <Group Mask> <RP address>
```

```
no ipv6 pim rp-static rp-address <Group Address> <Group Mask>
```

### Syntax Description

**Group Address** - Indicates the PIMv6 Sparse multicast group address using the listed RP

**Group Mask** - IPv6 multicast group address mask that gives the group prefix for which this entry contains information about RP

**RP address** - IPv6 address of the Rendezvous Point

### Mode

PIM Component Mode

### Example:

```
SMIS(pim-comp)# ipv6 pim rp-static rp-address ff02::e001:0000 112  
3333::1111
```

- ➔ The Static configuration allows additional structuring of the multicast traffic by directing the multicast join/prune messages to statically configured RPs.

### Related Commands

**show ipv6 pim rp-static** – Displays the RP-static information

## 23.12 ipv6 pim query-interval

This command sets the frequency at which PIMv6 hello messages are transmitted on the interface. The “no” form of the command sets the default hello timer interval for the interface.

```
ipv6 pim query-interval <Interval (0-65535) secs>
```

```
no ipv6 pim query-interval
```

### Mode

Interface Configuration Mode

### Defaults

30

### Example:

```
iss (config-if)# ipv6 pim query-interval 60
```

The query message informs the presence of a PIMv6 router on the interface to the neighboring PIMv6 routers.

### Related Command

**show ipv6 pim interface** – Displays the PIMv6 interfaces of the router

## 23.13 ipv6 pim message-interval

This command sets the frequency at which the PIMv6 Join/Prune messages are transmitted on the PIMv6 interface. The “no” form of the command sets the default value for the PIMv6 Join/Prune messages.

```
ipv6 pim message-interval <Interval (0-65535)>
```

```
no ipv6 pim message-interval
```

### Mode

Interface Configuration Mode

### Defaults

60

### Example:

```
iss (config-if)# ipv6 pim message-interval 120
```

- ➔ The Join/Prune message interval used on all the PIMv6 routers in the PIMv6 domain must be the same. If all the routers do not use the same timer interval, the performance of PIMv6 Sparse can be adversely affected.

### Related Command

**show ipv6 pim interface** – Displays the PIMv6 interfaces of the router



## 23.14 ipv6 pim bsr-candidate

This command sets the preference value for the local PIMv6 interface as a candidate bootstrap router. The “no” form of the command sets the default preference value for the local PIMv6 interface as a candidate bootstrap router.

```
ipv6 pim bsr-candidate <value (0-255)>
```

```
no ipv6 pim bsr-candidate
```

### Mode

Interface Configuration Mode

### Defaults

0

### Example:

```
iss (config-if)# ipv6 pim bsr-candidate 1
```

➡ A BSR is a dynamically elected router within the PIMv6 domain.

### Related Command

**show ipv6 pim bsr** – Displays the PIMv6 BSR information

## 23.15 ipv6 pim componentId

This command adds the interface to the component.

```
ipv6 pim componentId <value (1-255)>
```

### Mode

Interface Configuration Mode

### Defaults

1

### Example:

```
iss (config-if)# ipv6 pim componentId 1
```

This command adds the current VLAN into the specified PIMv6 component.

### Related Commands

**set ipv6 pim** – Enables or disables PIMv6 globally

**show ipv6 pim component** – Displays the component information

## 23.16 ipv6 pim hello-holdtime

This command sets the holdtime for the hello message for the PIMv6 interface. The “no” form of the command sets the default holdtime for the hello message for the interface.

```
ipv6 pim hello-holdtime <holdtime(1-65535)>
```

```
no ipv6 pim hello-holdtime
```

### Mode

Interface Configuration Mode

### Defaults

105

### Example:

```
iss (config-if)# ipv6 pim hello-holdtime 180
```

Holdtime is the amount of time a receiver must keep the neighbor reachable, in seconds.

### Related Commands

**show ipv6 pim neighbor** – Displays the PIMv6 neighbor(s) information of the router

## 23.17 ipv6 pim dr-priority

This command sets the designated router priority value configured for the PIMv6 router interface. The “no” form of the command sets the default designated router priority value for the PIMv6 router interface.

```
ipv6 pim dr-priority <priority(1-65535)>
```

```
no ipv6 pim dr-priority
```

### Mode

Interface Configuration Mode

### Defaults

1

### Example:

```
iss (config-if)# ipv6 pim dr-priority 100
```

- ➔ The DR sets up multicast route entries and sends corresponding Join/Prune and Register messages on behalf of directly-connected receivers and sources, respectively.

### Related Command

**show ipv6 pim interface** – Displays the PIMv6 interfaces of the router

## 23.18 ipv6 pim override-interval

This command sets the override interval configured for the PIMv6 router interface. The “no” form of the command sets the default override interval for the PIMv6 router interface.

```
ipv6 pim override-interval <interval(0-65535)>
```

```
no ipv6 pim override-interval
```

### Mode

Interface Configuration Mode

### Defaults

0

### Example:

```
iss (config-if)# ipv6 pim override-interval 100
```

- ➔ The Override interval is the random amount of time delayed for sending override messages to avoid synchronization of override messages when multiple downstream routers share a multi-access link.

### Related Command

**show ipv6 pim interface** – Displays the PIMv6 interfaces of the router

## 23.19 ipv6 pim lan-delay

This command sets the LanDelay configured for the PIMv6 router interface. The “no” form of the command sets the default LanDelay for the PIMv6 router per interface.

```
ipv6 pim lan-delay <value(0-65535)>
```

```
no ipv6 pim lan-delay
```

### Mode

Interface Configuration Mode

### Defaults

0

### Example:

```
iss (config-if)# ipv6 pim lan-delay 120
```

- ➔ The LAN Delay inserted by a router in the LAN Prune Delay option expresses the expected message propagation delay on the interface. It is used by upstream routers to find out the delayed time interval for a Join override message before pruning an interface.

### Related Command

**show ipv6 pim interface** – Displays the PIMv6 interfaces of the router

## 23.20 set ipv6 pim lan-prune-delay

This command sets the LanPruneDelay bit configured for the PIMv6 router interface to advertise the Lan delay. The command specifies whether to use LAN prune delay or not.

```
set ipv6 pim lan-prune-delay { enable | disable }
```

### Syntax Description

**enable** - Enables LAN-prune-delay

**disable** - Disables LAN-prune-delay

### Mode

Interface Configuration Mode

### Defaults

disable

### Example:

```
iss (config-if)# set ipv6 pim lan-prune-delay enable
```

### Related Command

**show ipv6 pim interface** – Displays the PIMv6 interfaces of the router

## 23.21 no ipv6 pim interface

This command deletes the IPv6 PIM Interface, that is, this command is used to destroy the interface at PIMv6.

**no ipv6 pim interface**

### Mode

Interface Configuration Mode

### Example:

```
iss (config-if)# no ipv6 pim interface
```

### Related Command

**show ipv6 pim interface** – Displays the PIMv6 interfaces of the router



## 23.22 debug ipv6 pim

This command enables PIMv6 trace and the “no” form of the command disables PIMv6 trace.

```
debug ipv6 pim {[nbr][grp][jp][ast][bsr][io][pmbr][mrt][mdh][mgmt] |  
[all]}
```

```
no debug ipv6 pim {[nbr][grp][jp][ast][bsr][io][pmbr][mrt][mdh][mgmt] |  
[all]}
```

### Syntax Description

**nbr** - Neighbor Discovery traces

**grp** - Group Membership traces

**jp** - Join or Prune traces

**ast** - Assert state traces

**bsr** - Bootstrap/RP traces

**io** - Input Output traces

**pmbr** - Interoperability traces

**mrt** - Multicast Route Table Update traces

**mdh** - Multicast Data Handling traces

**mgmt** - Configuration traces

**all** - All traces

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# debug ipv6 pim all
```

A Four byte integer value is specified for enabling the level of debugging. Each bit in the four byte integer variable represents a level of debugging. Combinations of levels are also allowed. The user has to enter the corresponding integer value for the bit set.

### Related Command

**show ipv6 pim interface**— Displays the PIMv6 interfaces of the router



## 23.23 show ipv6 pim interface

This command displays the PIMv6 interfaces of the router. It shows the list of Interface addresses, the mode of the interface, Designated Router on that interface, Hello Interval, Join/Prune Interval of the interface.

```
show ipv6 pim interface [{ Vlan <vlan-id> | detail }]
```

### Syntax Description

**vlan** - VLAN ID

**detail** - Detailed information of the interface

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 pim interface
```

```
Address IfName/ Ver/ Nbr Qry DR DR
```

```
IfId Mode
```

```
Count Interval Address Prio-
```

```
-----
fe80::2:a00:1 vlan1/33 2/Sparse 0 150 fe80::2:a00:1 1
fe80::2:1400:1 vlan2/34 2/Sparse 0 30 fe80::2:1400:1 1
fe80::2:1e00:1 vlan3/35 2/Sparse 0 30 fe80::2:1e00:1 1
```

```
SMIS# show ipv6 pim interface vlan 1
```

```
Address IfName/ Ver/ Nbr Qry DR DR
```

```
IfId Mode
```

```
Count Interval Address Prio-
```

```
-----
fe80::2:a00:1 vlan1/33 2/Sparse 0 150 fe80::2:a00:1 1
```

```
SMIS# show ipv6 pim interface detail
```

```
vlan1 33 is up
```

```
Internet Address is fe80::2:a00:1
```

```
Multicast Switching : Enabled
PIM : Enabled
PIMv6 : Enabled
PIM version : 2, mode
    Sparse
PIM DR : fe80::2:a00:1
PIM DR Priority : 1
PIM Neighbour Count : 0
PIM Hello/Query Interval : 150
PIM Message Interval : 200
PIM Override Interval : 0
PIM Lan Delay : 0
PIM Lan-Prune-Delay : Disabled
PIM Component Id : 1
PIM domain border : disabled
```

### Related Commands

**set ipv6 pim** – Enables or disables PIMv6

**ipv6 pim query-interval** – Sets the frequency at which PIMv6 hello messages are transmitted on the interface

**ipv6 pim message-interval** – Sets the frequency at which PIMv6 Join/Prune messages are transmitted on the PIMv6 interface

**ipv6 pim bsr-candidate** – Sets the preference value for the local PIMv6 interface as a candidate bootstrap router

**ipv6 pim dr-priority** – Sets the designated router priority value configured for the PIMv6 router interface

**ipv6 pim override-interval** – Sets the override interval configured for the PIMv6 router interface

**ipv6 pim lan-delay** – Sets the LanDelay configured for the PIMv6 router interface

**set ipv6 pim lan-prune-delay** – Sets the LanPruneDelay bit configured for the PIMv6 router interface to advertise the lan delay

**no ipv6 pim interface** – Deletes an interface at PIMv6 level

**debug ipv6 pim** – Enables PIMv6 trace

## 23.24 show ipv6 pim neighbor

This command displays the PIMv6 neighbor(s) information of the router. It displays the Neighbor Address, the interface used to reach the PIMv6 Neighbor, the Up time (the time since this neighbor became the neighbor of the local router), Expiry Time (the minimum time remaining before this PIMv6 neighbor will be aged out), Lan delay and Override interval.

**show ipv6 pim neighbor [ Vlan <vlan-id>]**

### Syntax Description

**vlan** - VLAN ID

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 pim neighbor
```

```
Nbr If Uptime/ Ver DRPri/ Comp Over- Lan
```

```
Address Name Expiry Mode
```

```
Id ride Delay
```

```
/Idx Interval
```

```
-----
```

```
fe80::2:a00:a vlan1/33 00:02:33/0 v2 0/S 1 0 0
```

```
fe80::2:1400:a vlan2/34 00:02:33/0 v2 0/S 1 0 0
```

```
SMIS# show ipv6 pim neighbor vlan 1
```

```
Nbr If Uptime/ Ver DRPri/ Comp Over- Lan
```

```
Address Name Expiry Mode
```

```
Id ride Delay
```

```
/Idx Interval
```

```
-----
```

```
fe80::2:a00:a vlan1/33 00:02:58/0 v2 0/S 1 0 0
```

### Related Commands

- ipv6 pim query-interval** – Sets the frequency at which PIMv6 hello messages are transmitted on the interface
- ipv6 pim message-interval** – Sets the frequency at which PIMv6 Join/Prune messages are transmitted on the PIMv6 interface
- ipv6 pim bsr-candidate** – Sets the preference value for the local PIMv6 interface as a candidate bootstrap router
- ipv6 pim hello-holdtime** – Sets the holdtime for the hello message for the PIMv6 interface

## 23.25 show ipv6 pim rp-candidate

This command displays the PIMv6 RP-candidate information. It displays the Group addresses, the Group Mask and the RP address that indicates the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.

```
show ipv6 pim rp-candidate [ComponentId <1-255>]
```

### Syntax Description

**ComponentId** - Component ID

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 pim rp-candidate 1
```

```
CompId GroupAddress/PrefixLength RPAddress/Priority
```

```
-----
```

```
1 ff02::e000:0/112 3333::a00:1/192
```

### Related Commands

**ipv6 pim rp-candidate rp-address** – Sets the address of the interface, which will be advertised as a Candidate-RP

**ipv6 pim rp-static rp-address** – Sets the address of the interface, which will be advertised as a Static-RP

## 23.26 show ipv6 pim rp-set

This command displays the PIMv6 RP-set information. It displays details of the Group Prefix, RP address, Hold time and Expiry Time.

```
show ipv6 pim rp-set [rp-address]
```

### Syntax Description

**rp-address** - Indicates the IPv6 address of the Rendezvous Point (RP) for the listed PIM Sparse group.

### Mode

Privileged EXEC Mode

### Example:

```
show ipv6 pim rp-set 3333::a00:a
PIM Group-to-RP mappings
-----
Group Address : ff00::Group Mask : 8
RP: 3333::a00:a
Component-Id : 1
Hold Time : 102, Expiry Time : 00:00:35
```

### Related Commands

**ipv6 pim rp-candidate rp-address** – Enables the address of the interface, which will be advertised as a Candidate-RP

**ipv6 pim rp-static rp-address** – Sets the address of the interface, which will be advertised as a Static-RP



## 23.27 show ipv6 pim bsr

This command displays the PIMv6 BSR information.

```
show ipv6 pim bsr [Component-Id (1-255)]
```

### Syntax Description

**Component-Id** - Component ID

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 pim bsr 1
PIMv2 Bootstrap Configuration For Component 1
-----
Elected BSR for Component 1
V6 BSR Address : 3333::a00:1
V6 BSR Priority : 100, Hash Mask Length : 126
This System is V6 Candidate BSR for Component 1
V6 BSR Address : 3333::a00:1
V6 BSR Priority : 100
```

### Related Command

**ipv6 pim bsr-candidate** – Sets the preference value for the local interface as a candidate bootstrap router

## 23.28 show ipv6 pim rp-static

This command displays the static RP information.

```
show ipv6 pim rp-static [ComponentId <1-255>]
```

### Syntax Description

**ComponentId** - Component ID

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 pim rp-static
Static-RP Enabled
CompId GroupAddress/PrefixLength RPAddress
-----
1 ff02::1111:2222/64 3333::4444
```

### Related Command

**ipv6 pim rp-static rp-address** – Enables or disables the Static RP configuration Status

## 23.29 show ipv6 pim component

This command displays the component information.

```
show ipv6 pim component [ComponentId <1-255>]
```

### Syntax Description

**ComponentId** - Component ID

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 pim component 1
```

```
PIM Component Information
```

```
-----
```

```
Component-Id: 1
```

```
PIM Mode
```

```
  sparse, PIM Version: 2
```

```
Elected BSR: 10.0.0.1
```

```
Candidate RP Holdtime: 0
```

### Related Commands

**ipv6 pim componentId** – Adds the interface to the component

## 23.30 show ipv6 pim thresholds

This command displays threshold configured for SPT, RP thresholds, and rate limit values for both SM and DM.

**show ipv6 pim thresholds**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 pim thresholds
PIM SPT Threshold Information
-----
Group Threshold : 111
Source Threshold : 222
Switching Period : 100
PIM SPT-RP Threshold Information
-----
Register Threshold : 333
RP Switching Period : 300
Register Stop rate limit : 400
```

### Related Commands

**set ip pim threshold** – Configures the SPT group or source threshold

**set ip pim spt-switchperiod**– Configures the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree

**set ip pim rp-threshold**– Sets the threshold at which the RP initiates switching to source specific shortest path tree

**set ip pim rp-switchperiod**– Sets the period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree

**set ip pim regstop-ratelimit-period**– Sets the period over which RP monitors number of register packets after sending the register stop message

**set ip pim pmbr**– Enables or disables the PMBR (PIM Multicast Border Router) Status

**ipv6 pim dr-priority**– Sets the designated router priority value configured for the router interface

## 23.31 show ipv6 pim mroute

This command displays the IPv6 PIM mroute information.

```
show ipv6 pim mroute [ {compid(1-255) | group <group-address> | source
<source-address> } summary ]
```

### Syntax Description

**compid** - Component ID

**group-address** - Indicates the PIMv6 multicast group address using the listed RP

**source-address** - The network address which identifies the sources for which this entry contains multicast routing information

**summary** - Summary of PIMv6 mroute information

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 pim mroute
```

```
IP Multicast Routing Table
```

```
-----
```

```
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
```

```
Timers: Uptime/Expires
```

```
Interface State: Interface, State/Mode
```

```
PIM Multicast Routing Table For Component 1
```

```
(*, ff02::e001:0) ,00:03:54/---3401:510a::3401:51a) Incoming
```

```
Interface : vlan1
```

```
,RPF nbr : fe80::2:a00:a ,Route Flags : WR
```

```
Outgoing InterfaceList :
```

```
vlan2, Forwarding/Sparse ,00:03:54/---
```

```
SMIS# show ipv6 pim mroute group ff02::e001:0 summary
```

```
IP Multicast Routing Table
```

```
-----
```

```
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
```

Timers: Uptime/Expires

PIM Multicast Routing Table For Component 1

```
(* , ff02::e001:0) ,00:02:49/---3401:510a::3401:51a) ,Route Flags  
: WR
```

SMIS# show ipv6 pim mroute source ca8d:5102::ca8d:5102 summary

IP Multicast Routing Table

-----

Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit

Timers: Uptime/Expires

```
(ca8d:5102::ca8d:5102,ff02::e001:0) ,00:01:04/04:01:45 ,Route  
Flags : ---
```

It shows details of the (S ,G) ,(\*,G) and (\*,\*,RP) entries.

### Related Command

**ipv6 pim bsr-candidate** – Sets the preference value for the local IPv6 interface as a candidate bootstrap router

## 24 VRRP

VRRP (Virtual Router Redundancy Protocol) is an election protocol that dynamically assigns responsibility for one or more virtual router(s) to the VRRP routers(s) on a LAN, allowing several routers on a multi-access link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP setup, one router is elected as the master router with the other routers acting as backups in case of the failure of the master router. VRRP is designed to eliminate the single point of failure inherent in the static default routed environment

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

[router vrrp](#)

[interface](#)

[vrrp - ip address](#)

[vrrp - priority](#)

[vrrp - preempt](#)

[vrrp - text-authentication](#)

[vrrp - interval](#)

[show vrrp](#)

[show vrrp interface](#)

[debug vrrp](#)

## 24.1 router vrrp

This command enables VRRP in the router and is used to enter the VRRP Configuration Mode  
The “no” form of the command disables VRRP in the router.

**router vrrp**

**no router vrrp**

### Mode

Global Configuration Mode

### Defaults

VRRP is disabled by default

### Example:

```
SMIS(config)# router vrrp
```

Enabling the VRRP router will transition the state of the virtual router from 'initialize' to 'backup' or 'master' (Initialize indicates that the virtual router is waiting for a startup event.

Backup indicates that the virtual router is monitoring the availability of the master router.

Master indicates that the virtual router is forwarding the packets for IP addresses that are associated with this router.).

Disabling the VRRP router will transition the state from 'backup' or 'master' to 'initialize'. State transitions may not be immediate but may depend on other factors such as the interface state.

### Related Command

**show vrrp** – Displays the VRRP status information



## 24.2 interface vlan

This command selects an interface to configure. The “no” form of the command deletes the virtual router entries on the given Interface.

```
interface [{ vlan <integer (1-4069)> | <iftype> <ifnum> }]
```

```
no interface [{ vlan <integer (1-4069)> | <iftype> <ifnum> }]
```

### Syntax Description

**vlan-id** - VLAN Identifier

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

VRRP Router Configuration Mode

### Example:

```
SMIS(config-vrrp)# interface vlan 3
```

- VRRP must be enabled prior to the execution of this command.
- This interface must have an ip address prior to the execution of this command

### Related Commands

**router vrrp** – Enables VRRP in the router

**show vrrp** – Displays the VRRP status information

## 24.3 vrrp - ip address

This command sets the Associated IP addresses for the virtual router. The “no” form of the command deletes the Associated IP addresses for the virtual router.

```
vrrp <vrid(1-255)> ipv4 <uicast_addr > [secondary]
```

```
no vrrp <vrid(1-255)> ipv4 [<uicast_addr>[secondary]]
```

### Syntax Description

**vrid** - Virtual Router ID

**ipv4** - IP address

**secondary** - Associated IP addresses

### Mode

VRRP Interface Configuration Mode

### Example:

```
SMIS(config-vrrp-if)# vrrp 3 ipv4 10.0.0.1
```

VRID is a number which along with an interface index uniquely identifies a virtual router on a given VRRP router.

Once this command is executed, the VRRP Module starts the transition from "Initial" state to either "Backup" state or "Master" state as per the election process on the specific interface

This command should precede any other interface command for this vrid.

### Related Commands

**router vrrp** – Enables VRRP in the router

**show vrrp** – Displays the VRRP status information

## 24.4 vrrp - priority

This command sets the priority for the virtual router. The “no” form of the command sets the priority for the virtual router to default value.

```
vrrp <vrid(1-255)> priority <priority(1-254)>
```

```
no vrrp <vrid(1-255)> priority
```

### Syntax Description

**vrid** - Virtual Router ID

**priority** - Priority used for the virtual router master election process

### Mode

VRRP Interface Configuration Mode

### Defaults

priority – 100

### Example:

```
SMIS(config-vrrp-if)# vrrp 3 priority 7
```

Higher values imply higher priority.

A priority of 255 is used for the router that owns the associated IP address (es).

The command **vrrp <vrid(1-255)> ipv4 <ip address>** must be entered for the current interface (with the proper vrid) before the execution of this command.

### Related Commands

**router vrrp** – Enables VRRP in the router

**show vrrp** – Displays the VRRP status information

## 24.5 vrrp - preempt

This command enables the pre-emption of state change from either Backup to Master or vice versa based on the election process. The “no” form of the command disables the preempt mode

```
vrrp <vrid(1-255)> preempt
```

```
no vrrp <vrid(1-255)> preempt
```

### Syntax Description

**vrid** - Virtual Router ID

**preempt** - Enables preemption of VRRP router states

### Mode

VRRP Interface Configuration Mode

### Defaults

Pre-emption is enabled by default

### Example:

```
SMIS(config-vrrp-if)# vrrp 5 preempt
```

The command **vrrp <vrid(1-255)> ipv4 <ip address>** must be entered for the current interface (with the proper vrid) before the execution of this command.

### Related Commands

**router vrrp** – Enables VRRP in the router

**show vrrp** – Displays the VRRP status information

## 24.6 vrrp - text-authentication

This command sets the authentication type for the virtual router to simple password. The “no” form of the command sets the authentication type for the virtual router to none.

```
vrrp <vrid(1-255)> text-authentication <password>
```

```
no vrrp <vrid(1-255)> text-authentication
```

### Syntax Description

**vrid** - Virtual Router ID

**textauthentication** - Authentication password

### Mode

VRRP Interface Configuration Mode

### Example:

```
SMIS(config-vrrp-if)# vrrp 4 text-authentication abcdefgh
```

The authentication password can be alphanumeric characters up to 8 digits.

The command **vrrp <vrid(1-255)> ipv4 <ip address>** must be entered for the current interface (with the proper vrid) before the execution of this command.

### Related Commands

**router vrrp** – Enables VRRP in the router

**show vrrp** – Displays the VRRP status information

## 24.7 vrrp - interval

This command sets the advertisement timer for a virtual router. The “no” form of the command sets the advertisement timer for a virtual router to default value.

```
vrrp <vrid(1-255)> timer <interval(1-255)secs>
```

```
no vrrp <vrid(1-255)> timer
```

### Syntax Description

**vrid** - Virtual Router ID

**timer** - The time interval, in seconds, between sending advertisement messages

### Mode

VRRP Interface Configuration Mode

### Defaults

1 second

### Example:

```
SMIS(config-vrrp-if)# vrrp 4 timer 6
```

Only the master router sends advertisements.

On expiry of the advertise timer, the Master sends advertisement packets to the Backup.

The command **vrrp <vrid(1-255)> ipv4 <ip address>** must be entered for the current interface (with the proper vrid) before the execution of this command

### Related Commands

**router vrrp** – Enables VRRP in the router

**show vrrp** – Displays the VRRP status information

## 24.8 show vrrp

This command displays the VRRP status information.

```
show vrrp [interface [{ vlan <VlanId(1-4069)> | <interface-type>
<interface-id> }] <VrId(1-255)>] [{brief|detail |statistics}]
```

### Syntax Description

**VrId** – Any valid VRID number between 1 to 255

**interface vlan** - VRRP information on the given VLAN ID andVRID

**brief** - Information about VRRP in brief

**detail** - Information about VRRP in detail

**statistics** - VRRP statistics

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show vrrp interface vlan 2 detail
vlan2 - vrID 1
-----
State is Master
Virtual IP address is 12.0.0.2
Virtual MAC address is 00:00:5e:00:01:01
Master router is 12.0.0.2
Associated IpAddresses :
-----
12.0.0.2
Advertise time is 1 secs
Current priority is 100
Configured priority is 100, may preempt
vlan2 - vrID 2
-----
State is Master
Virtual IP address is 12.0.0.1
```

```
Virtual MAC address is 00:00:5e:00:01:02
Master router is 12.0.0.1
Associated IpAddresses :
-----
12.0.0.1
Advertise time is 1 secs
Current priority is 255
Configured priority is 255, may preempt
```

### Related Commands

**router vrrp** – Enables VRRP in the router

**interface** – Selects an interface to configure

**vrrp - ip address** – Sets the IP address for the virtual router



## 24.9 show vrrp interface

This command displays the VRRP status information for the given interface.

```
show vrrp interface [{ vlan <VlanId(1-4069)> | <interface-type>
<interface-id> }] [{brief|detail |statistics}]
```

### Syntax Description

**interface vlan** - VRRP information on the given VLAN ID andVRID

**brief** - Information about VRRP in brief

**detail** - Information about VRRP in detail

**statistics** - VRRP statistics

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show vrrp interface vlan 2 detail
vlan2 - vrID 1
-----
State is Master
Virtual IP address is 12.0.0.2
Virtual MAC address is 00:00:5e:00:01:01
Master router is 12.0.0.2
Associated IpAddresses :
-----
12.0.0.2
Advertise time is 1 secs
Current priority is 100
Configured priority is 100, may preempt
vlan2 - vrID 2
-----
State is Master
Virtual IP address is 12.0.0.1
Virtual MAC address is 00:00:5e:00:01:02
```

```
Master router is 12.0.0.1
Associated IpAddresses :
-----
12.0.0.1
Advertise time is 1 secs
Current priority is 255
Configured priority is 255, may preempt
```

```
SMIS# show vrrp interface vlan 2 brief
P indicates configured to preempt
Interface vrID Priority P State Master VRouter
Addr Addr
-----
vlan2 1 100 P Master local 12.0.0.2
vlan2 2 255 P Master local 12.0.0.1
```

```
SMIS# show vrrp interface vlan 2 statistics
vlan2 - vrID 1
-----
Transitions to Master : 2
Advertisements Received : 0
Advertise Internal Errors : 0
Authentication Failures : 0
TTL Errors : 0
Zero Priority Packets Received : 1
Zero Priority Packets Sent : 0
Invalid Type Packets Received : 0
Address List Errors : 0
Invalid Authentication Type : 0
Authentication Type Mismatch : 0
Packet Length Errors : 0
vlan2 - vrID 2
-----
Transitions to Master : 1
Advertisements Received : 0
Advertise Internal Errors : 0
Authentication Failures : 0
```

```
TTL Errors : 0
Zero Priority Packets Received : 0
Zero Priority Packets Sent : 0
Invalid Type Packets Received : 0
Address List Errors : 0
Invalid Authentication Type : 0
Authentication Type Mismatch : 0
Packet Length Errors : 0
```

```
SMIS# show vrrp interface vlan 2
P indicates configured to preempt
Interface vrID Priority P State Master VRouter
Addr Addr
-----
vlan2 1 100 P Master local 12.0.0.2
vlan2 2 255 P Master local 12.0.0.1
```

### Related Commands

**router vrrp** – Enables VRRP in the router  
**interface** – Selects an interface to configure  
**vrrp - ip address** – Sets the IP address for the virtual router

## 24.10 debug vrrp

This command enables the display of link aggregation debug messages.

The “no” form of this command disables the display of link aggregation debug messages.

```
debug vrrp {all | all-pkt-dump | state-machine | resource | ip-pkt-dump
| timer }
```

```
no debug vrrp {all | all-pkt-dump | state-machine | resource | ip-pkt-
dump | timer}
```

### Syntax Description

**all** – displays all debug messages

**all-pkt-dump** – displays the contents of all VRRP packets

**state-machine** – displays the state machine transition debug messages

**resource** – displays the resources (like memory) utilization debug messages

**ip-pkt-dump** – displays the contents of all VRRP IP packets

**timer** – displays the timer start and expiry related debug messages

### Mode

Privileged/User EXEC Mode

### Defaults

Disabled

### Example:

```
SMIS# debug vrrp all
```

### Related Commands

## 25 RIP

RIP (Routing Information Protocol) is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network or an interconnected group of such LANs. RIP is classified by the Internet Engineering Task Force (IETF) as one of several internal gateway protocols (Interior Gateway Protocol).

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination.

After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet to for a specified destination.

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

[router rip](#)

[ip rip security](#)

[ip rip retransmission](#)

[network](#)

[neighbor](#)

[passive-interface vlan](#)

[output-delay](#)

[redistribute](#)

[default-metric](#)

[route-tag](#)

[auto-summary](#)

[ip rip default route originate](#)

[ip rip summary-address](#)

[ip rip default route install](#)

[ip rip send version](#)

[ip rip receive version](#)

[ip rip authentication mode](#)

[timers basic](#)

[ip split-horizon](#)

[debug ip rip](#)

[show ip rip](#)

## 25.1 router rip

This command enters the router configuration mode and the “no” form of the command disables RIP on all the interfaces.

```
router rip
```

```
no router rip
```

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# router rip
```

### Related Commands

**network** – Enables RIP on an IP network

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.2 ip rip security

This command accepts/ignores RIP1 packets when authentication is in use and the no form of the command sets the security level to its default value.

```
ip rip security { minimum | maximum }
```

```
no ip rip security
```

### Syntax Description

**minimum** - Denotes that the RIP1 packets will be accepted even when authentication is in use

**maximum** - Denotes that RIP1 packets will be ignored when authentication is in use

### Mode

Router Configuration Mode

### Defaults

maximum

### Example:

```
SMIS(config-router)# ip rip security minimum
```

### Related Command

**show ip rip** – Displays IP RIP protocol database or statistics



## 25.3 ip rip retransmission

This command configures the timeout interval and number of retries to retransmit the update request packet or an unacknowledged update response packet and the “no” form of the command sets the retransmission timeout interval or the number of retransmission retries to its default value.

```
ip rip retransmission { interval <timeout-value (5-10)> | retries  
<value (10- 40)> }
```

```
no ip rip retransmit { interval | retries }
```

### Syntax Description

**interval** - The timeout interval to be used to retransmit the Update request packet or an unacknowledged update response packet

**retries** - The maximum number of retransmissions of the update request and update response packets

### Mode

Router Configuration Mode

### Defaults

Interval - 5

Retries - 36

### Example:

```
SMIS(config-router)# ip rip retransmission interval 6
```

- ➡ During retries, if no response is received then the routes through the next hop router are marked unreachable.

### Related Command

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.4 network

This command enables RIP on an IP network and the “no” form of the command disables RIP on an IP network.

```
network <ip-address>
```

```
no network <ip-address>
```

### Syntax Description

**ip-address** - IP address for the entry

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# network 10.0.0.1
```

- ➔ The network number specified must not contain any subnet information. RIP routing updates will be sent and received only through interfaces on this network. RIP sends updates to the interfaces in the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP update.

### Related Commands

**router rip** – Enables RIP on all the interfaces

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.5 neighbor

This command adds a neighbor router and the “no” form of the command deletes a neighbor router.

```
neighbor <ip address>
```

```
no neighbor <ip address>
```

### Syntax Description

**ip-address** - IP address of the neighbor router

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# neighbor 10.0.0.5
```

This command permits the point-to-point (no broadcast) exchange of routing information. When it is used in combination with the passive-interface router configuration command, routing information can be exchanged between a subset of routers and access servers on a LAN. Multiple neighbor commands can be used to specify additional neighbors or peers.

**Note:** This configuration will not result in sending unicast routing information to neighbors.

### Related Command

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.6 passive-interface vlan

This command suppresses routing updates on an interface. The “no” form of the command does not suppress routing updates from an interface.

```
passive-interface vlan <vlan-id(1-4069)>
```

```
no passive-interface vlan <vlan-id(1-4069)>
```

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# passive-interface vlan 1
```

If the sending of routing updates is disabled on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

### Related Command

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.7 output-delay

This command enables interpacket delay for RIP updates and the “no” form of the command disables interpacket delay for RIP updates.

**output-delay**

**no output-delay**

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# output-delay
```

➔ Configuring this command will help prevent the routing table from losing information.

### Related Command

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.8 redistribute

This command enables redistribution of corresponding protocol routes into RIP and the “no” form of the command disables redistribution of corresponding protocol routes into RIP.

```
redistribute { all | bgp | connected | ospf | static }
```

```
no redistribute { all | bgp | connected | ospf | static }
```

### Syntax Description

**all** - Advertises all routes learnt in the RIP process

**bgp** - Advertises routes learnt by BGP in the RIP process

**connected** - Connected routes redistribution

**ospf** - Advertises routes learnt by OSPF in the RIP process

**static** - Statically configured routes to advertise in the RIP process

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# redistribute all
```

### Related Commands

**default-metric** – Sets the RIP default metric

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.9 default-metric

This command sets the metric to be used for redistributed routes and the “no” form of the command sets the metric used with redistributed routes to its default value.

**default-metric** <value>

**no default-metric**

### Mode

Router Configuration Mode

### Defaults

3

### Example:

```
SMIS(config-router)# default-metric 1
```

The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes.

### Related Commands

**redistribute** – Enables redistribution of corresponding protocol routes into RIP

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.10 route-tag

This command sets the route tag to be used for redistributed routes and the “no” form of the command sets the route tag to its default value 0.

```
route-tag <tag-value>
```

```
no route-tag
```

### Syntax

<tag-value> - Any number between 1 to 65535

### Mode

Router Configuration Mode

### Defaults

0

### Example:

```
SMIS(config-router)# route-tag 1
```

### Related Commands

**redistribute** – Enables redistribution of corresponding protocol routes into RIP

**show ip rip** – Displays IP RIP protocol database or statistics



## 25.11 auto-summary

This command enables/disables auto summarization of routes in RIP.

```
auto-summary {enable | disable}
```

### Syntax Description

**enable** - Enables auto summarization feature in RIP

**disable** - Disables auto summarization feature in RIP

### Mode

Router Configuration Mode

### Defaults

enable

### Example:

```
SMIS(config-router)# auto-summary disable
```

- ➔ It is recommended to disable auto-summarization and configure interface specific aggregation with RIP version 2.

### Related Command

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.12 ip rip default route originate

This command sets the metric to be used for default route propagated over the interface. The no form of the command disables origination of default route over the interface.

```
ip rip default route originate <metric(1-15)>
```

```
no ip rip default route originate
```

### Mode

Interface Configuration Mode

### Defaults

no ip rip default route originate

### Example:

```
SMIS(config-if)# ip rip default route originate 10
```

The RIP must be enabled on the interface.

### Related Commands

**show ip rip** – Displays IP RIP protocol database or statistics

**show ip protocols** – Displays information about the active routing protocol process

## 25.13 ip rip summary-address

This command sets route aggregation over an interface for all subnet routes that falls under the specified IP address and mask. The “no” form of the command disables route aggregation with the specified IP address and mask.

```
ip rip summary-address <ip-address> <mask>
```

```
no ip rip summary-address <ip-address> <mask>
```

### Syntax Description

**ip-address** - IP Address of the interface specific aggregation

**mask** - Subnet Mask

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ip rip summary-address 60.0.0.0 255.0.0.0
```

- ▶ This command must not be used with RIPv1 send version.  
Auto-summarization overrides interface specific aggregation. Therefore, auto summarization must be disabled for interface specific route aggregation.

### Related Command

**show ip protocols** - Displays information about the active routing protocol process

## 25.14 ip rip default route install

This command installs the default route received in updates to the RIP database. The “no” form of the command does not install default route received in updates to the rip database.

```
ip rip default route install
```

```
no ip rip default route install
```

### Mode

Interface Configuration Mode

### Defaults

no ip rip default route install

### Example:

```
SMIS(config-if)# ip rip default route install
```

RIP must be enabled on the interface on which this command is executed.

### Related Command

**show ip protocols** - Displays information about the active routing protocol process

## 25.15 ip rip send version

This command sets the IP RIP version number for transmitting advertisements and the “no” form of the command sets IP RIP send version number to its default value.

```
ip rip send version { 1 | 2 | 1 2 | none }
```

```
no ip rip send version
```

### Syntax Description

1 | 2 | 1 2 | none - Indicates which version of RIP updates are to be sent

### Mode

Interface Configuration Mode

### Defaults

1 2

### Example:

```
SMIS(config-if)# ip rip send version 1
```

1 implies sending RIP updates compliant with RFC 1058. 2 implies multicasting RIP updates. 1 2 implies both 1 & 2.

### Related Commands

**ip rip receive version** – Sets IP RIP version number for receiving advertisements

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.16 ip rip receive version

This command sets IP RIP version number for receiving advertisements and the “no” form of the command sets IP RIP receive version number to its default value.

```
ip rip receive version { 1 | 2 | 1 2 | none }
```

```
no ip rip receive version
```

### Syntax Description

1 | 2 | 1 2 | none - Indicates which version of RIP updates, are to be accepted

### Mode

Interface Configuration Mode

### Defaults

1 2

### Example:

```
SMIS(config-if)# ip rip receive version 1
```

The command indicates which version of RIP updates are to be accepted. rip2 and rip1 2 implies reception of multicast packets.

### Related Commands

**ip rip send version**— Sets IP RIP version number for transmitting advertisements

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.17 ip rip authentication mode

This command configures authentication mode and key. The “no” form of the command disables authentication.

```
ip rip authentication mode { text | md5 } key-chain <key-chain-name>
(16)>
```

```
no ip rip authentication
```

### Syntax Description

**text** - Clear text authentication

**md5** - Keyed Message Digest 5 (MD5) authentication. More than one entry can be configured for an interface

**key-chain** - The value to be used as the Authentication Key

### Mode

Interface Configuration Mode

### Defaults

No authentication

### Example:

```
SMIS(config-if)# ip rip authentication mode text key-chain asdf123
```

If a string shorter than 16 octets is supplied, it will be left-justified and padded to 16 octets, on the right, with nulls (0x00).

### Related Command

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.18 timers basic

This command sets update, route age and garbage collection timers. The “no” form of the command sets update, route age and garbage collection timers to the default values.

```
timers basic <update-value (10-3600)> <routeage-value (30-500)>  
<garbage-value (120-180)>
```

```
no timers basic
```

### Syntax Description

**update-value** - Interval Time Between Updates

**routeage-value** - Time after which the entry is put into garbage collect interval

**garbage-value** - Interval before deleting an entry after not hearing it

### Mode

Interface Configuration Mode

update-value - 30

routeage-value - 180

### Defaults

garbage-value - 120

### Example:

```
SMIS(config-if)# timers basic 20 40 150
```

The advertisements of garbage-value entry is set to INFINITY, while sending to others.

### Related Command

**show ip rip** – Displays IP RIP protocol database or statistics



## 25.19 ip split-horizon

This command sets the split horizon status and the “no” form of the command disables the split horizon status.

```
ip split-horizon [poisson]
```

```
no ip split-horizon
```

### Syntax Description

**poisson** - Split horizon with poisson reverse is enabled

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ip split-horizon
```

The value splitHorizon denotes that splitHorizon must be applied in the response packets that are going out.

### Related Command

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.20 debug ip rip

This command sets the debug level for RIP module and the “no” form of the command resets the debug level for RIP module.

```
debug ip rip { all | init | data | control | dump | os | mgmt | failure  
| buffer }
```

```
no debug ip rip { all | init | data | control | dump | os | mgmt |  
failure | buffer }
```

### Syntax Description

**all** - All resources

**init** - Initialization and Shutdown messages

**data** - Data path messages

**control** - Control Plane messages

**dump** - Packet Dump messages

**os** - OS Resource Messages

**mgmt** - Management messages

**failure** - All failure messages (All failures including Packet Validation)

**buffer** - Buffer messages

### Mode

Privileged EXEC Mode

### Defaults

init

### Example:

```
SMIS# debug ip rip all
```

### Related Command

**show ip rip** – Displays IP RIP protocol database or statistics

## 25.21 show ip rip

This command displays IP RIP protocol database or statistics.

```
show ip rip { database [ <ip-address> <ip-mask> ] | statistics }
```

### Syntax Description

**database** - RIP protocol database for the specified IP address and IP mask of the RIP interface entry

**statistics** - RIP statistics on the router

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip rip database 40.0.0.0 255.0.0.0
40.0.0.0/8 directly connected, vlan1
```

```
SMIS# show ip rip statistics
```

```
RIP Global Statistics:
```

```
-----
```

```
Total number of route changes is 1
Total number of queries responded is 0
Total number of periodic updates sent is 2
Total number of dropped packets is 0
```

```
RIP Interface Statistics:
```

```
-----
```

```
Interface Periodic BadRoutes Triggered BadPackets Admin
IP Address Updates Sent Rcd Updates Sent Rcd Status
```

```
--- -----
```

```
40.0.0.1 2 0 1 2 Enabled
```

```
SMIS# show ip rip database
```

```
10.0.0.0/8 [1 ] auto-summary
10.2.0.0/16 [1 ] directly connected, vlan1
30.0.0.0/8 [1 ] auto-summary
```

30.2.0.0/16 [1 ] directly connected, vlan2

**Related Commands**

**router rip** – Enables RIP on all the interfaces

**ip rip security** – Accepts/ignores RIP1 packets when authentication is in use

**ip rip retransmission** – Configures the timeout interval and number of retries to retransmit the

update request packet or an unacknowledged update response packet

**network** – Enables RIP on an IP network

**neighbor** – Adds a neighbor router

**passive-interface vlan** – Suppresses routing updates on an interface

**output-delay** – Enables interpacket delay for RIP updates

**redistribute** – Enables redistribution of corresponding protocol routes into RIP

**default-metric** – Sets the RIP default metric

**ip rip send version** – Sets IP RIP version number for transmitting advertisements

**ip rip receive version** – Sets IP RIP version number for receiving advertisements

**ip rip authentication mode**

– Configures authentication mode and key

**timers basic** – Sets update, route age and garbage collection timers

**ip split-horizon** – Sets the split horizon status

**debug ip rip** – Sets the debug level for RIP module

## 26 OSPF

OSPF (Open Shortest Path First ) protocol, is an Interior Gateway Protocol used to distribute routing information within a single Autonomous System. Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations), which describes the state of its own links, and it also sends the complete routing structure (topography).

The advantage of shortest path first algorithms is that they result in smaller more frequent updates everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (when routers continuously increment the hop count to a particular network). This makes for a stable network.

Before configuring OSPF, RRD needs to be enabled. This will be done by defining RRD\_WANTED in LR/make.h in compilation. In addition, all OSPF interface related configurations, can be done only when the global OSPF is enabled.

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

[router ospf](#)

[router-id](#)

[area - Stability interval](#)

[area - translation-role](#)

[compatible rfc1583](#)

[abr-type](#)

[neighbor](#)

[area-default cost](#)

[area- nssa](#)

[area-stub](#)

[default-information originate always](#)

[area - virtual-link](#)

[ASBR Router](#)

[area - range](#)

[summary-address](#)

[redistribute](#)

[redist-config](#)

[network](#)

[set nssa asbr-default-route translator](#)

[passive-interface vlan](#)

[passive-interface default](#)

[ip ospf demand-circuit](#)

[ip ospf retransmit-interval](#)

[ip ospf transmit-delay](#)

[ip ospf priority](#)

[ip ospf hello-interval](#)

[ip ospf dead-interval](#)

[ip ospf cost](#)

[ip ospf network](#)

[ip ospf authentication-key](#)

[ip ospf message-digest-key](#)

[debug ip ospf](#)

[show ip ospf interface](#)

[show ip ospf neighbor](#)

[show ip ospf request-list](#)

[show ip ospf retransmission-list](#)

[show ip ospf virtual-links](#)

[show ip ospf border-routers](#)

[show ip ospf - summary address](#)

[show ip ospf info](#)

[show ip ospf route](#)

[show ip ospf - database summary](#)

[show ip ospf - database](#)

## 26.1 router ospf

This command enables OSPF routing process and the “no” form of the command disables OSPF routing process.

```
router ospf
```

```
no router ospf
```

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# router ospf
```

The command `no router ospf` disables the OSPF Router Admin Status to terminate the OSPF process.

### Related Commands

`router-id` – Sets the router-id for the OSPF process

`network` – Defines the interfaces on which OSPF runs and area ID for those interfaces

`show ip ospf route` – Displays routes learnt by OSPF process

`show ip ospf - database` – Displays OSPF Database summary for the LSA type



## 26.2 router-id

This command sets the router-id for the OSPF process.

```
router-id <router ip address>
```

### Syntax Description

**router ip address** - Specifies the OSPF router ID as an IP address

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# router-id 10.0.0.1
```

An arbitrary value for the ip-address for each router can be configured; however, each router ID must be unique. To ensure uniqueness, the router-id must match with one of the router's IP interface addresses.

### Related Commands

**router ospf** – Enables OSPF routing process

**show ip ospf route** – Displays routes learnt by OSPF process

## 26.3 area - Stability interval

This command configures the Stability interval for NSSA and the “no” form of the command configures default Stability interval for NSSA.

```
area <area-id> stability-interval <Interval-Value (0 - 0x7fffffff)>
```

```
no area <area-id> stability-interval
```

### Syntax Description

**area-id** - Area associated with the OSPF address range. It is specified as an IP address

**stabilityinterval** - The number of seconds after an elected translator determines its services are no longer required, that it must continue to perform its translation duties

### Mode

Router Configuration Mode

### Defaults

40

### Example:

```
SMIS(config-router)# area 10.0.0.1 stability-interval 10000
```

Area ID 0.0.0.0 is used for the OSPF backbone.

The OSPF Sequence Number is a 32 bit signed integer. It starts with the value '80000001'h, -- or '-7FFFFFFF'h, and increments until '7FFFFFFF'h. Thus, a typical sequence number will be very negative.

### Related Command

**show ip ospf info** – Displays general information about OSPF routing process

## 26.4 area - translation-role

This command configures the translation role for the NSSA and the “no” form of the command configures the default translation role for the NSSA.

```
area <area-id> translation-role { always | candidate }
```

```
no area <area-id> translation-role
```

### Syntax Description

**area-id** - Area associated with the OSPF address range. It is specified as an IP address

**translation-role** - An NSSA Border router's ability to perform NSSA Translation of Type-7 LSAs to Type-5 LSAs.

### Mode

Router Configuration Mode

### Defaults

candidate

### Example:

```
SMIS(config-router)# area 10.0.0.1 translation-role always
```

Type-5 LSAs- Originated by AS boundary routers, and flooded through-out the AS. Each AS-external-LSA describes a route to a destination in another Autonomous System.

Default routes for the AS can also be described by AS-external-LSAs.

### Related Command

**area- nssa** – Configures an area as a NSSA and other parameters related to that area

## 26.5 compatible rfc1583

This command sets OSPF compatibility list compatible with RFC 1583 and the “no” form of the command disables RFC 1583 compatibility.

```
compatible rfc1583
```

```
no compatible rfc1583
```

### **Mode**

Router Configuration Mode

### **Defaults**

Enabled

### **Example:**

```
SMIS(config-router)# compatible rfc1583
```

This command enables support of RFC1583 compatibility in products that support later standards. It controls the preference rules, when choosing among multiple AS external LSAs advertising the same destination. When set to enabled, the preference rules remain those specified by RFC 1583. When set to disabled, the preference rules are those stated in RFC 2178.

To minimize the chance of routing loops, all OSPF routers in an OSPF routing domain must have RFC compatibility set identically.

## 26.6 abr-type

This command sets the Alternative ABR Type.

```
abr-type { standard | cisco | ibm }
```

### Syntax Description

**standard** - Standard ABR type as defined in RFC 2328

**cisco** - CISCO ABR type as defined in RFC 3509

**ibm** - IBM ABR type as defined in RFC 3509

### Mode

Router Configuration Mode

### Defaults

standard

### Example:

```
SMIS(config-router)# abr-type standard
```

RFC 2328 – OSPF Version 2.

RFC-3509 -- Alternative Implementations of OSPF Area Border Routers.

### Related Commands

**router ospf** – Enables OSPF routing process

**show ip ospf info** – Displays general information about the OSPF routing process

## 26.7 neighbor

This command specifies a neighbor router and its priority. The “no” form of the command removes the neighbor/Set default value for the Neighbor Priority.

```
neighbor <neighbor-id> [priority <priority value (0-255)>]
```

```
no neighbor <neighbor-id> [priority]
```

### Syntax Description

**neighbor-id** - Neighbor router ID

**priority** - A number value that specifies the router priority

### Mode

Router Configuration Mode

### Defaults

priority - 1

### Example:

```
SMIS(config-router)# neighbor 20.0.0.1 priority 25
```

The value 0 signifies that the neighbor is not eligible to become the designated router on this particular network.

### Related Commands

**ip ospf priority** – Sets the router priority

**ip ospf network** – Configures the OSPF network type to a type other than the default for a given media

**show ip ospf neighbor**– Displays OSPF neighbor information list

## 26.8 area-default cost

This command specifies a cost for the default summary route sent into a stub or NSSA and the “no” form of the command removes the assigned default route cost.

```
area <area-id> default-cost <cost> [tos <tos value(0-30)>]
```

```
no area <area-id> default-cost [tos <tos value (0-30)>]
```

### Syntax Description

**area-id** - Area associated with the OSPF address range. It is specified as an IP address

**default-cost** - Cost for the default summary route used for a stub area

**tos** - Type of Service of the route being configured

### Mode

Router Configuration Mode

### Defaults

default-cost - 10

tos - 0

### Example:

```
SMIS(config-router)# area 10.0.0.1 default-cost 5
```

A default cost can be defined only for a valid area.

tos can be configured only if the code is compiled with TOS Support

### Related Commands

**area-stub** - Specifies an area as a stub area and other parameters related to that area

**area - range** - Consolidates and summarizes routes at an area boundary

**ip ospf cost** - Specifies the cost of sending a packet on an interface

**ip ospf authentication** - Specifies the authentication type for an interface





## 26.9 area- nssa

This command configures an area as a NSSA and other parameters related to that area.

```
area <area-id> nssa [{ no-summary | default-information-originate
[metric <value>] [metric-type <Type(1-3)>] [tos <tos value (0-30)>] }]
```

### Syntax Description

**area-id** - Area associated with the OSPF address range. It is specified as an IP address

**nssa** - Configures an area as a not-so-stubby area (NSSA)

**no-summary** - Allows an area to be a not-so-stubby area but not have summary routes injected into it

**defaultinformationoriginate** - Default route into OSPF

**metric** - The Metric value applied to the route before it is advertised. into the OSPF Domain

**metric-type** - The Metric Type applied to the route before it is advertised. into the OSPF Domain

**tos** - Type of Service of the route being configured

### Mode

Router Configuration Mode

### Defaults

metric - 10

metric-type - 1

tos - 0

### Example:

```
SMIS(config-router)# area 10.0.0.1 nssa
```

The **no area <area-id> [{ stub | nssa }]** command removes an area or converts stub/nssa to normal area.

tos can be configured only if the code is compiled with TOS Support

### Related Commands

**area - range** – Consolidates and summarizes routes at an area boundary

**area - translation-role**– Configures the translation role for the NSSA



## 26.10 area-stub

This command specifies an area as a stub area and other parameters related to that area and the “no” form of the command removes an area or converts stub/nssa to normal area.

```
area <area-id> stub [no-summary]
```

```
no area <area-id> [{ stub | nssa }]
```

### Syntax Description

**area-id** - Area associated with the OSPF address range. It is specified as an IP address

**stub** - Stub area. If the area type is no-summary, the router will neither originate nor propagate summary LSAs into the stub area

**nssa** - Not So Stubby Area

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# area 10.0.0.1 stub
```

The command must be configured on all routers and access servers in the stub area.

### Related Commands

**area-default cost** – Specifies a cost for the default summary route sent into a stub or NSSA

**area - range** – Consolidates and summarizes routes at an area boundary

**ip ospf authentication** – Specifies the authentication type for an interface

## 26.11 default-information originate always

This command enables generation of a default external route into an OSPF routing domain and other parameters related to that area. The no form of the command disables generation of a default external route into an OSPF routing domain.

```
default-information originate always [metric <metric-value (0-0xffffffff)>] [metric-type <type (1-2)>]
```

```
no default-information originate always [metric <metric-value (0-0xffffffff)>] [metric-type <type (1-2)>]
```

### Syntax Description

**metric** - The Metric value applied to the route before it is advertised into the OSPF Domain

**metric-type** - The Metric Type applied to the route before it is advertised into the OSPF Domain

### Mode

Router Configuration Mode

### Defaults

metric - 10

metric-type - 2

### Example:

```
SMIS(config-router)# default-information originate always metric 1  
metric-type 1
```

### Related Command

**redistribute** - Configures the protocol from which the routes have to be redistributed into OSPF



## 26.12 area - virtual-link

This command defines an OSPF virtual link and its related parameters. The “no” form removes an OSPF virtual link.

```
area <area-id> virtual-link <router-id> [authentication {message-digest
| null}] [hello-interval <value (1-65535)>] [retransmit-interval <value
(0- 3600)>] [transmit-delay <value (0-3600)>] [dead-interval <value>]
[authentication-key <key (8)> | message-digest-key <Key-id (0-255)>
md5 <key (16)>}]
```

```
no area <area-id> virtual-link <router-id> [authentication] [hello-
interval] [retransmit-interval] [transmit-delay] [dead-interval]
[authentication-key | message-digest-key <Key-id (0-255)>}]
```

### Syntax Description

**area-id** - The Transit Area that the Virtual Link traverses. It is specified as an IP address

**virtual-link** - The Router ID of the Virtual Neighbor

**authentication** - The authentication type for an interface

**hello-interval** - The interval between hello packets that the software sends on the OSPF virtual link interface

**retransmitinterval** - The time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPF virtual link interface

**transmit-delay** - The time the router will stop using this key for packets generation

**dead-interval** - The interval at which hello packets must not be seen before its neighbors declare the router down (the range of values for the dead interval is 0–0x7ffffff)

**authenticationkey** - Identifies the secret key used to create the message digest appended to the OSPF packet

**message-digestkey** - OSPF MD5 authentication. Enables Message Digest 5 (MD5) authentication on the area specified by the area-id

**md5** - The secret key which is used to create the message digest appended to the OSPF packet

### Mode

Router Configuration Mode

### Defaults

Authentication - null

hello-interval - 10

retransmit-interval - 5

transmit-delay - 1

dead-interval - 40

**Example:**

```
SMIS(config-router)# area 10.0.0.1 virtual-link 20.0.0.1 authentication
message-digest hello-interval 100 retransmitinterval 100 transmit-delay
50 dead-interval 200 authenticationkey asdf
```

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link hello-interval and dead-interval: The value must be the same for all routers and access servers on a specific network

**Related Commands**

**area - range** – Consolidates and summarizes routes at an area boundary

**ip ospf authentication** – Specifies the authentication type for an interface

**show ip ospf info**– Displays general information about OSPF routing process

**show ip ospf virtual-links** – Displays OSPF Virtual link information

## 26.13 ASBR Router

This command specifies this router as ASBR. The “no” form of the command disables this router as ASBR.

**ASBR Router**

**no ASBR Router**

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# ASBR Router
```

Routers that act as gateways (redistribution) between OSPF and other routing protocols (IGRP, EIGRP, RIP, BGP, Static) or other instances of the OSPF routing process are called autonomous system boundary router (ASBR).

### Related Commands

**set nssa asbr-default-route translator** – Enables/disables setting of P bit in the default Type-7 LSA generated by NSSA internal ASBR

**show ip ospf info** – Displays general information about the OSPF routing process



## 26.14 area - range

This command consolidates and summarizes routes at an area boundary. The “no” form of the command deletes the Summary Address.

```
area <AreaId> range <Network> <Mask> {summary | Type7} [{advertise | notadvertise}] [tag <value>]
```

```
no area <AreaId> range <Network> <Mask>
```

### Syntax Description

**Area-id** - Area associated with the OSPF address range. It is specified as an IP address

**range** - OSPF address range

**Network** - The IP address of the Net indicated by the range

**Mask** - The subnet mask that pertains to the range

**summary** - Summary LSAs

**Type7** - Type-7 LSA

**advertise** - When set to advertise and associated areald is 0.0.0.0, aggregated Type-5 are generated. Otherwise if associated areald is x.x.x.x (other than 0.0.0.0) aggregated Type-7 is generated in NSSA x.x.x.x

**not-advertise** - When set to doNotAdvertise (2) and associated areald is 0.0.0.0, Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. While if associated areald is x.x.x.x(other than 0.0.0.0), Type-7 are not generated in NSSA x.x.x.x for the specified range

**tag** - The Tag Type describes whether Tags will be automatically generated or will be manually configured

### Mode

Router Configuration Mode

### Defaults

tag - 2

### Example:

```
SMIS(config-router)# area 10.0.0.1 range 10.0.0.0 255.0.0.0 summary  
advertise tag 10
```

The mask indicates the range of addresses being described by the particular route.

For Example:, a summary-LSA for the destination 128.185.0.0 with a mask of 0xffff0000 actually is describing a single route to the collection of destinations 128.185.0.0 - 128.185.255.255

This command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR.

### Related Commands

**ip ospf authentication** – Specifies the authentication type for an interface

**area-default cost** – Specifies a cost for the default summary route sent into a stub or NSSA

**area- nssa** – Configures an area as a NSSA and other parameters related to that area

**area-stub**– Specifies an area as a stub area and other parameters related to that area

**area - virtual-link** – Defines an OSPF virtual link and its related parameters

**summary-address** – Creates aggregate addresses for OSPF

**show ip ospf - summary address** – Displays OSPF Summary-address redistribution Information

## 26.15 summary-address

This command creates aggregate addresses for OSPF and the “no” form of the command deletes the External Summary Address.

```
summary-address <Network> <Mask> <AreaId> [{allowAll | denyAll |
advertise | not-advertise}] [Translation {enabled | disabled}]
```

```
no summary-address <Network> <Mask> <AreaId>
```

### Syntax Description

**Network** - The IP address of the Net indicated by the range

**Mask** - The subnet mask that pertains to the range

**AreaId** - Area associated with the OSPF address range. It is specified as an IP address

**allowAll** - When set to allowAll and associated areald is 0.0.0.0 aggregated Type-5 are generated for the specified range. In addition aggregated Type-7 are generated in all attached NSSA, for the specified range

**denyAll** - When set to denyAll neither Type-5 nor Type-7 will be generated for the specified range

**advertise** - When set to advertise and associated areald is 0.0.0.0, aggregated Type-5 are generated. Otherwise if associated areald is x.x.x.x(other than 0.0.0.0) aggregated Type-7 is generated in NSSA x.x.x.x

**not-advertise** - When set to doNotAdvertise (2) and associated areald is 0.0.0.0, Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. While associated areald is x.x.x.x(other than 0.0.0.0), Type-7 are not generated in NSSA x.x.x.x for the specified range

**Translation** - Indicates how an NSSA Border router is performing NSSA translation of Type-7 into Type-5 LSAs. When set to **enabled**, P Bit is set in the generated Type-7 LSA. When set to **disabled** P Bit is cleared in the generated Type-7 LSA for the range

### Mode

Router Configuration Mode

### Defaults

summary-address - advertise

translation - disabled

**Example:**

```
SMIS(config-router)# summary-address 10.0.0.6 255.0.0.0 10.0.0.0
allowAll Translation enabled
```

When translation {enabled | disabled} is set to enabled, the NSSA border router's futOspfAreaNssaTranslatorRole has been set to always. When this object is set to disabled, a candidate NSSA Border router does not perform translation. Indicates whether Type-5/Type-7 will be aggregated or not generated for the specified range. allowAll and denyAll are not valid for areald other than 0.0.0.0.

Routes learnt from other routing protocols can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes.

This command helps reduce the size of the routing table.

**Related Commands**

**ip ospf authentication-key** – Specifies a password to be used by neighboring routers that are using the OSPF simple password authentication

**area - range** – Consolidates and summarizes routes at an area boundary

**ip ospf message-digest-key** – Enables OSPF MD5 authentication

**show ip ospf - summary address** – Displays OSPF Summary-address redistribution Information

**show ip ospf - database summary** – Displays OSPF LSA Database summary

## 26.16 redistribute

This command configures the protocol from which the routes have to be redistributed into OSPF and the “no” form of the command disables redistribution of routes from the given protocol into OSPF.

```
redistribute {static | connected | rip | bgp | all}
```

```
no redistribute {static | connected | rip | bgp | all}
```

### Syntax Description

**static** - Redistributes routes, configured statically, to the OSPF routing protocol

**connected** - Redistributes directly connected network routes, to the OSPF routing protocol

**rip** - Redistributes routes that are learnt by the RIP process, to the OSPF routing protocol

**bgp** - Redistributes routes, that are learnt by the BGP process, to the OSPF routing protocol

**all** - Redistributes all routes to the OSPF routing protocol

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# redistribute static
```

The **ASBR Router** command must be configured prior to the execution of this command.

### Related Commands

**default-information originate always** – Enables generation of a default external route into an OSPF routing domain

**redist-config** – Configures the information to be applied to routes learnt from RTM

## 26.17 redist-config

This command configures the information to be applied to routes learnt from RTM and the “no” form of the command deletes the information applied to routes learnt from RTM.

```
redist-config <Network> <Mask> [metric-value <metric (1 - 16777215)>]
[metric-type {asExttype1 | asExttype2}] [tag <tag-value>]
```

```
no redist-config <Network> <Mask>
```

### Syntax Description

**Network** - IP Address of the Destination route

**Mask** - Mask of the Destination route

**metric-value** - The Metric value applied to the route before it is advertised into the OSPF Domain

**metric-type** - The Metric Type applied to the route before it is advertised into the OSPF Domain

**tag** - The Tag Type describes whether Tags will be automatically generated or will be manually configured

### Mode

Router Configuration Mode

### Defaults

metric-value - 10

metric-type - asExttype2

tag - manual

### Example:

```
SMIS(config-router)# redist-config 10.0.0.0 255.0.0.0 metricvalue
100 metric-type asExttype1 tag 10
```

tag <tag-value>: This is not used by OSPF protocol itself. It may be used to communicate information between AS boundary routers. The precise nature of this information is outside the scope of OSPF. If tags are manually configured, the futospfRRDRRouteTag MIB has to be set with the Tag value needed.

**Related Command**

**redistribute** – Configures the protocol from which the routes have to be redistributed into OSPF

## 26.18 network

This command defines the interfaces on which OSPF runs and the area ID for those interfaces. The “no” form of the command disables OSPF routing for interfaces defined and to remove the area ID of that interface.

```
network <Network number> area <area-id> [unnum Vlan <PortNumber>]
```

```
no network <Network number> area <area-id> [unnum Vlan <PortNumber>]
```

### Syntax Description

**Network number** - Network type

**area** - Area associated with the OSPF address range. It is specified as an IP address

**unnum Vlan** - VLAN id for which no ip address is configured

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# network 20.0.0.1 area 20.0.0.0 unnum Vlan 1
```

When a more specific OSPF network range is removed, interfaces belonging to that network range will be retained and remain active if and only if a less specific network range exists.

There is no limit to the number of network commands that can be used on the router

### Related Commands

**router ospf** – Enables OSPF routing process

**show ip ospf - database** – Displays OSPF Database summary for the LSA type

**show ip ospf interface** – Displays OSPF interface information



## 26.19 set nssa asbr-default-route translator

This command enables/disables setting of P bit in the default Type-7 LSA generated by NSSA internal ASBR.

```
set nssa asbr-default-route translator { enable | disable }
```

### Syntax Description

**enable** - When set to enabled, P-Bit is set in the generated Type-7 default LSA

**disable** - When set disabled, P-Bit is clear in the generated default LSA

### Mode

Router Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config-router)# set nssa asbr-default-route translator enable
```

Specifies the P-Bit setting for the default Type-7 LSA generated by ASBR(which is not ABR).

### Related Command

**ASBR Router** – Specifies this router as ASBR

## 26.20 passive-interface vlan

This command suppresses routing updates on an interface and the “no” form of the command enables routing updates on an interface.

```
passive-interface vlan <vlan-id(1-4069)>}
```

```
no passive-interface vlan <vlan-id(1-4069)>
```

### Syntax Description

**vlan-id** - LSA retransmissions for adjacencies belonging to the VLAN interface

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# passive-interface vlan 1
```

OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

### Related Commands

**passive-interface default** – Suppresses routing updates on all interfaces

**show ip ospf interface** – Displays OSPF interface information

**show ip ospf request-list** – Displays OSPF Link state request list information

## 26.21 passive-interface default

This command suppresses routing updates on all interfaces and the “no” form of the command enables routing updates on all interfaces.

**passive-interface default**

**no passive-interface default**

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# passive-interface default
```

All the OSPF interfaces created after the execution of this command will be passive.

This is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

### Related Commands

**passive-interface vlan** – Suppresses routing updates on an interface

**show ip ospf interface** – Displays OSPF interface information

**show ip ospf request-list** – Displays OSPF Link state request list information

## 26.22 ip ospf demand-circuit

This command configures OSPF to treat the interface as an OSPF demand circuit and the “no” form of the command removes the demand circuit designation from the interface.

```
ip ospf demand-circuit
```

```
no ip ospf demand-circuit
```

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ip ospf demand-circuit
```

It indicates whether Demand OSPF procedures (hello suppression to FULL neighbors and setting the DoNotAge flag on prorgated LSAs) must be performed on this interface.

On point-to-point interfaces, only one end of the demand circuit must be configured with this command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit

### Related Command

**show ip ospf interface** – Displays OSPF interface information

## 26.23 ip ospf retransmit-interval

This command specifies the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface and the “no” form of the command uses the default time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.

```
ip ospf retransmit-interval <seconds (0 - 3600)>
```

```
no ip ospf retransmit-interval
```

### Mode

Interface Configuration Mode

### Defaults

5

### Example:

```
SMIS(config-if)# ip ospf retransmit-interval 300
```

This value is also used while retransmitting database description and link-state request packets.

### Related Commands

**ip ospf hello-interval** – Specifies the interval between hello packets sent on the interface

**ip ospf dead-interval** – Sets the interval at which hello packets must not be seen before neighbors declare the router down

**ip ospf transmit-delay** – Sets the estimated time it takes to transmit a link state update packet on the interface

**show ip ospf retransmission-list** – Displays OSPF Link state retransmission list information

## 26.24 ip ospf transmit-delay

This command sets the estimated time it takes to transmit a link state update packet on the interface and the “no” form of the command sets the default estimated time it takes to transmit a link state update packet on the interface.

```
ip ospf transmit-delay <seconds (0 - 3600)>
```

```
no ip ospf transmit-delay
```

### Mode

Interface Configuration Mode

### Defaults

1

### Example:

```
SMIS(config-if)# ip ospf transmit-delay 50
```

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the seconds argument before transmission.

### Related Commands

**ip ospf hello-interval** – Specifies the interval between hello packets sent on the interface

**ip ospf dead-interval** – Sets the interval at which hello packets must not be seen before neighbors declare the router down

**ip ospf retransmit-interval** – Specifies the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface

## 26.25 ip ospf priority

This command sets the router priority and the “no” form of the command sets default value for router priority.

```
ip ospf priority <value (0 - 255)>
```

```
no ip ospf priority
```

### Mode

Interface Configuration Mode

### Defaults

1

### Example:

```
SMIS(config-if)# ip ospf priority 25
```

When two routers attached to a network attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence.

### Related Commands

**ip ospf network** – Configures the OSPF network type to a type other than the default for a given media

**neighbor** – Specifies a neighbor router and its priority

## 26.26 ip ospf hello-interval

This command specifies the interval between hello packets sent on the interface and the “no” form of the command sets default value for, interval between hello packets sent on the interface.

```
ip ospf hello-interval <seconds (1 - 65535)>
```

```
no ip ospf hello-interval
```

### Mode

Interface Configuration Mode

### Defaults

10

### Example:

```
SMIS(config-if)# ip ospf hello-interval 75
```

This value must be the same for all routers attached to a common network.

### Related Commands

**ip ospf retransmit-interval** – Specifies the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface

**ip ospf dead-interval** – Sets the interval at which hello packets must not be seen before neighbors declare the router down

**ip ospf transmit-delay** – Sets the estimated time it takes to transmit a link state update packet on the interface

**show ip ospf interface** – Displays OSPF interface information



## 26.27 ip ospf dead-interval

This command sets the interval at which hello packets must not be seen before neighbors declare the router down and the “no” form of the command sets default value for the interval at which hello packets must not be seen before neighbors declare the router down.

```
ip ospf dead-interval <seconds (0-0x7fffffff)>
```

```
no ip ospf dead-interval
```

### Mode

Interface Configuration Mode

### Defaults

40

### Example:

```
SMIS(config-if)# ip ospf dead-interval 1000
```

This value must be the same for all routers and access servers on a specific network.

### Related Commands

**ip ospf retransmit-interval** – Specifies the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface

**ip ospf hello-interval** – Specifies the interval between hello packets sent on the interface

**ip ospf transmit-delay** – Sets the estimated time it takes to transmit a link state update packet on the interface

**show ip ospf interface** – Displays OSPF interface information

## 26.28 ip ospf cost

This command explicitly specifies the cost of sending a packet on an interface and the “no” form of the command resets the path cost to the default value.

```
ip ospf cost <cost (1-65535)> [tos <tos value (0-30)>]
```

```
no ip ospf cost [tos <tos value (0-30)>]
```

### Syntax Description

**cost** - Type 1 external metrics which is expressed in the same units as OSPF interface cost that is in terms of the OSPF link state metric

**tos** - Type of Service of the route being configured

### Mode

Interface Configuration Mode

### Defaults

0

### Example:

```
SMIS(config-if)# ip ospf cost 10
```

In general, the path cost is calculated using the following formula:  $108 / \text{bandwidth}$   
Using this formula, the default path costs are calculated.

Example:: 56-kbps serial link-Default cost is 1785

Ethernet-Default cost is 10

tos can be configured only if the code is compiled with TOS Support

### Related Commands

**area-default cost**– Specifies a cost for the default summary route sent into a stub or NSSA

**show ip ospf interface** – Displays OSPF interface information

## 26.29 ip ospf network

This command configures the OSPF network type to a type other than the default for a given media and the “no” form of the command sets the OSPF network type to the default type.

```
ip ospf network {broadcast | non-broadcast | point-to-multipoint |  
point-topoint}
```

```
no ip ospf network
```

### Syntax Description

**broadcast** - Networks supporting many (more than two) attached routers, together with the capability to address a single physical message to all of the attached routers (broadcast)

**non-broadcast** - Networks supporting many (more than two) routers, but having no broadcast capability

**point-to-multipoint** - Treats the non-broadcast network as a collection of point-to-point links

**point-to-point** - A network that joins a single pair of routers

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ip ospf network broadcast
```

Each pair of routers on a broadcast network is assumed to be able to communicate directly. An Ethernet is an Example: of a broadcast network. A 56Kb serial line is an Example: of a point-to-point network.

### Related Commands

**neighbor**— Specifies a neighbor router and its priority

**ip ospf priority** – Sets the router priority

**show ip ospf interface** – Displays OSPF interface information

## 26.30 ip ospf authentication-key

This command specifies a password to be used by neighboring routers that are using the OSPF simple password authentication. The “no” form of the command removes a previously assigned OSPF password.

```
ip ospf authentication-key <password (8)>
```

```
no ip ospf authentication-key
```

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ip ospf authentication-key asdf123
```

The password string can contain from 1 to 8 uppercase and lowercase alphanumeric characters. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

### Related Commands

**ip ospf authentication** – Specifies the authentication type for an interface

**summary-address** – Creates aggregate addresses for OSPF

**show ip ospf info** – Displays general information about OSPF routing process

## 26.31 ip ospf authentication

This command specifies the authentication type for an interface and the “no” form of the command

removes the authentication type for an interface and set it to NULL authentication.

```
ip ospf authentication [{message-digest | null}]
```

```
no ip ospf authentication
```

### Syntax Description

**message-digest** - Message Digest authentication

**null** - NULL authentication

### Mode

Interface Configuration Mode

### Defaults

null

### Example:

```
SMIS(config-if)# ip ospf authentication
```

Before using the ip ospf authentication command, a password for the interface must be configured using the ip ospf authentication-key command.

If the authentication type is ‘message digest’ then key will be selected from the md-5 table.

### Related Commands

**area-stub** – Specifies an area as a stub area and other parameters related to that area

**area-default cost** – Specifies a cost for the default summary route sent into a stub or NSSA

**area - virtual-link** – Defines an OSPF virtual link and its related parameters

**area - range** – Consolidates and summarizes routes at an area boundary

**ip ospf authentication-key** – Specifies a password to be used by neighboring routers that are using the OSPF simple password authentication

**ip ospf message-digest-key** – Enables OSPF MD5 authentication



## 26.32 ip ospf message-digest-key

This command enables OSPF MD5 authentication and the “no” form of the command removes an old MD5 key.

```
ip ospf message-digest-key <Key-ID (0-255)> md5 <md5-Key (16)>
```

```
no ip ospf message-digest-key <Key-ID (0-255)>
```

### Syntax Description

**Key-ID** - Identifies the secret key, which is used to create the message digest appended to the OSPF packet

**md5** - Secret key, which is used to create the message digest appended to the OSPF packet

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ip ospf message-digest-key 5 md5 abcd123
```

Message Digest authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a "message digest" that gets appended to the packet.

Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same key value.

### Related Commands

**ip ospf authentication** – Specifies the authentication type for an interface

**summary-address** – Creates aggregate addresses for OSPF

**show ip ospf** – Displays general information about OSPF routing process

## 26.33 debug ip ospf

This command sets the OSPF debug level, and the “no” form of the command removes an old MD5 key.

```
debug ip ospf { pkt { hp | ddp | lrq | lsu | lsa } | module {  
adj_formation | ism | nsm | config | interface } }
```

```
no debug ip ospf { pkt { hp | ddp | lrq | lsu | lsa } | module {  
adj_formation | ism | nsm | config | interface } | all }
```

### Syntax Description

**pkt** - Packet High Level Dump debug messages

**hp** - Hello packet debug messages

**ddp** - DDP packet debug messages

**lrq** - Link State Request Packet debug messages

**lsu** - Link State Update Packet debug messages

**lsa** - Link State Acknowledge Packet debug messages

**module** - RTM Module debug messages

**adj\_formation** - Adjacency formation debug messages

**ism** - Interface State Machine debug messages

**nsm** - Neighbor State Machine debug messages

**config** - Configuration debug messages

**interface** - Interface

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# debug ip ospf pkt hp
```

The information displayed by the show ip ospf retransmission-list command is useful in debugging OSPF routing operations.

### Related Commands

**show ip ospf info** – Displays general information about OSPF routing process

**show debugging** – Displays the state of each debugging option





## 26.34 show ip ospf interface

This command displays OSPF interface information.

```
show ip ospf interface [ { vlan <integer(1-4069)> | <iftype> <ifnum> }]
```

### Syntax Description

**vlan** - LSA retransmissions for adjacencies belonging to the VLAN interface

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip ospf interface
vlan10 is up, line protocol is up
Internet Address 10.0.0.1, Mask 255.0.0.0, Area 33.0.0.12
AS 1, Router ID 10.0.0.1, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 4, Priority 1
Designated RouterId 10.0.0.1, Interface address 10.0.0.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
Hello due in 4 sec
Neighbor Count is 0, Adjacent neighbor count is 0
vlan1 is up, line protocol is up
Internet Address 40.0.0.1, Mask 255.0.0.0, Area 33.0.0.12
AS 1, Router ID 10.0.0.1, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 5, Priority 1
Designated RouterId 20.0.0.2, Interface address 40.0.0.2
Backup Designated RouterId 10.0.0.1, Interface address
40.0.0.1
Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
Hello due in 4 sec
Neighbor Count is 1, Adjacent neighbor count is 1
```

[Adjacent with the neighbor 20.0.0.2](#)

### Related Commands

**passive-interface vlan** – Suppresses routing updates on an interface

**passive-interface default** – Suppresses routing updates on all interfaces

**ip ospf demand-circuit** – Configures OSPF to treat the interface as an OSPF demand circuit

**ip ospf hello-interval** – Specifies the interval between hello packets sent on the interface

**ip ospf dead-interval** – Sets the interval at which hello packets must not be seen before neighbors declare the router down

**ip ospf cost** – Specifies the cost of sending a packet on an interface

## 26.35 show ip ospf neighbor

This command displays OSPF neighbor information list.

```
show ip ospf neighbor [vlan <vlan-id (1-4069)> | <iftype> <ifnum>]  
[Neighbor ID] [detail]
```

### Syntax Description

**vlan** - LSA retransmissions for adjacencies belonging to the VLAN interface

**Neighbor ID** - Neighbor router ID

**detail** - OSPF Neighbor information in detail

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip ospf neighbor
```

```
Neighbor-ID Pri State DeadTime Address Interface
```

```
-----
```

```
20.0.0.2 1 FULL/BACKUP 33 40.0.0.2 vlan1
```

### Related Command

**neighbor** – Specifies a neighbor router and its priority

## 26.36 show ip ospf request-list

This command displays OSPF Link state request list information.

```
show ip ospf request-list [<neighbor-id>] [vlan <vlan-id (1-4069)> |  
<iftype> <ifnum>]
```

### Syntax Description

**neighbor-id** - Neighbor router ID

**vlan** - LSA retransmissions for adjacencies belonging to the VLAN interface

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip ospf request-list  
OSPF Router with ID (20.0.0.2)  
Neighbor 10.0.0.1, interface vlan1 address 40.0.0.1  
Type LS-ID ADV-RTR SeqNo Age Checksum  
-----  
Neighbor 20.0.0.2, interface vlan1 address 40.0.0.2  
Type LS-ID ADV-RTR SeqNo Age Checksum  
-----
```

### Related Commands

**passive-interface vlan** – Suppresses routing updates on an interface

**passive-interface default** – Suppresses routing updates on all interfaces

## 26.37 show ip ospf retransmission-list

This command displays OSPF Link state retransmission list information.

```
show ip ospf retransmission-list [<neighbor-id>] [vlan <vlan-id (1-4069)>] | <iftype> <ifnum> ]
```

### Syntax Description

**neighbor-id** - Neighbor router ID

**vlan** - LSA retransmissions for adjacencies belonging to the VLAN interface

**iftype** - Interface type, can either be a gi, ex or qx ethernet interfaces

**ifnum** - Physical interface ID including slot and port number

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip ospf retransmission-list
OSPF Router with ID (20.0.0.2)
Neighbor 10.0.0.1, interface vlan1 address 10.0.0.2
Link State Retransmission due in 30 ticks, Queue length 3
Type LS-ID ADV-RTR SeqNo Age Checksum
```

This value is also used while retransmitting database description and link-state request packets.

### Related Command

**ip ospf retransmit-interval** – Specifies the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface

## 26.38 show ip ospf virtual-links

This command displays OSPF Virtual link information.

```
show ip ospf virtual-links
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip ospf virtual-links
```

```
Virtual Link to router 10.0.0.1, Interface State is DOWN
```

```
Transit Area 33.0.0.12
```

```
Transmit Delay is 1 sec, Neighbor State DOWN
```

```
Timer intervals configured, Hello 10, Dead 60, Retransmit 5
```

### Related Command

**area - virtual-link** – Defines an OSPF virtual link and its related parameters

## 26.39 show ip ospf border-routers

This command displays OSPF Border and Boundary Router Information.

```
show ip ospf border-routers
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip ospf border-routers
OSPF Process Border Router Information
Destination TOS Type NextHop Cost Rt.Type Area
-----
10.0.0.1 0 ASBR 40.0.0.1 1 intraArea 33.0.0.12
```

### Related Commands

**abr-type** – Sets the Alternative ABR Type

**ASBR Router** – Specifies this router as ASBR



## 26.40 show ip ospf - summary address

This command displays OSPF summary-address redistribution Information.

```
show ip ospf {area-range | summary-address}
```

### Syntax Description

**area-range** - Area associated with the OSPF address range. It is specified as an IP address

**summary-address** - Aggregate addresses for OSPF

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip ospf area-range
```

Display of Summary addresses for Type3 and Translated Type5

OSPF Summary Address Configuration Information

-----

Network Mask LSAType Area Effect Tag

-----

10.0.0.0 255.0.0.0 Summary 33.0.0.12 Advertise 1074636208

```
SMIS# show ip ospf summary-address
```

Display of Summary addresses for Type5 and Type7 from

redistributed routes

OSPF External Summary Address Configuration Information

-----

Network Mask Area Effect TranslationState

-----

10.0.0.1 255.0.0.0 33.0.0.12 advertiseMatching enabled

### Related Commands

**area - range** – Consolidates and summarizes routes at an area boundary

**summary-address** – Creates aggregate addresses for OSPF

## 26.41 show ip ospf info

This command displays general information about the OSPF routing process.

```
show ip ospf info
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip ospf info
OSPF Router ID 10.0.0.1
Supports only single TOS(TOS0) route
ABR Type supported is Standard ABR
Number of Areas in this router is 1
Area is 33.0.0.12
Number of interfaces in this area is 2
SPF algorithm executed 3 times
```

### Related Commands

**area - Stability interval** – Configures the Stability interval for NSSA

**area - virtual-link** – Defines an OSPF virtual link and its related parameters

**ip ospf authentication-key** – Specifies a password to be used by neighboring routers that are using the OSPF simple password authentication

**debug ip ospf** – Sets the OSPF debug level

## 26.42 show ip ospf route

This command displays routes learnt by OSPF process.

**show ip ospf route**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip ospf route
OSPF Process Routing Table
Dest/Mask TOS NextHop/Interface Cost Rt.Type Area
----- -- -
10.0.0.0/255.0.0.0 0 0.0.0.0/vlan10 1 IntraArea 33.0.0.12
40.0.0.0/255.0.0.0 0 0.0.0.0/vlan1 1 IntraArea 33.0.0.12
```

### Related Commands

**router ospf** – Enables OSPF routing process

**router-id** – Sets the router-id for the OSPF process

## 26.43 show ip ospf - database summary

This command displays OSPF LSA Database summary.

```
show ip ospf [area-id] database [{database-summary | self-originate |
advrouter <ip-address>}]
```

### Syntax Description

**area-id** - Area associated with the OSPF address range. It is specified as an IP address.

**database** - Displays how many of each type of LSA for each area there are in the database

**database-summary** - Displays how many of each type of LSA for each area there are in the database, and the total number of LSA types

**self-originate** - Displays only self-originated LSAs (from the local router)

**adv-router** - Displays all the specified router link-state advertisements (LSAs). If no IP address is included, the information is about the local router itself

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip ospf database
OSPF Router with ID (10.0.0.1)
Router Link States (Area 33.0.0.12)
-----
Link ID ADV Router Age Seq# Checksum Link count
-----
20.0.0.2 20.0.0.2 1 0x80000004 0xfa0 36
Network Link States (Area 33.0.0.12)
-----
Link ID ADV Router Age Seq# Checksum Link count
-----
40.0.0.2 20.0.0.2 1 0x80000001 0xce09 32
Router Link States (Area 33.0.0.12)
-----
Link ID ADV Router Age Seq# Checksum Link count
-----
```

```
10.0.0.1 10.0.0.1 0 0x80000004 0x9d0e 48
```

```
SMIS# show ip ospf database database-summary
```

```
OSPF Router with ID (10.0.0.1)
```

```
Area 0.0.0.0 database summary
```

```
-----
```

```
LSA Type Count Maxage
```

```
-----
```

```
Router 0 0
```

```
Network 0 0
```

```
Summary Net 0 0
```

```
Summary ASBR 0 0
```

```
Type-7 Ext 0 0
```

```
Opaque Link 0 0
```

```
Opaque Area 0 0
```

```
Subtotal 0 0
```

```
Area 33.0.0.12 database summary
```

```
-----
```

```
LSA Type Count Maxage
```

```
-----
```

```
Router 2 0
```

```
Network 1 0
```

```
Summary Net 0 0
```

```
Summary ASBR 0 0
```

```
Type-7 Ext 0 0
```

```
Opaque Link 0 0
```

```
Opaque Area 0 0
```

```
Subtotal 3 0
```

```
OSPF Process database summary
```

```
-----
```

```
LSA Type Count Maxage
```

```
-----
```

```
Router 2 0
```

```
Network 1 0
```

```
Summary Net 0 0
```

```
Summary ASBR 0 0
```

```
Type-5 Ext 0 0
```

```
Type-7 Ext 0 0
Opaque Link 0 0
Opaque Area 0 0
Opaque AS 0 0
Total 3 0
```

```
SMIS# show ip ospf database self-originate
```

```
OSPF Router with ID (10.0.0.1)
```

```
Router Link States (Area 33.0.0.12)
```

```
-----
Link ID ADV Router Age Seq# Checksum Link count
-----
10.0.0.1 10.0.0.1 0 0x80000004 0x9d0e 48
```

```
SMIS# show ip ospf database adv-router 20.0.0.2
```

```
OSPF Router with ID (10.0.0.1)
```

```
Router Link States (Area 33.0.0.12)
```

```
-----
Link ID ADV Router Age Seq# Checksum Link count
-----
20.0.0.2 20.0.0.2 1 0x80000004 0xfa0 36
Network Link States (Area 33.0.0.12)
```

```
-----
Link ID ADV Router Age Seq# Checksum Link count
-----
40.0.0.2 20.0.0.2 1 0x80000001 0xce09 32
```

**Related Command**

**summary-address** – Creates aggregate addresses for OSPF

## 26.44 show ip ospf - database

This command displays OSPF Database summary for the LSA type.

```
show ip ospf [area-id] database { asbr-summary | external | network |
nssaexternal | opaque-area | opaque-as | opaque-link | router | summary
} [linkstate- id] [{adv-router <ip-address> | self-originate}]
```

### Syntax Description

**area-id** - Area associated with the OSPF address range. It is specified as an IP address

**database** - Displays how many of each type of LSA for each area there are in the database

**asbr-summary** - Displays information only about the Autonomous System Boundary Router (ASBR) summary LSAs

**external** - Displays information only about the external LSAs

**network** - Displays information only about the network LSAs

**nssa-external** - Displays information about the NSSA external LSAs

**opaque-area** - Displays information about the Type-10 LSAs

**opaque-as** - Displays information about the Type-11 LSAs

**opaque-link** - Displays information about the Type-9 LSAs

**router** - Displays information only about the router LSAs

**summary** - Displays information only about the summary LSAs

**link-state-id** - Portion of the Internet environment that is being described by the advertisement. The value entered depends on the type of the LSA. The value must be entered in the form of an IP address

**adv-router** - Displays all the specified router link-state advertisements (LSAs). If no IP address is included, the information is about the local router itself

**self-originate** - Displays only self-originated LSAs (from the local router)

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip ospf database summary
```

```
OSPF Router with ID (10.0.0.1)
```

```
Summary Link States (Area 33.0.0.12)
```

```
-----
```

```
LS age : 300
Options : (No ToS Capability, DC)
LS Type : Summary Links(Network)
Link State ID : 10.0.0.0
Advertising Router : 10.0.0.1
LS Seq Number : 0x80000002
Checksum : 0xae77
Length : 28
```

```
SMIS# show ip ospf database network
OSPF Router with ID (20.0.0.2)
Network Link States (Area 33.0.0.12)
-----
LS age : 900
Options : (No ToS Capability, DC)
LS Type : Network Links
Link State ID : 40.0.0.2
Advertising Router : 20.0.0.2
LS Seq Number : 0x80000001
Checksum : 0xce09
Length : 32
```

## Related Commands

**network** – Defines the interfaces on which OSPF runs and to define the area ID for those interfaces

**router ospf** – Enables OSPF routing process



## 27 BGP

The BGP (Border Gateway Protocol) is an interautonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems and is used between Internet service providers (ISP). BGP is often the protocol used between gateway hosts on the Internet. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. Hosts using BGP communicate using the Transmission Control Protocol (TCP) and send updated router table information only when one host has detected a change. BGP is commonly used within and between Internet Service Providers (ISPs). The protocol is defined in RFC 1771.

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

[router bgp](#)

[ip bgp dampening](#)

[ip bgp overlap-policy](#)

[ip bgp synchronization](#)

[clear ip bgp](#)

[bgp router-id](#)

[bgp default local-preference](#)

[neighbor - remote-as](#)

[neighbor - ebgp-multihop](#)

[neighbor - next-hop-self](#)

[neighbor - interval](#)

[neighbor - timers](#)

[neighbor - shutdown](#)

[neighbor - send-community](#)

[bgp nonbgproute-adv](#)

[redistribute](#)

[bgp always-compare-med](#)

[default-metric](#)

[bgp med](#)

[bgp local-preference](#)

[bgp update-filter](#)

[aggregate-address index](#)

[bgp cluster-id](#)

[bgp client-to-client reflection](#)

[neighbor - route-reflector-client](#)

[bgp comm-route](#)

[bgp comm-peer](#)

[bgp comm-filter](#)

[bgp comm-policy](#)

[bgp ecomm-route](#)

[bgp ecomm-peer](#)

[bgp ecomm-filter](#)

[bgp ecomm-policy](#)

[bgp confederation identifier](#)

[bgp confederation peers](#)

[bgp bestpath med confed](#)

[neighbor - password](#)

[clear ip bgp](#)

[shutdown ip bgp](#)

[debug ip bgp](#)

[show bgp-version](#)

[show ip bgp](#)

[show ip bgp community - routes](#)

[show ip bgp extcommunity - routes](#)

[show ip bgp summary](#)

[show ip bgp filters](#)

[show ip bgp aggregate](#)

[show ip bgp med](#)

[show ip bgp dampening](#)

[show ip bgp local-pref](#)

[show ip bgp timers](#)

[show ip bgp info](#)

[show ip bgp rfl info](#)

[show ip bgp confed info](#)

[show ip bgp community](#)

[show ip bgp extcommunity](#)

[show ip bgp dampened-paths](#)

[show ip bgp flap-statistics](#)

## 27.1 router bgp

This command sets the AS number of the BGP Speaker. The “no” form of the command brings the BGP Speaker Global Admin status DOWN and resets the AS number of the BGP Speaker.

```
router bgp <AS no(1-65535)>
```

```
no router bgp
```

### Syntax Description

**AS no** - Autonomous system number that identifies the BGP router to other routers and tags the routing information passed along

### Mode

Global Configuration Mode

### Defaults

0

### Example:

```
SMIS(config)# router bgp 100
```

The command makes the BGP speaker Global Admin Status ACTIVE.

### Related Commands

**ip bgp dampening** – Configures the Dampening Parameters

**ip bgp overlap-policy** – Configures the Overlap Route policy for the BGP Speaker

**ip bgp synchronization** – Enables synchronization between BGP and IGP

**bgp router-id** – Configures the BGP Identifier of the BGP Speaker

**bgp default local-preference** – Configures the Default Local Preference value

**neighbor - remote-as** – Creates a Peer and initiates the connection to the peer

**neighbor - ebgp-multihop** – Enables BGP to establish connection with external peers

**neighbor - next-hop-self** – Enables BGP to send itself as the next hop for advertised routes

**neighbor - interval** – Configures neighbor interval

**neighbor - timers** – Configures neighbor KeepAlive Time and Hold Time Intervals

**neighbor - shutdown** – Disables the Peer session

**neighbor - send-community** – Enables advertisement of community attributes to (standard/extended) to peer

**bgp nonbgproute-advt** – Controls the advertisement of Non-BGP routes

**no ip bgp overlap-policy** – Resets the Overlap route policy to default

**redistribute** – Configures the protocol from which the routes have to be redistributed into BGP

**bgp always-compare-med** – Enables the comparison of med for routes received from different autonomous system

**default-metric** – Configures the Default IGP Metric value

**bgp med** – Configures an entry in MED Table

**bgp local-preference** – Configures an entry in Local Preference Table

**bgp update-filter** – Configures an entry in Update Filter Table

**aggregate-address index** – Configures an entry in Aggregate Table

**bgp cluster-id** – Configures the Cluster ID for Route Reflector

**bgp client-to-client reflection** – Configures the Route Reflector to support route reflection to Client Peers

**neighbor - route-reflector-client** – Configures the Peer as Client of the Route Reflector

**bgp comm-route** – Configures an entry in additive or delete community table

**bgp comm-peer** – Enables/disables advertisement of community attributes to peer

**bgp comm-filter** – Allows/filters the community attribute while receiving or advertising

**bgp comm-policy** – Configures the community attribute advertisement policy for specific destination

**bgp ecomm-route** – Configures an entry in additive or delete ext community table

**bgp ecomm-peer** – Enables/disables advertisement of ext community attributes to peer

**bgp ecomm-filter** – Allows/filters the ext community attribute while receiving or advertising

**bgp ecomm-policy** – Configures the extended community attribute advertisement policy for specific destination

**bgp confederation identifier** – Specifies the BGP confederation identifier

**bgp confederation peers** – Configures the ASs that belongs to the confederation

**bgp bestpath med confed** – Enables MED comparison among paths learnt from confed peers

**neighbor - password** – Configures the password for TCP-MD5 authentication with peer

**debug ip bgp** – Configures the Trace levels

**show bgp-version** – Displays the BGP Version information

**show ip bgp** – Displays the BGP related information

**show ip bgp community - routes** – Displays routes that belong to specified BGP communities

**show ip bgp extcommunity - routes** – Displays routes that belong to specified BGP extended-communities

**show ip bgp summary** – Displays the status of all BGP4 connections

**show ip bgp filters** – Displays the contents of filter table

**show ip bgp aggregate** – Displays the contents of aggregate table

**show ip bgp med** – Displays the contents of MED table

**show ip bgp dampening** – Displays the contents of dampening table

**show ip bgp local-pref** – Displays the contents of local preference table

**show ip bgp timers** – Displays the value of BGP timers

**show ip bgp info** – Displays the general info about BGP protocol

**show ip bgp rfl info** – Displays info about RFL feature

**show ip bgp confed info** – Displays info about confederation feature

**show ip bgp community** – Displays the contents of community tables

**show ip bgp extcommunity** – Displays the contents of ext-community tables

## 27.2 ip bgp dampening

This command Configures the Dampening Parameters and the “no” form of the command resets the Dampening Parameters to default.

```
ip bgp dampening [<HalfLife-Time> [<Reuse Value> [<Suppress Value>
[<Max-Suppress Time>]]]] [-s <Decay Granularity> [<Reuse Granularity>
[<Reuse Array Size>]]]
```

```
no ip bgp dampening [HalfLife-Time [Reuse-Value [Suppress-Value [Max-
Suppress-Time]]]] [-s [Decay-Granularity [Reuse-Granularity [Reuse-
Array-Size]]]
```

### Syntax Description

**HalfLife-Time** - Time (in seconds) after which a penalty is decreased by half. Once a route has been assigned a penalty, the penalty is decreased by half after the half-life time

**Reuse Value** - If the penalty associated with a suppressed route falls below this value, the route is re-used

**Suppress Value** - A route is suppressed when the penalty associated with the route exceeds this value

**Max-Suppress Time** - Maximum time (in seconds) a route can be suppressed

**Decay Granularity** - Time granularity in seconds used to perform all decay computations

**Reuse Granularity** - Time interval between evaluations of the reuse-lists. Each reuse lists corresponds to an additional time increment

**Reuse Array Size** - Size of reuse index arrays. This size determines the accuracy with which suppressed routes can be placed within the set of reuse lists when suppressed for a long time

### Mode

Global Configuration Mode

### Defaults

HalfLife-Time - 900

Reuse Value - 500

Suppress Value - 3500

Max-Suppress Time - 3600

Decay Granularity - 1

Reuse Granularity - 15

Reuse Array Size - 1024

**Example:**

```
SMIS(config)# ip bgp dampening 100 -s 1 15
```

BGP Speaker Local AS number must be configured.

BGP Administrative status must be DOWN (use Shutdown Command).

**Related Commands**

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp dampening** – Displays the contents of dampening table



## 27.3 ip bgp overlap-policy

This command configures the Overlap Route policy for the BGP Speaker. The “no” form of the command. Resets the Overlap route policy to default. By default, both less and more specific routes are installed.

```
ip bgp overlap-policy <more-specific|less-specific|both>
```

```
no ip bgp overlap-policy
```

### Syntax Description

**more-specific** - This installs only more-specific routes in the RIB

**less-specific** - This installs only less-specific routes in the RIB

**both** - This installs all routes(more-specific and less-specific) in the RIB

### Mode

Global Configuration Mode

### Defaults

Both

### Example:

```
SMIS(config)# ip bgp overlap-policy more-specific
```

BGP Speaker Local AS number must be configured.

BGP Speaker Admin Status must be DOWN

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp info** – Displays the general info about BGP protocol

**shutdown ip bgp** – Sets the BGP Speaker Global Admin status DOWN

**show ip bgp summary** – Displays the status of all BGP4 connections

## 27.4 ip bgp synchronization

This command enables synchronization between BGP and IGP and the "no" form of the command disables synchronization between BGP and IGP.

**ip bgp synchronization**

**no ip bgp synchronization**

### Mode

Global Configuration Mode

### Defaults

Disable

### Example:

```
SMIS(config)# ip bgp synchronization
```

BGP Speaker Local AS number must be configured.

BGP must be administratively down.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp info** – Displays the general info about BGP protocol

**shutdown ip bgp** – Sets the BGP Speaker Global Admin status DOWN

## 27.5 clear ip bgp - Flap-Statistics

This command clears the flap-statistics counters for all paths from the neighbor at the IP address.

```
clear ip bgp <ip-address> flap-statistics
```

### Syntax Description

**ip-address** - IP Address of the peer

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# clear ip bgp 22.0.0.1 flap-statistics
```

The flap statistics are cleared only when routes from the given peer are already flapped.

### Related Commands

**show ip bgp dampened-paths** - Displays the dampened routes

**show ip bgp flap-statistics** - Displays the statistics of flapped routes

## 27.6 bgp router-id

This command configures the BGP Identifier of the BGP Speaker and the "no" form of the command resets the BGP Identifier of the BGP Speaker to default value.

```
bgp router-id <bgp router id (ip-address)>
```

```
no bgp router-id
```

### Mode

Router Configuration Mode

### Defaults

The highest interface address is used as the router id

### Example:

```
SMIS(config-router)# bgp router-id 10.0.0.1
```

Bgp router id is a unique number associated with the BGP speaker. This router-id is advertised to other peers and identifies the BGP speaker uniquely.

Administrator can set the router-id of BGP to any value. If router-id is changed, then all the active peer sessions will go DOWN and will be re-started with the new configured router-id.

BGP Speaker Local AS number must be configured

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp** – Displays the BGP related information

**show ip bgp summary** – Displays the status of all BGP4 connections

## 27.7 bgp default local-preference

This command configures the Default Local Preference value and the "no" form of the command resets the Default Local Preference to its default value.

```
bgp default local-preference <Local Pref Value>
```

```
no bgp default local-preference
```

### Mode

Router Configuration Mode

### Defaults

100

### Example:

```
SMIS(config-router)# bgp default local-preference 100
```

BGP Speaker Local AS number must be configured.

If required administrator can use this command to change this Default Local Preference value

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp info** – Displays the general info about BGP protocol

**show ip bgp summary** – Displays the status of all BGP4 connections

## 27.8 neighbor - remote-as

This command creates a Peer and initiates the connection to the peer and the "no" form of the command disables the peer session and deletes the peer information.

```
neighbor <ip-address> remote-as <AS no(1-65535)>
```

```
no neighbor <ip-address>
```

### Syntax Description

**ip-address** - BGP peer's remote IP address

**remote-as** - Autonomous system to which the BGP peer belongs

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# neighbor 23.45.0.1 remote-as 200
```

BGP Speaker Local AS number must be configured.

The administrator can create a peer and set the peer AS number with this command. This configured peer AS number is compared with the AS number received in the open message and a peer session is initiated only if both the AS numbers match.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**neighbor - password** – Configures the password for TCP-MD5 authentication with peer

**show ip bgp summary** – Displays the status of all BGP4 connections

**show ip bgp** – Displays the BGP related information

## 27.9 neighbor - ebgp-multihop

This command enables BGP to establish connection with external peers that are not directly connected and the "no" form of the command resets the peer EBGP-Multihop status to default. By default, EBGP Multihop is disabled.

```
neighbor <ip-address> ebgp-multihop
```

```
no neighbor <ip-address> ebgp-multihop
```

### Syntax Description

**ip-address** - Peer's Remote IP address

### Mode

Router Configuration Mode

### Defaults

Disable

### Example:

```
SMIS(config-router)# neighbor 23.45.0.1 ebgp-multihop
```

By default external BGP peers need to be directly connected. If external BGP peers are not connected directly, then ebgp-multihop is enabled to initiate the connection with that external peer. If ebgp-multihop is disabled and external BGP peers are indirectly connection, then BGP peer session will not be established BGP Speaker Local AS number must be configured Peer must have been created and peer AS must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp info** – Displays the general info about BGP protocol

## 27.10 neighbor - next-hop-self

This command enables BGP to send itself as the next hop for advertised routes and the "no" form of the command resets the peer nexthop-self status to default. By default, Self Next Hop is disabled.

```
neighbor <ip-address> next-hop-self
```

```
no neighbor <ip-address> next-hop-self
```

### Syntax Description

**ip-address** - The IP address of the BGP peer

### Mode

Router Configuration Mode

### Defaults

By default, the next hop will be generated based on the IP address of the destination and the present next hop in the route information.

### Example:

```
SMIS(config-router)# neighbor 23.45.0.1 next-hop-self
```

The Administrator can use this command to make the BGP speaker fill its address when advertising routes to the BGP peer.

The BGP Speaker Local AS number must be configured

A Peer must have been created and peer AS must be configured

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp info** – Displays the general info about BGP protocol



## 27.11 neighbor - interval

This command configures neighbor interval and the "no" form of the command resets neighbor interval.

```
neighbor <ip-address> {advertisement-interval <seconds> | as-  
originationinterval <seconds> | connect-retry-interval <seconds>}
```

```
no neighbor <ip-address> {advertisement-interval | as-origination-  
interval | connect-retry-interval}
```

### Syntax Description

**ip-address** - Peer ip address

**advertisementinterval** - The time-interval ( in seconds) for spacing advertisement of successive external route-updates to the same destination

**as-originationinterval** - The time-interval (in seconds) for spacing successive route-updates originating within the same AS

**connect-retryinterval** - The time interval (in seconds) after which a transport connection with peer is re-initiated

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# neighbor 23.45.0.1 advertisement-interval 45  
as-origination-interval 30 connect-retry-interval 15
```

The BGP Speaker Local AS number must be configured

A Peerr must have been created and peer AS must be configured

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp info** – Displays the general info about BGP protocol

## 27.12 neighbor - timers

This command configures neighbor KeepAlive Time and Hold Time Intervals and the "no" form of the command resets neighbor KeepAlive Time and Hold Time Intervals.

```
neighbor <ip-address> timers {keepalive <seconds> | holdtime <seconds>}
```

```
no neighbor <ip-address> timers {keepalive | holdtime}
```

### Syntax Description

**ip-address** - Peer IP address

**timers** - Timers.

**keepalive** - keep-alive interval for the peer session. The keep-alive value must always be less than the configured hold-time value

**holdtime** - The hold-time interval for the peer . This is sent in the OPEN message to the peer

### Mode

Router Configuration Mode

### Defaults

Default keep-alive is one-third the value of the Default Hold-time.

### Example:

```
SMIS(config-router)# neighbor 23.45.0.1 timers keepalive 40
```

The BGP Speaker Local AS number must be configured Peer must be created and peer AS must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp info** – Displays the general info about BGP protocol

## 27.13 neighbor - shutdown

This command disables the Peer session and the "no" form of the command enables the Peer session.

```
neighbor <ip-address> shutdown
```

```
no neighbor <ip-address> shutdown
```

### Syntax Description

**ip-address** - Peer ip address

**shutdown** - Terminates the peer session

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# neighbor 23.45.0.1 shutdown
```

BGP Speaker Local AS number must be configured.

Peer must be created and peer AS must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp** – Displays the BGP related information

## 27.14 neighbor - send-community

This command enables advertisement of community attributes to (standard/extended) peer and the "no" form of the command disables advertisement of community attributes to standard/extended) peer.

```
neighbor <ip-address> send-community {both | standard | extended}
```

```
no neighbor <ip-address> send-community {both | standard | extended}
```

### Syntax Description

**ip-address** - Peer IP address

**send-community** - Sends Communities.

**both** - Send both communities and extended communities to peer

**standard** - Send only communities to the peer

**extended** - Send only extended communities to peer

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# neighbor 23.45.0.1 send-community both
```

Peer must be created and peer AS must be configured.

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp community** – Displays the contents of community route/peer/policy/ filter tables

## 27.15 bgp nonbgproute-adv

This command controls the advertisement of Non-BGP routes either to the external peer or both to internal and external peer and the "no" form of the command resets the Non BGP routes adv policy to default. By default, the non BGP routes are advertised to internal and external peers.

```
bgp nonbgproute-adv <external|both>
```

```
no bgp nonbgproute-adv
```

### Syntax Description

**external** - Denotes that the non-BGP routes need to be advertised to external peers

**both** - Determines that the non-BGP routes need to be advertised to both internal and external peers

### Mode

Router Configuration Mode

### Defaults

both

### Example:

```
SMIS(config-router)# bgp nonbgproute-adv both
```

The Administrator can effectively control the advertisement of the route learnt through Redistribution.

BGP Speaker Local AS number must be configured

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp info** – Displays the general info about BGP protocol

## 27.16 redistribute

This command configures the protocol from which the routes have to be redistributed into BGP and the “no” form of the command disables the redistribution of routes from the given protocol into BGP.

```
redistribute <static|connected|rip|ospf|all>
```

```
no redistribute <static|connected|rip|ospf|all>
```

### Syntax Description

**static** - Advertises routes, configured statically, in the BGP routing process

**connected** - Advertises directly connected networks routes, in the BGP routing process

**rip** - Advertises routes, that are learnt by the RIP process, in the BGP routing process

**ospf** - Advertises routes, that are learnt by the BGP process, in the BGP routing process

**all** - Advertises routes, that are learnt by the all processes (RIP ,OSPF, statically configured and connected routes), in the BGP routing process

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# redistribute ospf
```

BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp info** – Displays the general info about BGP protocol

## 27.17 **bgp always-compare-med**

This command enables the comparison of med for routes received from different autonomous system and the “no” form of the command Disables the comparison of med for routes received from different autonomous system. Med will be compared only for routes from same neighbor autonomous system.

**bgp always-compare-med**

**no bgp always-compare-med**

### **Mode**

Router Configuration Mode

### **Defaults**

Disable

### **Example:**

```
SMIS(config-router)# bgp always compare-med
```

The BGP Speaker Local AS number must be configured.

By default in the BGP route selection algorithm, MED attributes are compared between two routes only if both the routes are received from the same autonomous system.

An Administrator can change this default behavior by enabling the always-compare-med option. If this option is enabled, then in the BGP route selection algorithm, MED attributes are compared between routes even if they are received from different autonomous systems.

### **Related Commands**

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp info** – Displays the general info about BGP protocol

## 27.18 default-metric

This command configures the Default IGP Metric value and the “no” form of the command resets the Default IGP Metric value.

```
default-metric <Default Metric Value>
```

```
no default-metric
```

### Mode

Router Configuration Mode

### Defaults

0

### Example:

```
SMIS(config-router)# default-metric 300
```

This command sets the default metric to be associated with all redistributed routes. If a metric value is not supplied, the default metric value is assigned as 0.

If the default metric value is 0, then the received route-metric is advertised. Any non-zero metric value is used as the metric value for all the redistributed routes.

The metric of redistributed Local Routes is not affected by the default-metric value.

The BGP Speaker Local AS number must be configured

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp info** – Displays the general info about BGP protocol



## 27.19 bgp med

This command configures an entry in MED Table and the “no” form of the command deletes the entry from MED Table.

```
bgp med <1-100> remote-as <0-65535> <ip-address> <ip_mask>
[intermediate-as <AS-no list- AS1,AS2,...>] value <value> direction
<in|out> [override]
```

```
no bgp med <1-100>
```

### Syntax Description

**remote-as** - AS number of BGP peer associated with the route-prefix

**ip-address** - Route-prefix on which MED policy needs to be applied

**ip\_mask** - Mask associated with the route

**intermediate-as** - The sequence of intermediate Autonomous system numbers through which the route update is expected to travel

**value** - Value assigned to the MED attribute

**direction** - Direction of application of med policy Incoming - On received route-update with other matching attributes like as-number, intermediate-as numbers Outgoing - On route-update that needs to be advertised to peer

**override** - This setting decides whether configured MED value will override the received MED value

### Mode

Router Configuration Mode

### Defaults

direction - In

med - 0

### Example:

```
SMIS(config-router)# bgp med 5 remote-as 200 212.23.45.0 24
intermediate-as 150 value 50 direction in override
```

Bgp Speaker Local AS number must be configured.

**Related Commands**

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp med** – Displays the contents of MED table

## 27.20 bgp local-preference

This command configures an entry in the Local Preference Table and the “no” form of the command deletes the entry from Local Preference Table.

```
bgp local-preference <1-100> remote-as <0-65535> <ip-address> <ip_mask>  
[intermediate-as <AS-no list- AS1,AS2,...>] value <value> direction  
<in|out> [override]
```

```
no bgp local-preference <1-100>
```

### Syntax Description

**remote-as** - AS number of BGP peer associated with the route-prefix

**ip-address** - Route-prefix on which local-preference policy needs to be applied

**ip\_mask** - Mask associated with the route

**intermediate-as** - The sequence of intermediate Autonomous system numbers through which the route update is expected to travel

**value** - The local-preference value that needs to be associated with the route-update

**direction** - Direction of application of local-preference policy Incoming - On received route-update with other matching attributes like as-number, intermediate-as numbers Outgoing - On route-update that needs to be advertised to peer

**override** - This setting decides whether configured local-preference value overrides the received local-preference value. If this keyword is not specified, then the received value will have precedence over configured value.

### Mode

Router Configuration Mode

### Defaults

remote-as - 0

Direction - in

Value - 100

ip-address - 0.0.0.0

mask - 0

### Example:

```
SMIS(config-router)# bgp local-preference-table index 5 remote-as
```

```
200 21.3.0.0 16 intermediate-as 150 local-pref 250 direction out  
override
```

The BGP Speaker Local AS number must be configured.

### **Related Commands**

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp local-pref** – Displays the contents of local preference table

## 27.21 bgp update-filter

This command configures an entry in Update Filter Table and the “no” form of the command deletes the entry from Update Filter Table.

```
bgp update-filter <1-100> <permit|deny> remote-as <0-65535> <ip-
address> <ip_mask> [intermediate-as <AS-no list-AS1,AS2,...>] direction
<in|out>
```

```
no bgp update-filter <1-100>
```

### Syntax Description

**permit** - Allow route to pass filter policy test

**deny** - Filter routes when it passes through filter policy test

**remote-as** - AS number of BGP peer associated with the route-prefix

**ip-address** - Route-prefix on which Filter policy needs to be applied

**ip\_mask** - Mask associated with the route-prefix

**intermediate-as** - The sequence of intermediate Autonomous system numbers through which the route update is expected to travel

**direction** - Direction of application of med policy

**in** - On received route-update with other matching attributes like as-number, intermediate-as nos

**out** - On route-update that needs to be advertised to peer

### Mode

Router Configuration Mode

### Defaults

remote-as - 0

direction - In

prefix - 0.0.0.0

prefixlen - 0

action - filter

### Example:

```
SMIS(config-router)# bgp update-filter 6 deny remote-as 145
72.93.0.0 255.255.0.0 intermediate-as 150 direction in
```

The BGP Speaker Local AS number must be configured

### **Related Commands**

`router bgp` – Sets the AS number of the BGP Speaker

`show ip bgp filters` – Displays the contents of filter table

## 27.22 aggregate-address index

This command configures an entry in Aggregate Table and the “no” form of the command deletes the entry from Aggregate Table.

```
aggregate-address index <1-100> <ip-address> <ip_mask> [summary-only]
```

```
no aggregate-address index <1-100>
```

### Syntax Description

**ip-address** - The Aggregate address

**ip\_mask** - The mask associated with the aggregated route

**summary-only** - Creates an aggregated route for advertisement to peers and also suppresses the advertisement of more-specific routes to the peers

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# aggregate-address index 1 21.1.0.0 16 summary-only
```

The BGP Speaker Local AS number must be configured.

This command configures the (aggregation policy) route details for forming an aggregated route and creates an entry in the aggregation table. When summaryonly is given, then, aggregated route alone will be sent to the peers. Otherwise, both more-specific and aggregated route are advertised.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp aggregate** – Displays the contents of aggregate table

## 27.23 bgp cluster-id

This command configures the Cluster ID for Route Reflector and the “no” form of the command resets the Cluster ID for Route Reflector.

```
bgp cluster-id <cluster id value(ip_address)>
```

```
no bgp cluster-id
```

### Syntax Description

**cluster id value** - The cluster Id associated with the route-reflector

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp cluster-id 10.0.0.1
```

BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp rfl info** – Displays info about RFL feature



## 27.24 bgp client-to-client reflection

This command configures the Route Reflector to support route reflection to Client Peers and the “no” form of the command configures the Route Reflector not to reflect routes to Client Peers.

**bgp client-to-client reflection**

**no bgp client-to-client reflection**

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp client-to-client reflection
```

The BGP Speaker Local AS number must be configured.

The BGP Cluster-id must be configured.

By default, Route Reflector will reflect routes learned from a client peer to all other client peers. If required, administrator can disable this feature by disabling client-to-client reflection. If disabled, then Route Reflector will not advertise routes learnt from a client peer to other client peers. This occurs when all peers within a cluster are fully-meshed and the client peer itself is able to advertise routes to other clients of the route-reflector

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp rfl info** – Displays info about RFL feature

## 27.25 neighbor - route-reflector-client

This command configures the Peer as Client of the Route Reflector and the “no” form of the command resets the Peer as conventional BGP Peer.

```
neighbor <ip-address> route-reflector-client
```

```
no neighbor <ip-address> route-reflector-client
```

### Syntax Description

**ip-address** - Peer's Remote IP address

**route-reflectorclient** - Specifies the BGP peer as a client of the Route-Reflector

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# neighbor 23.45.0.1 route-reflector-client
```

The BGP Speaker Local AS number must be configured.

Route Reflector must be enabled.

Peer must be created and peer AS must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp rfl info** – Displays info about RFL feature

## 27.26 bgp comm-route

This command configures an entry in additive or delete community table and the “no” form of the command removes the entry from additive or delete community table.

```
bgp comm-route {additive|delete} <ip-address> <ip_mask> comm-value  
<4294967041-4294967043,65536-4294901759>  
no bgp comm-route {additive|delete} <ip-address> <ip_mask> comm-value  
<4294967041-4294967043,65536-4294901759>
```

### Syntax Description

**additive** - Add associated community value with the already existing communities in the route update

**delete** - Remove the community attribute from the route-prefix when it passes through the filter process

**ip-address** - Route prefix on which community policy needs to be applied

**ip\_mask** - Mask associated with the route-prefix

**comm-value** - Community attribute value

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp comm-route-table 24.5.0.0 16 commvalue  
4294967045
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp community** – Displays the contents of route/peer/filter/policy community tables

## 27.27 bgp comm-peer

This command enables/disables advertisement of community attributes to peer and the “no” form of the command disables advertisement of community attributes to peer.

```
bgp comm-peer <ip-address> <permit|deny>
```

```
no bgp comm-peer <ip-address>
```

### Syntax Description

**ip-address** - Route prefix on which community policy needs to be applied

**permit** - Allow advertisement of community attributes to peer

**deny** - Filters advertisement of community attributes to peer

### Mode

Router Configuration Mode

### Defaults

Deny

### Example:

```
SMIS(config-router)# bgp comm-peer 23.45.0.1 deny
```

BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp community** – Displays the contents of route/peer/filter/policy community tables

## 27.28 bgp comm-filter

This command allows/filters the community attribute while receiving or advertising. The “no” form of the command removes the filter policy for the community attribute.

```
bgp comm-filter <comm-value (4294967041-4294967043,65536-4294901759)>  
<permit|deny> <in|out>
```

```
no bgp comm-filter <comm-value (4294967041-4294967043,65536-4294901759)>  
<permit|deny> <in|out>
```

### Syntax Description

**comm.-value** - Community Attribute Value

**permit** - Allows a particular community attribute to be received or advertised in updates

**deny** - Filters routes containing the community attribute value in received or advertised updates

**in|out** - Specifies the direction of route-updates on which the community filter policy needs to be applied, i.e. whether the community filter needs to be applied on received routes or on routes advertised to peers

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp comm-filter 75100 deny in
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp community** – Displays the contents of route/peer/filter/policy community tables

## 27.29 bgp comm-policy

This command configures the community attribute advertisement policy for specific destination. The “no” form of the command removes the community attribute advertisement policy for specific destination.

```
bgp comm-policy <ip-address> <ip_mask> <set-add|set-none|modify>
```

```
no bgp comm-policy <ip-address> <ip_mask>
```

### Syntax Description

**ip-address** - Route prefix on which community policy needs to be applied

**ip-mask** - Mask associated with the ip address

**set-add** - Sends only the configured additive communities with associated route

**set-none** - Sends the associated route without any communities

**modify** - Removes the associated route with received delete communities and adds the configured additive communities

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp comm-policy
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp community** – Displays the contents of route/peer/filter/policy community tables

## 27.30 bgp ecomm-route

This command configures an entry in additive or delete ext community table. The “no” form of the command removes the entry from additive or delete ext community table.

```
bgp ecomm-route {additive|delete} <ip-address> <ip_mask> ecomm-value  
<value (xx:xx:xx:xx:xx:xx:xx:xx)>
```

```
no bgp ecomm-route {additive|delete} <ip-address> <ip_mask> ecomm-value  
<value (xx:xx:xx:xx:xx:xx:xx:xx)>
```

### Syntax Description

**additive** - Adds associated extended-community value with the already existing communities in the route update

**delete** - Removes the extended-community attribute from the route-prefix when it passes through the filter process

**ip-address** - Route prefix on which extended-community policy needs to be applied

**ip\_mask** - Mask associated with the ip address

**ecomm-value** - Extended Community Attribute Value

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp ecomm-route additive 12.0.0.0 255.0.0.0  
ecomm-value 01:01:22:33:44:55:66:77
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp extcommunity** – Displays the contents of route/peer/filter/policy ext-community route tables





## 27.31 bgp ecomm-peer

This command enables/disables advertisement of ext community attributes to peer. The “no” form of the command disables advertisement of ext community attributes to peer.

```
bgp ecomm-peer <ip-address> <permit|deny>
```

```
no bgp ecomm-peer <ip-address>
```

### Syntax Description

**ip-address** - IP address of the peer

**permit** - Allows advertisement of ext community attributes to peer

**deny** - Denies advertisement of ext community attributes to peer

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp ecomm-peer 10.0.0.2 permit
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp extcommunity** – Displays the contents of route/peer/filter/policy ext-community route tables

## 27.32 bgp ecomm-filter

This command allows/filters the ext community attribute while receiving or advertising. The “no” form of the command removes the filter policy for the ext community attribute.

```
bgp ecomm-filter <ecomm-value (xx:xx:...:xx)> <permit|deny> <in|out>
```

```
no bgp ecomm-filter <ecomm-value (xx:xx:...:xx)> <permit|deny> <in|out>
```

### Syntax Description

**ecomm-value** - The extended community value

**permit** - Allows the route -update with the associated extended community value to pass the filter test

**deny** - Denies the route-update with the associated extended community value to pass the filter test

**in** - Incoming direction of applied filter

**out** - Outgoing direction of applied filter

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp ecomm-filter 01:01:22:33:23:43:44:22 deny
in
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp extcommunity** – Displays the contents of route/peer/filter/policy ext-community route tables

## 27.33 bgp ecomm-policy

This command configures the extended community attribute advertisement policy for specific destination.

The “no” form of the command removes the extended community attribute advertisement policy for specific destination.

```
bgp ecomm-policy <ip-address> <ip_mask> <set-add|set-none|modify>
```

```
no bgp ecomm-policy <ip-address> <ip_mask>
```

### Syntax Description

**ip-address** - The route prefix on which extended community policy needs to be applied

**ip\_mask** - The mask associated with the ip address

**set-add** - Sends associated route with configured additive extended-communities only

**set-none** - Sends the associated route without any extendedcommunities

**modify** - Strips the associated route with received delete extended communities and adds the configured additive extended communities

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp ecomm-policy 12.0.0.0 255.0.0.0 setadd
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp extcommunity** – Displays the contents of route/peer/filter/policy ext-community route tables

## 27.34 bgp confederation identifier

This command specifies the BGP confederation identifier. The “no” form of the command removes the BGP confederation identifier.

```
bgp confederation identifier <AS no(1-65535)>
```

```
no bgp confederation identifier
```

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp confederation identifier 1000
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp confed info** – Displays info about confederation feature

## 27.35 bgp confederation peers

This command configures the ASs that belongs to the confederation. The “no” form of the command removes the ASs from the confederation.

```
bgp confederation peers <AS no(1-65535)>
```

```
no bgp confederation peers <AS no(1-65535)>
```

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp confederation peers 100
```

The BGP Speaker Local AS number must be configured.

The peer AS number must not be equal to BGP Speaker Local AS number

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp confed info** – Displays info about confederation feature

## 27.36 bgp bestpath med confed

This command enables MED comparison among paths learnt from confed peers. The “no” form of the command disables MED comparison among paths learnt from confed peers.

**bgp bestpath med confed**

**no bgp bestpath med confed**

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# bgp bestpath med confed
```

The BGP Speaker Local AS number must be configured.

By default, in BGP route selection algorithm, MED attributes comparison between two routes originated within the local confederation is disabled. Enabling this option, will allow the router to compare MED attribute between routes originated from the local confederation.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**show ip bgp confed info** – Displays info about confederation feature

## 27.37 neighbor - password

This command configures the password for TCP-MD5 authentication with peer. The “no” form of the command resets the TCP-MD5 password set for the peer.

```
neighbor <ip-address> password <password-string>
```

```
no neighbor <ip-address> password
```

### Syntax Description

**ip-address** - IP address of the BGP peer

**password** - The password that needs to be used for TCP-MD5 authentication with the peer

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# neighbor 10.0.0.2 password abcdef
```

The BGP Speaker Local AS number must be configured.

Peer must have been created.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**neighbor - remote-as** – Creates a Peer and initiates the connection to the peer

**show ip bgp info** – Displays the general info about BGP protocol

## 27.38 clear ip bgp

This command resets the bgp connection dynamically for inbound and outbound route policy.

```
clear ip bgp {* | <ip-address>} [soft {in|out}]
```

### Syntax Description

**\*** - All BGP peers

**ip-address** - Remote IP address associated with specific BGP peer

**soft** - Soft clear

**in** - Initiates inbound soft reconfiguration

**out** - Initiates outbound soft configuration

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# clear ip bgp
```

If the keyword **soft** and the associated direction are not specified, then this causes hard clear i.e. the BGP session with peer is reset.

### Related Command

**show ip bgp** – Displays the BGP related information



## 27.39 shutdown ip bgp

T

This command sets the BGP Speaker Global Admin status DOWN and the “no” form of the command sets the BGP Speaker Global Admin status UP.

```
shutdown ip bgp
```

```
no shutdown ip bgp
```

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# shutdown ip bgp
```

The shutdown command does not affect all the configurations. All peer sessions go down and routes learned through redistribution are lost. If RFD is enabled, then routes history is cleared.

### Related Commands

**ip bgp overlap-policy** – Configures the Overlap Route policy for the BGP Speaker

**ip bgp synchronization** – Enables synchronization between BGP and IGP

**show ip bgp info** – Displays the general info about BGP protocol

## 27.40 debug ip bgp

This command configures the Trace levels. The “no” form of the command resets the Trace levels.

```
debug ip bgp {peer | update | fdb | keep | in | out | damp | events |  
all }
```

```
no debug ip bgp {peer | update | fdb | keep | in | out | damp | events  
| all}
```

### Syntax Description

**peer** - Trace code related to peer processing  
**update** - Trace code related to update processing  
**fdb** - Trace code related to FIB updation  
**keep** - Trace code related to keep-alives  
**in** - Trace code related to incoming messages  
**out** - Trace code related to outgoing messages  
**damp** - Trace code related to dampening parameters  
**events** - Trace code related to BGP event processing  
**all** - All the BGP trace code

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# debug ip bgp peer
```

The BGP Speaker Local AS number must be configured.

### Related Command

**router bgp** – Sets the AS number of the BGP Speaker

## 27.41 show bgp-version

This command displays the BGP Version information.

**show bgp-version**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show bgp-version
```

```
show output Future BGP Version : 4
```

BGP Speaker Local AS number must be configured.

### Related Command

**router bgp** – Sets the AS number of the BGP Speaker

## 27.42 show ip bgp

This command displays the BGP related information.

```
show ip bgp {[neighbor [<peer-addr>]] | rib}
```

### Syntax Description

**neighbor** - IP address of the neighbor

**rib** - BGP local RIB (Routing Information Base)

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp neighbor 10.0.0.2
BGP neighbor is 10.0.0.2, remote AS 200, external link
BGP version 4, remote router ID 10.0.0.2
BGP state = Established, up for 21 minutes 26 seconds
Rcvd update before 0 secs, hold time is 120, keepalive
interval is 24 secs
Neighbors Capability:
Route-Refresh: Advertised and received
Address family IPv4 Unicast: Advertised and received
Received 44 messages, 0 Updates
Sent 56 messages, 5 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 300 seconds
Connections established 1 time(s)
Local host: 10.0.0.1, Local port: 179
Foreign host: 10.0.0.2, Foreign port: 49152
Last Error: Code 0, SubCode 0.
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**bgp router-id** – Configures the BGP Identifier of the BGP Speaker

**neighbor - shutdown** – Disables the Peer session

**neighbor - remote-as** – Creates a Peer and initiates the connection to the peer

**clear ip bgp** – Resets the BGP connection dynamically for inbound and outbound route policy

## 27.43 show ip bgp community - routes

This command displays routes that belong to specified BGP communities.

```
show ip bgp community community-number (4294967041-4294967043, 65536-4294901759) [exact]
```

### Syntax Description

**community-number** - BGP Community attribute

**exact** - Displays the routes that has the same specified communities

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp community 75000
BGP table version is 5, local router ID is 10.0.0.2
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Path
-----
76.0.0.0/8 10.0.0.1 1 100
77.0.0.0/8 10.0.0.1 1 100
78.0.0.0/8 10.0.0.1 1 100
```

```
SMIS# show ip bgp community 75000 exact
BGP table version is 5, local router ID is 10.0.0.2
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Path
-----
76.0.0.0/8 10.0.0.1 1 100
77.0.0.0/8 10.0.0.1 1 100
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**bgp comm-policy** – Configures the community attribute advertisement policy for specific destination

**bgp comm-filter** – Allows/filters the community attribute while receiving or advertising

**bgp comm-peer** – Enables/disables advertisement of community attributes to peer

**bgp comm-route** – Configures an entry in additive or delete community table

## 27.44 show ip bgp extcommunity - routes

This command displays routes that belong to specified BGP extended-communities.

```
show ip bgp extcommunity <value (xx:xx:xx:xx:xx:xx:xx:xx)> [exact]
```

### Syntax Description

**exact** - Displays the routes that has the same specified extended communities

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp extcommunity 01:02:33:33:33:33:33:33
BGP table version is 5,local router ID is 10.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Path
-----
75.0.0.0/8 10.0.0.1 1 100
79.0.0.0/8 10.0.0.1 1 100
```

```
SMIS# show ip bgp extcommunity 01:02:33:33:33:33:33:33 exact
BGP table version is 5,local router ID is 10.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Path
-----
75.0.0.0/8 10.0.0.1 1 100
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**bgp ecomm-route** – Configures an entry in additive or delete extended community table



**bgp ecomm-peer** – Enables/disables advertisement of extended community attributes to peer

**bgp ecomm-filter** – Allows/filters the extended community attribute while receiving or advertising

**bgp ecomm-policy** – Configures the extended community attribute advertisement policy for specific destination

## 27.45 show ip bgp summary

This command displays the status of all BGP4 connections.

**show ip bgp summary**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp summary
BGP router identifier is 10.0.0.1, local AS number 100
BGP table version is 5
Neighbor Version AS MsgRcvd MsgSent Up/Down State/PfxRcd
-----
10.0.0.2 4 200 44 56 00:00:21:26 Established
10.0.0.3 4 100 0 0 - Idle
10.0.0.4 4 100 0 0 - Idle
10.0.0.6 4 600 0 0 - Connect
10.0.0.7 4 700 0 0 - Connect
10.0.0.8 4 800 0 0 - Connect
```

The BGP Speaker Local AS number must be configured.

### Related Commands

- router bgp** – Sets the AS number of the BGP Speaker
- ip bgp dampening** – Configures the Dampening Parameters
- ip bgp overlap-policy** – Configures the Overlap Route policy for the BGP Speaker
- bgp router-id** – Configures the BGP Identifier of the BGP Speaker
- bgp default local-preference** – Configures the Default Local Preference value
- neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- no ip bgp overlap-policy** – Resets the Overlap route policy to default

## 27.46 show ip bgp filters

This command displays the contents of filter table.

**show ip bgp filters**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp filters
```

```
Index Admin Remote-AS PrefixLen Inter-AS Direction Action  
Status Prefix
```

```
-----  
1 up 500 12.0.0.0 8 555,444 out allow  
2 up 500 15.0.0.0 8 - in filter  
3 up 500 18.0.0.0 8 555,444 out allow  
4 up 500 19.0.0.0 8 888 in filter
```

The BGP Speaker Local AS number must be configured.

### Related Command

**bgp update-filter** – Configures an entry in Update Filter Table

## 27.47 show ip bgp aggregate

This command displays the contents of aggregate table.

**show ip bgp aggregate**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp aggregate
Index AdminStatus Prefix PrefixLen Advertise
-----
1 up 10.0.0.0 8 all
2 up 20.0.0.0 8 summary-only
3 up 50.0.0.0 8 all
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**aggregate-address index** – Configures an entry in Aggregate Table

## 27.48 show ip bgp med

This command displays the contents of MED table.

**show ip bgp med**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp med
```

```
Index Admin Remote Prefix Prefix Inter Direction Value Preference  
Status -AS Len -AS
```

```
-----  
1 up 300 77.0.0.0 8 556,664 in 400 true
```

```
2 up 400 78.0.0.0 8 - out 500 false
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**bgp med** – Configures an entry in MED Table

**bgp bestpath med confed** – Enables MED comparison among paths learnt from confed peers

## 27.49 show ip bgp dampening

This command displays the contents of dampening table.

**show ip bgp dampening**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp dampening
Half Life Time is 900
Reuse value is 500
Suppress value is 3500
Max Suppress time is 3600
Decay timer granularity is 1
Reuse timer granularity is 15
Reuse index array size is 1024
```

The BGP Speaker Local AS number must be configured.

### Related Command

**ip bgp dampening** – Configures the Dampening Parameters

## 27.50 show ip bgp local-pref

This command displays the contents of local preference table.

```
show ip bgp local-pref
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp local-pref
```

```
Index Admin Remote Prefix Prefix Inter Direction Value Preference
Status -AS Len -AS
```

```
-----
```

```
1 up 300 22.0.0.0 8 555,666 in 400 true
```

```
2 up 400 23.0.0.0 8 - out 500 false
```

```
3 up 400 27.0.0.0 8 - in 700 false
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**bgp default local-preference** – Configures the Default Local Preference value

**bgp local-preference** – Configures an entry in Local Preference Table

## 27.51 show ip bgp timers

This command displays the value of BGP timers.

```
show ip bgp timers
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp timers
```

```
Peer Timers
```

```
Peer Address Holdtime KeepAliveTime ConnectRetry ASOrig RouteAdvt
```

```
-----
```

```
10.0.0.2 500 100 400 350 300
```

```
10.0.0.3 120 30 30 15 30
```

```
10.0.0.4 120 30 30 15 30
```

```
10.0.0.6 120 30 30 15 30
```

```
10.0.0.7 120 30 30 15 30
```

```
10.0.0.8 120 30 30 15 30
```

The BGP Speaker Local AS number must be configured.

### Related Command

**ip bgp dampening** – Configures the Dampening Parameters



## 27.52 show ip bgp info

This command displays the general info about BGP protocol.

**show ip bgp info**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp info
Routing Protocol is "bgp 100"
IGP synchronization is disabled
Routing Protocol is bgp 100
Both more-specific and less-specific overlap route policy is set
Local Preference is 100
Non-bgp routes are advertised to both external and internal peers
MED Comparision is disabled
Metric is 0
Redistributing:static
Peer Table
Peer Address RemoteAS NextHop MultiHop
-----
10.0.0.2 200 self enable
10.0.0.3 100 automatic disable
10.0.0.4 100 automatic disable
10.0.0.6 600 automatic disable
10.0.0.7 700 automatic disable
10.0.0.8 800 automatic disable
TCPMD5 Auth Table
Peer Address Password
-----
10.0.0.2 qwert
10.0.0.3 asdfg
10.0.0.4 zxcvb
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**router bgp** – Sets the AS number of the BGP Speaker

**ip bgp overlap-policy** – Configures the Overlap Route policy for the BGP Speaker

**ip bgp synchronization** – Enables synchronization between BGP and IGP

**bgp default local-preference** – Configures the Default Local Preference value

**neighbor - ebgp-multihop** – Enables BGP to establish connection with external peers

**neighbor - next-hop-self** – Enables BGP to send itself as the next hop for advertised routes

**neighbor - interval** – Configures neighbor interval

**neighbor - timers** – Configures neighbor KeepAlive Time and Hold Time Intervals

**bgp nonbgproute-advt** – Controls the advertisement of Non-BGP routes

**redistribute** – Configures the protocol from which the routes have to be redistributed into BGP

**bgp always-compare-med** – Enables the comparison of med for routes received from different autonomous system

**default-metric** – Configures the Default IGP Metric value

**neighbor - password** – Configures the password for TCP-MD5 authentication with peer

**shutdown ip bgp** – Sets the BGP Speaker Global Admin status DOWN

## 27.53 show ip bgp rfl info

This command displays information about RFL feature.

```
show ip bgp rfl info
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp rfl info
Cluster id is 10.0.0.1
Desired Support of the route reflector - Client Support
BGP Peer Extension Table
Peer Address Client/Non-Client
----
10.0.0.2 Non-client
10.0.0.3 Non-client
10.0.0.4 Client
10.0.0.6 Non-client
10.0.0.7 Non-client
10.0.0.8 Non-client
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**bgp nonbgproute-adv** – Controls the advertisement of Non-BGP routes either to the external

peer (1) or both to internal & external peer (2)

**bgp client-to-client reflection** – Configures the Route Reflector to support route reflection to Client Peers

**neighbor - route-reflector-client** – Configures the Peer as Client of the Route Reflector

**bgp cluster-id** – Configures the Cluster ID for Route Reflector

## 27.54 show ip bgp confed info

This command displays info about confederation feature.

```
show ip bgp confed info
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp confed info
Confederation Identifier is 1000
Confederation best path med comparison is not set
Confederation peers: 200 300 400
```

The BGP Speaker Local AS number must be configured.

### Related Commands

**bgp confederation identifier** – Specifies the BGP confederation identifier

**bgp bestpath med confed** – Enables MED comparison among paths learnt from confed peers

**bgp confederation peers** – Configures the ASs that belongs to the confederation

## 27.55 show ip bgp community

This command displays the contents of community tables.

```
show ip bgp community {route|peer|policy|filter}
```

### Syntax Description

**route** - Entry in additive or delete community table

**peer** - Advertisement of community attributes to peer

**policy** - Community attribute advertisement policy for specific destination

**filter** - Filters the community attribute while receiving or advertising

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp community route
```

```
Additive Community Table
```

```
Prefix PrefixLen AddCommVal
```

```
-----
```

```
30.0.0.0 8 70000
```

```
60.0.0.0 8 75000
```

```
75.0.0.0 8 70000
```

```
76.0.0.0 8 75000
```

```
77.0.0.0 8 75000
```

```
78.0.0.0 8 75000
```

```
78.0.0.0 8 76000
```

```
Delete Community Table
```

```
Prefix PrefixLen DeleteCommVal
```

```
-----
```

```
40.0.0.0 8 80000
```

```
70.0.0.0 8 85000
```

```
SMIS# show ip bgp community filter
```

```
Incoming Filter Table
```

```
CommValue FilterStatus
```

```
-----
```

```
70000 accept
80000 deny
Outgoing Filter Table
CommValue FilterStatus
-----
```

```
75000 accept
85000 deny
```

```
SMIS# show ip bgp community policy
Community Policy Table
Prefix PrefixLen SendStatus
-----
20.0.0.0 8 set-add
30.0.0.0 8 set-none
40.0.0.0 8 modify
```

```
SMIS# show ip bgp community peer
Community Peer Table
IpAddress SendStatus
-----
10.0.0.2 send
10.0.0.3 donotsend
10.0.0.6 send
10.0.0.8 send
```

The BGP Speaker Local AS number must be configured.

**Related Commands**

- bgp comm-route** – Configures an entry in additive or delete community table
- bgp comm-peer** – Enables/disables advertisement of community attributes to peer
- bgp comm-filter** – Allows/filters the community attribute while receiving or advertising
- bgp comm-policy** – Configures the community attribute advertisement policy for specific destination
- neighbor - send-community** – Enables advertisement of community attributes to (standard/extended) peer

## 27.56 show ip bgp extcommunity

This command displays the contents of ext-community tables.

```
show ip bgp extcommunity {route|peer|policy|filter}
```

### Syntax Description

**route** - Entry in additive or delete ext community table

**peer** - Advertisement of ext community attributes to peer

**policy** - Extended community attribute advertisement policy for specific destination

**filter** - Filters the ext community attribute while receiving or advertising

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp extcommunity route
```

```
Additive Ext-Community Table
```

```
Prefix PrefixLen AddEcommVal
```

```
-----
```

```
30.0.0.0 8 1:1:22:33:44:55:66:77
```

```
60.0.0.0 8 1:1:22:33:44:55:66:88
```

```
75.0.0.0 8 1:1:33:33:33:33:33:33
```

```
76.0.0.0 8 1:2:44:33:33:33:33:33
```

```
78.0.0.0 8 1:2:33:33:33:33:33:33
```

```
78.0.0.0 8 1:2:33:33:33:33:33:44
```

```
79.0.0.0 8 1:2:33:33:33:33:33:44
```

```
79.0.0.0 8 1:2:33:33:33:33:33:33
```

```
Delete Ext-Community Table
```

```
Prefix PrefixLen DeleteEcommVal
```

```
-----
```

```
40.0.0.0 8 1:1:55:33:44:55:66:77
```

```
70.0.0.0 8 1:1:22:33:44:55:66:99
```

```
SMIS# show ip bgp extcommunity filter
```

```
Incoming Filter Table
```

```
EcommValue FilterStatus
```

```
-----  
1:1:22:33:44:55:34:77 deny  
1:1:22:33:44:55:66:77 accept  
Outgoing Filter Table  
EcommValue FilterStatus  
-----  
1:1:22:33:44:55:99:77 accept  
1:1:44:33:77:66:99:56 deny
```

```
SMIS# show ip bgp extcommunity policy  
Community Policy Table  
Prefix PrefixLen SendStatus  
-----  
20.0.0.0 8 set-add  
30.0.0.0 8 set-none  
40.0.0.0 8 modify
```

```
SMIS# show ip bgp extcommunity peer  
Ext-Community Peer Table  
IpAddress SendStatus  
-----  
10.0.0.2 send  
10.0.0.3 donotsend  
10.0.0.8 send
```

The BGP Speaker Local AS number must be configured.

**Related Commands**

- bgp ecomm-route** – Configures an entry in additive or delete ext community table
- bgp ecomm-peer** – Enables/disables advertisement of ext community attributes to peer
- bgp ecomm-filter** – Allows/filters the ext community attribute while receiving or advertising
- bgp ecomm-policy** – Configures the extended community attribute advertisement policy for specific destination



## 27.57 show ip bgp dampened-paths

This command displays the dampened routes.

**show ip bgp dampened-paths**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp dampened-paths
Status codes: s suppressed, d damped, * valid
Network From LastUpdt Path
-----
65.0.0.0 22.0.0.1 00:5:5:1 100
60.0.0.0 22.0.0.1 00:4:15:1 100
80.0.0.0 23.0.0.2 00:4:11:41 300
```

### Related Commands

**clear ip bgp - Flap-Statistics** - Clears the flap-statistics counters for all paths from the neighbor at the IP address

## 27.58 show ip bgp flap-statistics

This command displays the statistics of flapped routes.

```
show ip bgp flap-statistics [<ip-address><Mask>]
```

### Syntax Description

**ip-address** - IP Address of the Route

**Mask** - Subnet Mask

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ip bgp flap-statistics
Status codes: s suppressed, d damped, * valid
Network From Flaps LastUpdt Path
----- ----
65.0.0.0 22.0.0.1 1 00:5:5:1 100
60.0.0.0 22.0.0.1 4 00:4:15:1 100
80.0.0.0 23.0.0.2 3 00:4:11:41 300
```

### Related Commands

**clear ip bgp - Flap-Statistics** - Clears the flap-statistics counters for all paths from the neighbor at the IP address

## 28 IPv6

IPv6 is a new version of IP which is designed to be an evolutionary step from IPv4. It can be installed as a normal software upgrade in Internet devices and is interoperable with the current IPv4. It has expanded routing and addressing capabilities because of the 128 bit addressing as compared to the 32 bit addressing in IPv4. Its deployment strategy is designed to not have any flag days or other dependencies. IPv6 is designed to run well on high performance networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) and at the same time still be efficient for low bandwidth networks (e.g. wireless). In addition, it provides a platform for new Internet functionality that will be required in the near future.

IPv6 includes a transition mechanism, which is designed to allow users to adopt and deploy IPv6 in a highly diffuse fashion and to provide direct interoperability between IPv4 and IPv6 hosts. The IPv6 transition allows the users to upgrade their hosts to IPv6, and the network operators to deploy IPv6 in routers, with very little coordination between the two.

The changes from IPv4 to IPv6 fall primarily into the following categories

- Expanded Routing and Addressing Capabilities
- Usage of anycast address
- Header Format Simplification
- Improved Support for Options
- Quality-of-Service Capabilities
- Authentication and Privacy Capabilities

The list of CLI commands for the configuration of IPv6 is as follows:

[ipv6 enable](#)

[ipv6 unicast-routing](#)

[ipv6 - address](#)

[ipv6 - link local address](#)

[ipv6 - static routes](#)

[ipv6 - neighbor](#)

[ipv6 nd suppress-ra](#)

[ipv6 nd managed-config flag](#)

[ipv6 nd other-config flag](#)

[ipv6 hop-limit](#)

[ipv6 nd ra-lifetime](#)

[ipv6 nd dad attempts](#)

[ipv6 nd reachable-time](#)

[ipv6 nd retrans-time](#)

[ipv6 nd ra-interval](#)

[ipv6 nd prefix](#)

[show ipv6 interface](#)

[show ipv6 route](#)

[show ipv6 route summary](#)

[show ipv6 neighbors](#)

[ping ipv6](#)

[debug ipv6](#)

[traceroute](#)

[clear ipv6 neighbors](#)

[clear ipv6 traffic](#)

[clear ipv6 route](#)

## 28.1 `ipv6 enable`

This command enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address. The “no” form of the command disables IPv6 processing on the interface that has not been configured with an explicit IPv6 address.

`ipv6 enable`

`no ipv6 enable`

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# ipv6 enable
```

IPv6 is enabled on the default VLAN interface.

### Related Commands

`ipv6 - address` – Configures IPv6 address on the interface

`show ipv6 interface` – Displays the IPv6 interfaces

## 28.2 ipv6 unicast-routing

This command enables unicast routing. The “no” form of the command disables unicast routing.

**ipv6 unicast-routing**

**no ipv6 unicast-routing**

### **Mode**

Global Configuration Mode

### **Defaults**

Enabled

### **Example:**

```
SMIS(config)# ipv6 unicast-routing
```

## 28.3 ipv6 - address

This command configures IPv6 address on the interface. The “no” form of the command deletes the configured IPv6 address.

```
ipv6 address <prefix> <prefix Len> [{unicast | anycast | eui64}]
```

```
no ipv6 address <prefix> <prefix Len> [{unicast | anycast | eui64}]
```

### Syntax Description

**prefix** - IPv6 prefix for the interface

**prefix Len** - IPv6 prefix length

**unicast** - Unicast type of Prefix

**anycast** - Anycast type of Prefix

**eui64** - Type of Prefix where the latter 64 bits are formed from the link layer address

### Mode

Interface Configuration Mode

### Defaults

unicast

### Example:

```
SMIS(config-if)# ipv6 address 3333::1111 64 unicast
```

The prefix length for eui64 type must be 64.

### Related Command

**show ipv6 interface** – Displays the IPv6 interfaces

## 28.4 ipv6 - link local address

This command configures the IPv6 link-local address on the interface. The “no” form of the command deletes the configured IPv6 link-local address.

```
ipv6 address <prefix> link-local
```

```
no ipv6 address <prefix> link-local
```

### Syntax Description

**prefix** - IPv6 Prefix for the interface

**link-local** - Type of address

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ipv6 address fe80::2222 link-local
```

The prefix specified must be a valid link-local prefix.

### Related Command

**show ipv6 interface** – Displays the IPv6 interfaces



## 28.5 ipv6 - static routes

This command configures static routes. The “no” form of the command deletes the configured static routes.

```
ipv6 route <prefix> <prefix len> ([<NextHop>] {[vlan <id>}])  
[<administrative distance>] [unicast]
```

```
no ipv6 route <prefix> <prefix Len> {<NextHop>| {vlan <id>}}  
[<administrative distance>] [unicast]
```

### Syntax Description

**prefix** - IPv6 Prefix of the destination

**prefix Len** - Destination prefix length

**Next-Hop** - IPv6 prefix of the next hop that is used to reach the destination network

**vlan** - VLAN Identifier

**administrative distance** - Metric to reach the destination

**unicast** - Unicast type of prefix

### Mode

Global Configuration Mode

### Defaults

administrative distance – 1 unicast

### Example:

```
SMIS(config)# ipv6 route 2111::1111 64 3111::1111
```

A Route will be configured only when a proper route exists for the next-hop prefix in the route table.

### Related Commands

**ipv6 - link local address** – Configures the IPv6 link-local address on the interface

**show ipv6 route** – Displays the IPv6 Routes

## 28.6 ipv6 - neighbor

This command configures a static entry in the IPv6 neighbor cache table. The “no” form of the command removes the static entry from the IPv6 neighbor cache table.

```
ipv6 neighbor <prefix> {vlan <id> } <MAC ADDRESS (xx:xx:xx:xx:xx:xx)>
```

```
no ipv6 neighbor <prefix> {vlan <id>} <MAC ADDRESS  
(xx:xx:xx:xx:xx:xx)>
```

### Syntax Description

**prefix** - IPv6 Prefix of the neighbor

**vlan** - VLAN Identifier

**MAC ADDRESS** - Link layer address of the interface

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# ipv6 neighbor 3333::1111 vlan 1 00:11:22:33:44:55
```

### Related Command

**show ipv6 neighbors** – Displays the IPv6 Neighbour Cache Entries

## 28.7 ipv6 nd suppress-ra

This command suppresses IPv6 router advertisement. The “no” form of the command enables IPv6 router advertisement.

```
ipv6 nd suppress-ra
```

```
no ipv6 nd suppress-ra
```

### Mode

Interface Configuration Mode

### Defaults

Router advertisements are suppressed

### Example:

```
SMIS(config-if)# ipv6 nd suppress-ra
```

### Related Commands

**show ipv6 interface** – Displays the IPv6 interfaces

**show ipv6 traffic** – Displays the IPv6 ICMP and UDP statistics

## 28.8 ipv6 nd managed-config flag

This command sets the 'Managed config flag' which allows the host to use DHCP for address configuration. The “no” form of the command resets the 'Managed config flag' which in turn does not allow the host to use DHCP for address configuration.

```
ipv6 nd managed-config flag
```

```
no ipv6 nd managed-config flag
```

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ipv6 nd managed-config flag
```

### Related Command

```
no ipv6 nd suppress-ra – Enables IPv6 router advertisement
```

## 28.9 ipv6 nd other-config flag

This command sets the 'other config flag' which allows the host to use DHCP for other stateful configuration. The "no" form of the command resets the 'other config flag' which in turn does not allow the host to use DHCP for other stateful configuration.

```
ipv6 nd other-config flag
```

```
no ipv6 nd other-config flag
```

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ipv6 nd other-config flag
```

### Related Command

```
no ipv6 nd suppress-ra – Enables IPv6 router advertisement
```

## 28.10 ipv6 hop-limit

This command configures the maximum hoplimit for all IPv6 packets originating from the interface. The “no” form of the command resets the hoplimit to default value for all IPv6 packets originating from the interface

```
ipv6 hop-limit <HopLimit (1-255)>
```

```
no ipv6 hop-limit
```

### Mode

Interface Configuration Mode

### Defaults

64

### Example:

```
SMIS(config-if)# ipv6 hop-limit 100
```

## 28.11 ipv6 nd ra-lifetime

This command sets the IPv6 Router Advertisement lifetime.

```
ipv6 nd ra-lifetime <LifeTime (0-9000)>
```

### Mode

Interface Configuration Mode

### Defaults

1800 seconds

### Example:

```
SMIS(config-if)# ipv6 nd ra-lifetime 100
```

The ND RA lifetime value must be greater than or equal to the RA interval.

### Related Commands

**no ipv6 nd suppress-ra** – Enables IPv6 router advertisement

**show ipv6 interface** – Displays the IPv6 interfaces

## 28.12 ipv6 nd dad attempts

This command sets the number of duplicate address detection (dad) attempts. The “no” form of the

command resets the duplicate address detection attempts to its default value.

```
ipv6 nd dad attempts <no of attempts (1-10)>
```

```
no ipv6 nd dad attempts
```

### Mode

Interface Configuration Mode

### Defaults

1

### Example:

```
SMIS(config-if)# ipv6 nd dad attempts 5
```

### Related Commands

**show ipv6 interface** – Displays the IPv6 interfaces

**no ipv6 nd suppress-ra** – Enables IPv6 router advertisement



## 28.13 ipv6 nd reachable-time

This command sets the advertised reachability time. The “no” form of the command resets the advertised reachability time to default value.

```
ipv6 nd reachable-time <Reachable Time (1-3600)>
```

```
no ipv6 nd reachable-time
```

### Mode

Interface Configuration Mode

### Defaults

30

### Example:

```
SMIS(config-if)# ipv6 nd reachable-time 500
```

### Related Commands

**show ipv6 interface** – Displays the IPv6 interfaces

**no ipv6 nd suppress-ra** – Enables IPv6 router advertisement

## 28.14 ipv6 nd retrans-time

This command sets the advertised retransmit time. The “no” form of the command resets the advertised retransmit time to its default value 1.

```
ipv6 nd retrans-time <Retrans Time (1-3600)>
```

```
no ipv6 nd retrans-time
```

### Syntax

<Retrans Time (1-3600)> - Any valid number between 1 to 3600

### Mode

Interface Configuration Mode

### Defaults

1

### Example:

```
SMIS(config-if)# ipv6 nd retrans-time 300
```

### Related Commands

**show ipv6 interface** – Displays the IPv6 interfaces

**no ipv6 nd suppress-ra** – Enables IPv6 router advertisement

## 28.15 ipv6 nd ra-interval

This command sets the IPv6 Router Advertisement interval. The “no” form of the command resets the IPv6 Router Advertisement interval to its default value.

```
ipv6 nd ra-interval <interval (4-1800)>
```

```
no ipv6 nd ra-interval
```

### Mode

Interface Configuration Mode

### Defaults

600 seconds

### Example:

```
SMIS(config-if)# ipv6 nd ra-interval 200
```

### Related Commands

**show ipv6 interface** – Displays the IPv6 interfaces

**no ipv6 nd suppress-ra** – Enables IPv6 router advertisement

## 28.16 ipv6 nd prefix

This command configures the prefix to be advertised in IPv6 Router Advertisement. The “no” form of the command removes the prefix from the IPv6 Router Advertisement.

```
ipv6 nd prefix {<prefix addr> <prefixlen> | default} [{{<valid
lifetime> | infinite | at <var valid lifetime>}}{<preferred lifetime>
|infinite | at <var preferred lifetime>} | no-advertise}] [off-link]
[no-autoconfig]
```

```
no ipv6 nd prefix {<prefix addr> <prefix len> | default}
```

### Syntax Description

**no-autoconfig** - Sets the no-autoconfig flag

**prefix addr** - IPv6 prefix to be advertised

**prefixlen** - Length of the configured prefix

**default** - Changes the default value of the rest of the parameters

**valid lifetime** - Sets the valid lifetime value for the prefix

**infinite** - Sets the infinite valid lifetime value for the prefix

**at** - Sets the variable valid lifetime value for the prefix

**preferred lifetime** - Sets the preferred lifetime value for the prefix

**infinite** - Sets the infinite Preferred lifetime value for the prefix

**at** - Sets the variable valid lifetime value for the prefix

**no-advertise** - Sets the No-Advertise flag

**off-link** - Sets the off-link flag

### Mode

Interface Configuration Mode

### Defaults

ra valid lifetime - 25,9200 seconds

ra preferred lifetime - 60,4800 seconds

### Example:

```
SMIS(config-if)# ipv6 nd prefix 3333::1111 64 500 400
```

Valid life-time must be greater than or equal to preferred life-time

## Related Command

`show ipv6 interface` – Displays the IPv6 interfaces

## 28.17 ping ipv6

This command sends IPv6 echo messages.

```
ping ipv6 <prefix> [data <hex_str>] [repeat <count>] [size <value>]
[anycast] [source {vlan <id> | <source_prefix>}] [timeout <value (1-
100)>]
```

### Syntax Description

**prefix** - IPv6 Destination Prefix

**data** - Data to be sent in ping message

**repeat** - Number of ping messages

**size** - Size of the ping message

**anycast** - Type of Prefix

**source** - Source Interface of the ping message can be vlan or source\_prefix

**Timeout** - Duration to wait for the reply

### Mode

Privileged EXEC Mode

### Defaults

data - a5a5

repeat <count> - 5

size - 100 bytes

timeout - 5 seconds

### Example:

```
SMIS# ping ipv6 3333::1111 data a6b6
```

## 28.18 debug ipv6

This command enables IPv6 Trace. The “no” form of the command disables IPv6 Trace.

```
debug ipv6 {IP6|ICMP|UDP6|ND|PING6|Packet}
```

```
no debug ipv6
```

### Syntax Description

**IP6** - IP6 Trace

**ICMP** - ICMP Trace

**UDP6** - UDP6 Trace

**ND** - Neighbor Discovery Trace

**PING6** - PING6 Trace

**Packet** - Packet Trace

### Mode

Privileged EXEC Mode

### Defaults

Disabled

### Example:

```
SMIS# debug ipv6 IP6
```

## 28.19 traceroute

This command traces route to the destination.

```
traceroute [ipv6 <prefix>]
```

### Syntax Description

**ipv6** - IPv6 Destination Prefix

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# traceroute ipv6 4444::1111
```



## 28.20 clear ipv6 neighbors

This command removes all the entries in the IPv6 neighbor table.

```
clear ipv6 neighbors
```

### **Mode**

Privileged EXEC Mode

### **Example:**

```
SMIS# clear ipv6 neighbors
```

### **Related Command**

**show ipv6 neighbors** – Displays the IPv6 Neighbour Cache Entries

## 28.21 clear ipv6 traffic

This command removes all the entries in the IPv6 traffic table.

**clear ipv6 traffic**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# clear ipv6 traffic
```

### Related Command

**show ipv6 traffic** – Displays the IPv6 ICMP and UDP statistics

## 28.22 clear ipv6 route

This command removes all the entries in IPv6 route table.

**clear ipv6 route**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# clear ipv6 route
```

### Related Command

**show ipv6 route** – Displays the IPv6 Routes

## 28.23 show ipv6 interface

This command displays the IPv6 interfaces.

```
show ipv6 interface [{vlan <id>}[prefix]]
```

### Syntax Description

**vlan** - VLAN Identifier

**prefix** - Prefix information

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 interface vlan 1 prefix
Codes: A - Address , P - Prefix-Advertisement
D - Default , N - Not Advertised
AD 2222:: 64 [LA] Valid lifetime 2592000 , Preferred lifetime
604800
AD 2223:1:2:3:: 64 [LA] Valid lifetime 2592000 , Preferred
lifetime 604800
P 3333:: 64 [LA] Valid lifetime 700 , Preferred lifetime
600
PD 3334:: 64 [LA] Valid lifetime 2592000 , Preferred lifetime
604800
PN 3335:: 64 [] Valid lifetime 2592000 , Preferred lifetime
604800
```

### Related Commands

**ipv6 enable** – Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address

**ipv6 - address** – Configures IPv6 address on the interface

**ipv6 - link local address** – Configures the IPv6 link-local address on the interface

**ipv6 nd suppress-ra** – Suppresses IPv6 router advertisement

**ipv6 nd ra-lifetime** – Sets the IPv6 Router Advertisement lifetime

**ipv6 nd dad attempts** – Sets Duplicate Address Detection attempts

**ipv6 nd reachable-time** – Sets the advertised reachability time

**ipv6 nd ra-interval** – Sets the IPv6 Router Advertisement interval

**ipv6 nd prefix** – Configures the prefix to be advertised in IPv6 Router Advertisement

## 28.24 show ipv6 route

This command displays the IPv6 Routes.

**show ipv6 route**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 route
IPv6 Routing Table - 4 entries
Codes : C - Connected, S - Static
O - OSPF, R - RIP, B - BGP
C 2222::/64 [1/1]
via ::, vlan1
C 2223:1:2:3::/64 [1/1]
via ::, vlan1
S 4444::/64 [1/20]
via 2222::2222, vlan1
S 4445::/64 [1/20]
via 2222::2222, vlan1
```

### Related Command

**ipv6 - static routes** – Configures static routes

## 28.25 show ipv6 route summary

This command displays the summary of IPv6 Routes.

```
show ipv6 route summary
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 route summary
IPv6 Routing Table Summary - 4 entries
2 Connected, 2 Static, 0 RIP, 0 BGP, 0 OSPF
Number of prefixes:
/64: 4
```

### Related Command

**show ipv6 route** – Displays the IPv6 Routes

## 28.26 show ipv6 neighbors

This command displays the IPv6 Neighbour Cache Entries.

**show ipv6 neighbors**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 neighbors
```

```
IPv6 Address Age Link-layer Addr State Interface
5555::1111 58 00:11:22:33:44:55 Static vlan1
5556::1111 58 11:22:33:44:55:66 Static vlan1
```

### Related Command

**ipv6 - neighbor** – Configures a static entry in the IPv6 neighbor cache table



## 28.27 show ipv6 traffic

This command displays the IPv6 ICMP and UDP statistics.

**show ipv6 traffic**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 traffic
```

```
IPv6 Statistics
```

```
*****
```

```
0 Rcvd 0 HdrErrors 0 TooBigErrors
```

```
0 AddrErrors 0 FwdDgrams 0 UnknownProtos
```

```
0 Discards 0 Delivers 3 OutRequests
```

```
0 OutDiscards 0 OutNoRoutes 0 ReasmReqds
```

```
0 ReasmOKs 0 ReasmFails
```

```
0 FragOKs 0 FragFails 0 FragCreates
```

```
0 RcvdMcastPkt 3 SentMcastPkts 0 TruncatedPkts
```

```
0 RcvdRedirects 0 SentRedirects
```

```
ICMP Statistics
```

```
*****
```

```
Received :
```

```
0 ICMPPkts 0 ICMPErrPkt 0 DestUnreach 0 TimeExcds
```

```
0 ParmProbs 0 PktTooBigMsg 0 ICMPEchoReq 0
```

```
ICMPEchoReps
```

```
0 RouterSols 0 RouterAdv 0 NeighSols 0 NeighAdv
```

```
0 Redirects 0 AdminProhib 0 ICMPBadCode
```

```
Sent
```

```
0 ICMPMsgs 0 ICMPErrMsgs 0 DstUnReach 0 TimeExcds
```

```
0 ParmProbs 0 PktTooBigs 0 EchoReq 0 EchoReply
```

```
0 RouterSols 0 RouterAdv 3 NeighSols 0 NeighborAdv
```

```
0 RedirectMsgs 0 AdminProhibMsgs
```

```
UDP statistics
```

```
*****
```

```
Received :
```

```
0 UDPDgrams 2 UDPNoPorts 0 UDPErrPkts
```

Sent :

0 UDPDgrams

## 29 RRD6

RRD6 (Route Redistribution) allows different routing protocols to exchange IPv6 routing information.

The list of CLI commands for the configuration of RRD6 is as follows:

[export ospfv3](#)

[redistribute-policy](#)

[default redistribute-policy](#)

[throt](#)

[show redistribute-policy ipv6](#)

[show redistribute information ipv6](#)

## 29.1 export ospfv3

This command enables redistribution of OSPF area/External routes to the protocol. The “no” form of the command disables redistribution of OSPF area/External routes to the protocol.

```
export ospfv3 {area-route|external-route} {rip}
```

```
no export ospfv3 {area-route|external-route} {rip}
```

### Syntax Description

**area-route** - OSPFv3 inter-area and intra-area address/mask pairs to be exported into the routing protocol

**external-route** - OSPFv3 Type 1 and Type 2 External address/mask pairs to be exported into the routing protocol

**rip** - Routing Information Protocol

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# export ospfv3 area-route rip
```

### Related Command

**show redistribute information ipv6** – Displays the RTM6 RRD status for registered protocols

## 29.2 redistribute-policy

This command adds the IPv6 permit/deny Redistribution Policy. The “no” form of the command removes the IPv6 permit/deny Redistribution Policy.

```
redistribute-policy {ipv6} {permit|deny} <DestIp> <DestRange>
{static|local|rip|ospf} {rip|ospf|all}
```

```
no redistribute-policy {ipv6} <DestIp> <DestRange>
```

### Syntax Description

**ipv6** - IPv6 Protocol

**permit** - Sets the default rule for all prefixes to 'permit'

**deny** - Sets the default rule for all prefixes to 'deny'

**DestIp** - Destination IP address

**DestRange** - Destination range

**static** - Static routes

**local** - Local routes

**rip** - Routing Information Protocol

**ospf** - Open Shortest Path First Protocol

**all** - All

### Mode

Global Configuration Mode

### Defaults

permit all

### Example:

```
SMIS(config)# redistribute-policy permit 4444::1111 64.static
ospf
```

The addresses learnt within the specified range through the specified routing protocol will be redistributed to other routing protocols

No routes will be exchanged between RTM and the re-distributing protocols

### Related Command

**show redistribute-policy ipv6** – Displays route redistribution filters



## 29.3 default redistribute-policy

This command sets the default behavior of the RRD6 Control Table.

```
default redistribute-policy {ipv6} {permit | deny}
```

### Syntax Description

**ipv6** - IPv6 Protocol

**permit** - Sets the default rule for all prefixes to 'permit'

**deny** - Sets the default rule for all prefixes to 'deny'

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# default redistribute-policy ipv6 permit
```

### Related Command

**show redistribute-policy ipv6** – Displays route redistribution filters

## 29.4 `throt`

This command configures the maximum number of routes processed for every iteration.

`throt <value>`

### **Mode**

Global Configuration Mode

### **Defaults**

1000

### **Example:**

```
SMIS(config)# throt 100
```



## 29.5 show redistribute-policy ipv6

This command displays the route redistribution filters

```
show redistribute-policy ipv6
```

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show redistribute-policy ipv6
Destination Range SrcProto DestProto Flag
-----
3434::1111 64 static rip Deny
:: 128 all others Allow
```

### Related Commands

**redistribute-policy** – Adds the IPv6 permit/deny Redistribution Policy

**default redistribute-policy** – Sets the default behavior of the RRD6 Control Table

## 29.6 show redistribute information ipv6

This command displays the RTM6 RRD status for registered protocols.

**show redistribute information ipv6**

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show redistribute information ipv6
```

```
Current State is enabled
```

```
ProtoName OspfAreaRoutes OspfExtRoutes
```

```
-----
```

```
local Disable Disable
```

```
static Disable Disable
```

```
rip Enable Enable
```

### Related Command

**export ospfv3** – Enables redistribution of OSPF area/External routes to the protocol

## 30 RIPv6

IPv6 RIP functions the same and offers the same benefits as RIP in IPv4. RIP enhancements for IPv6, detailed in RFC 2080, include support for IPv6 addresses and prefixes, and the use of all-RIP-routers multicast group address as the destination address for RIP update messages. This module describes how to configure Routing Information Protocol for IPv6. IPv6 RIP process maintains a local routing table, referred to as a Routing Information Database (RIB). The IPv6 RIP RIB contains a set of IPv6 RIP routes learnt from all its neighboring networking devices. Before configuring the router to run IPv6 RIP, the ipv6 unicast-routing must be enabled globally, and IPv6 must be enabled on any interface in which IPv6 RIP is to be processed.

The list of CLI commands for the configuration of RIP6 are as follows:

[ipv6 router rip](#)

[ipv6 split-horizon](#)

[ipv6 rip enable](#)

[ipv6 poison reverse](#)

[ipv6 rip default-information originate](#)

[ipv6 rip metric-offset](#)

[redistribute](#)

[distribute prefix](#)

[debug ipv6 rip](#)

[show ipv6 rip database](#)

[show ipv6 rip stats](#)

[show ipv6 rip filter](#)

## 30.1 ipv6 router rip

This command enables the router configuration mode and the “no” form of the command disables RIP6 on all the interfaces.

```
ipv6 router rip
```

```
no ipv6 router rip
```

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# ipv6 router rip
```

Before configuring the router to run IPv6 RIP, the ipv6 unicast-routing must be enabled globally, and IPv6 must be enabled on any interface in which IPv6 RIP is to be processed.

### Related Command

**show ipv6 rip database** – Displays IPv6 Local RIB and routing protocol information

## 30.2 ipv6 split-horizon

This command enables the split horizon updates and the “no” form of the command disables the split horizon updates.

```
ipv6 split-horizon
```

```
no ipv6 split-horizon
```

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ipv6 split-horizon
```

The value splitHorizon denotes that splitHorizon algorithm must be applied in the response packets that are going out.

### Related Command

**show ipv6 rip database** – Displays IPv6 Local RIB and routing protocol information

## 30.3 ipv6 rip enable

This command enables RIP Routing and the “no” form of the command disables the RIP Routing.

```
ipv6 rip enable
```

```
no ipv6 rip
```

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ipv6 rip enable
```

### Related Command

**show ipv6 rip database** – Displays IPv6 Local RIB and routing protocol information

## 30.4 ipv6 poison reverse

This command enables poison reverse.

**ipv6 poison reverse**

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ipv6 poison reverse
```

The value poison reverse denotes that the poison reverse algorithm must be applied in the response packets that are going out.

### Related Command

**show ipv6 rip database** – Displays IPv6 Local RIB and routing protocol information

## 30.5 ipv6 rip default-information originate

This command configures handling of default route originate and the “no” form of the command disables handling of default route originate.

```
ipv6 rip default-information originate
```

```
no ipv6 rip default-information
```

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ipv6 rip default-information originate
```

The command originates the IPv6 default route into the specified RIP routing process updates sent out of the specified interface.

### Related Command

**show ipv6 rip database** – Displays IPv6 Local RIB and routing protocol information



## 30.6 ipv6 rip metric-offset

This command adjusts the default metric increment.

```
ipv6 rip metric-offset <integer (1-15)>
```

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ipv6 rip metric-offset 6
```

The ipv6 rip metric-offset command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes.

The maximum metric that RIP can advertise is 16, and a metric of 16 denotes a route that is unreachable.

### Related Command

**show ipv6 rip database** – Displays IPv6 Local RIB and routing protocol information

## 30.7 redistribute

This command enables redistribution of IPv6 prefix from another protocol into RIP6 and the “no” form of the command disables redistribution of IPv6 prefix from another protocol into RIP6.

```
redistribute {static|connected|ospf} metric <integer(0-16)>
```

```
no redistribute {static|connected|ospf}
```

### Syntax Description

**static** - Statically configured routes to advertise in the RIP6 process

**connected** - Connected routes to advertise in the RIP6 process

**ospf** - OSPF routes to advertise in the RIP6 process

**metric** - Routing metric associated with the route

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# redistribute static metric 6
```

### Related Command

**show ipv6 rip database** – Displays IPv6 Local RIB and routing protocol information

## 30.8 distribute prefix

This command enables Filter network in routing updates sent or received and the “no” form of the command disables Filter network in routing updates sent or received.

```
distribute prefix <ip6_addr> {in | out}
```

```
no distribute prefix <ip6_addr> {in | out}
```

### Syntax Description

**ip6\_addr** - IPv6 Address

**in** - Filter network in routing updates received

**out** - Filter network in routing updates sent out

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# distribute prefix 3333::1111 in
```

Filtering is controlled by distribute lists. Input distribute lists control route reception and input filtering is applied to advertisements received from neighbors. Only those routes that pass input filtering are inserted in the RIP local routing table and become candidates for insertion into the IPv6 routing table.

Output distribute lists control route advertisement. Output filtering is applied to route advertisements sent to neighbors. Only those routes passing output filtering will be advertised.

### Related Commands

**show ipv6 rip database** – Displays IPv6 Local RIB and routing protocol information

**show ipv6 rip filter** – Displays peer and Advfilter table

## 30.9 debug ipv6 rip

This command enables IPv6 RIP routing protocol debugging and the “no” form of the command disables IPv6 RIP routing protocol debugging.

```
debug ipv6 rip { all | data | control }
```

```
no debug ipv6 rip
```

### Syntax Description

**all** - All resources

**data** - Data path messages

**control** - Control Plane messages

### Mode

Privileged EXEC Mode

### Defaults

Disabled

### Example:

```
SMIS# debug ipv6 rip all
```

### Related Commands

**show ipv6 rip database** – Displays IPv6 Local RIB and routing protocol information

## 30.10 show ipv6 rip database

This command displays IPv6 Local RIB and routing protocol information.

```
show ipv6 rip [ database ]
```

### Syntax Description

**database** - IPv6 RIP protocol database

### Mode

Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 rip database
RIP local RIB
4444::/64, metric 10, local
vlan1/::, expires in 180 secs
5555::/64, metric 10, local
vlan2/::, expires in 180 secs
6666::/64, metric 7, static
```

### Related Commands

**ipv6 router rip** – Enables the router configuration mode

**ipv6 split-horizon** – Enables the split horizon updates

**ipv6 rip enable** – Enables RIP Routing

**ipv6 poison reverse** – Enables poison reverse

**ipv6 rip default-information originate** – Configures handling of default route originate

**ipv6 rip metric-offset** – Adjusts default metric increment

**redistribute** – Redistributes IPv6 prefix from another protocol into RIP6

**distribute prefix** – Enables Filter network in routing updates sent or received

**debug ipv6 rip** – Enables IPv6 RIP routing protocol debugging

## 30.11 show ipv6 rip stats

This command displays all the interface statistics.

**show ipv6 rip stats**

**Mode**

Privileged EXEC Mode

**Example:**

```
SMIS# show ipv6 rip stats
Interface vlan1
Rcvd :
Messages 0 Requests 0 Responses 0
UnknownCommds 0 OtherVer 0 Discards 0
Sent :
Messages 1 Requests 1 Responses 0
Trigger Updates 0
```

## 30.12 show ipv6 rip filter

This command displays peer and Advfilter table.

```
show ipv6 rip filter
```

### **Mode**

Privileged EXEC Mode

### **Example:**

```
SMIS# show ipv6 rip filter
Filter Address FilterType
*****
fe80::200:ff:febb:e01 IN
fe80::200:ff:fecc:102 IN
3333::1111 OUT
```

### **Related Command**

**distribute prefix** – Enables Filter network in routing updates sent or received

## 31 OSPFv3

Open Shortest Path First (OSPF) is a link-state, hierarchical Interior Gateway Protocol (IGP) routing algorithm.

OSPFv3 is the modified form of OSPF to support version 6 of the Internet Protocol. The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, etc.) remain unchanged. However, some changes have been necessary, either due to changes in protocol semantics between IPv4 and IPv6, or simply to handle the increased address size of IPv6.

The list of CLI commands for the configuration of OSPFv3 are as follows:

[ipv6 router ospf](#)

[router-id](#)

[area - stub/nssa](#)

[area - stability-interval](#)

[area - translation-role](#)

[timers spf](#)

[abr-type](#)

[area - default-metric value](#)

[area - default-metric type](#)

[area - virtual-link](#)

[ASBR Router](#)

[area - range](#)

[area - external summary address](#)

[redistribute](#)

[passive-interface](#)

[host - metric/area-id](#)

[no area](#)

[nssaAsbrDfRtTrans](#)



[redist-config](#)

[as-external lsdb-limit](#)

[exit-overflow-interval](#)

[demand-extensions](#)

[reference-bandwidth](#)

[ipv6 ospf area](#)

[ipv6 ospf demand-circuit](#)

[ipv6 ospf retransmit-interval](#)

[ipv6 ospf transmit-delay](#)

[ipv6 ospf priority](#)

[ipv6 ospf hello-interval](#)

[ipv6 ospf dead-interval](#)

[ipv6 ospf poll-interval](#)

[ipv6 ospf metric](#)

[ipv6 ospf network](#)

[ipv6 ospf neighbor](#)

[ipv6 ospf passive-interface](#)

[ipv6 ospf neighbor probing](#)

[ipv6 ospf neighbor-probe retransmit-limit](#)

[ipv6 ospf neighbor-probe interval](#)

[debug ipv6 ospf](#)

[show ipv6 ospf interface](#)

[show ipv6 ospf neighbor](#)

[show ipv6 ospf - request/retrans-list](#)

[show ipv6 ospf virtual-links](#)

[show ipv6 ospf border-routers](#)

[show ipv6 ospf - area-range / summary-prefix](#)

[show ipv6 ospf - General Information](#)

[show ipv6 ospf - LSA Database](#)

[show ipv6 ospf route](#)

[show ipv6 ospf areas](#)

[show ipv6 ospf host](#)

[show ipv6 ospf redist-config](#)

## 31.1 ipv6 router ospf

This command enables the OSPFv3 routing protocol. The “no” form of the command disables the OSPFv3 routing protocol.

```
ipv6 router ospf
```

```
no ipv6 router ospf
```

### Mode

Global Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config)# ipv6 router ospf
```

The “no” form of the command disables all the interfaces and triggers flushing of selforiginated LSAs (Link State Advertisements) and deletes the router's Link State Database.

## 31.2 router-id

This command sets a fixed router ID.

```
router-id <IPv4-Address>
```

### Syntax Description

**IPv4-Address** - A 32-bit integer that uniquely identifies the router in the autonomous system.

### Mode

Router Configuration Mode

### Defaults

IPv4-Address - 0.0.0.0

### Example:

```
SMIS(config-router)# router-id 11.0.0.1
```

### Related Command

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process

## 31.3 area - stub/nssa

This command defines an area as a stub area or an NSSA (Not So Stubby Area).

```
area <area-id> {{ stub | nssa } [no-summary]}
```

### Syntax Description

**area-id** - A 32-bit integer

**stub** - Stub area

**nssa** - NSSA

**no-summary** - Allows an area to be a stubby/not-so-stubby but does not allow it to have summary routes injected into it

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# area 1.1.1.1 stub no-summary
```

In a stub area, the generation of a summary LSA is optional.

If the **no-summary** option is specified in the command, then the router neither originates nor propagates summary LSAs into the stubby area /NSSA. It relies entirely on its default route.

If the **no-summary** option is not specified, the router summarizes and propagates summary LSAs.

The **no-summary** option can be specified only in the Area Border Routers and by default, it is set to send summary.

### Related Command

**show ipv6 ospf areas** – Displays the Area Table

## 31.4 area - stability-interval

This command configures the stability interval (in seconds) for the NSSA. The “no” form of the command sets the default value of the stability interval for the NSSA.

```
area <area-id> stability-interval <1-65535>
```

```
no area <area-id> stability-interval
```

### Syntax Description

**area-id** - A 32 bit integer

**stabilityinterval** - The number of seconds after which an elected translator determines that its services are no longer required, and that it must continue to perform its translation duties.

### Mode

Router Configuration Mode

### Defaults

interval-value - 40

### Example:

```
SMIS(config-router)# area 0.0.0.1 stability-interval 50
```

### Related Command

**show ipv6 ospf areas** – Displays the Area Table

## 31.5 area - translation-role

This command configures the translation role for NSSA. The "no" form of the command configures the default translation role for the NSSA.

```
area <area-id> translation-role { always | candidate }
```

```
no area <area-id> translation-role
```

### Syntax Description

**area-id** - A 32 bit integer

**translation-role** - An NSSA Border router's ability to perform NSSA

Translation of Type-7 LSAs to Type-5 LSAs

### Mode

Router Configuration Mode

### Defaults

translation-role - candidate

### Example:

```
SMIS(config-router)# area 0.0.0.1 translation-role always
```

When the translator role is set to always, the Type-7 LSAs are always translated into Type-5 LSAs.

When the translator role is set to candidate, an NSSA border router participates in the translator election process.

### Related Command

**show ipv6 ospf areas** - Displays the Area Table

## 31.6 timers spf

This command configures the delay time and the hold time between two consecutive SPF calculations.

The “no” form of the command sets the default values for spf-delay and spf-holdtime.

```
timers spf <spf-delay> <spf-holdtime>
```

```
no timers spf
```

### Syntax Description

**spf-delay** - The interval by which SPF calculation is delayed after receipt of a topology change

.

**spf-holdtime** - The delay between two consecutive SPF calculations.

### Mode

Router Configuration Mode

### Defaults

spf-delay - 5

spf-holdtime - 10

### Example:

```
SMIS(config-router)# timers spf 10 20
```

### Related Command

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process



## 31.7 abr-type

This command sets the ABR (Area Border Router) type. The “no” form of the command sets the default ABR type.

```
abr-type { standard | cisco | ibm }
```

```
no abr-type
```

### Syntax Description

**standard** - Standard ABR type

**cisco** - CISCO ABR type

**ibm** - IBM ABR type

### Mode

Router Configuration Mode

### Defaults

standard

### Example:

```
SMIS(config-router)# abr-type cisco
```

### Related Command

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process

## 31.8 area - default-metric value

This command sets the default metric value for an area of type NSS/stub only.

```
area <area-id> default-metric <metric>
```

**area-id** - A 32 bit integer

### Syntax Description

**default-metric** - Cost for the default summary route in a stub/NSS area

### Mode

Router Configuration Mode

### Defaults

metric - 1

### Example:

```
SMIS(config-router)# area 1.1.1.1 default-metric 20
```

Default metric can be defined only for a valid area.

### Related Command

**area - stub/nssa** – Defines an area as a stub area or an NSSA (Not So Stubby Area)

## 31.9 area - default-metric type

This command sets the default metric-type for an area type of NSS/stub only.

```
area <area-id> default-metric type <metricType (1-3)>
```

### Syntax Description

**area-id** - A 32 bit integer

**default-metric type** - Type of metric

### Mode

Router Configuration Mode

### Defaults

metricType - 1

### Example:

```
SMIS(config-router)# area 1.1.1.1 default-metric type 2
```

Default metric can be defined only for a valid area.

### Related Command

**area - stub/nssa** – Defines an area as a stub area or an NSSA (Not So Stubby Area)

## 31.10 area - virtual-link

This command sets the Virtual Link between areas. In OSPFv3, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully partitioned, a virtual link can be established. The two endpoints of a virtual link are ABRs. The virtual link must be configured in both routers. The configuration information in each router consists of the other virtual endpoint (the other ABR) and the non-backbone area that the two routers have in common (called the transit area). If 20.0.0.3 is the Router ID of the Neighbor and 100 is the Interface Index assigned to the OSPFv3 virtual interface, then this interface index is advertised in Hello packet sent over the virtual link and in the router's router-LSAs.

```
area <area-id> virtual-link <router-id> <if-index> [hello-interval <1-65535>] [retransmit-interval <1-1800>] [transmit-delay <1-1800>] [dead-interval <1- 65535>]
```

### Syntax Description

**area-id** - A 32 bit integer

**virtual-link** - The Router ID of the Virtual Neighbor

**if-index** - Interface Index assigned to the OSPFv3 virtual interface

**hello-interval** - The interval between hello packets on the OSPFv3 virtual link interface.

**Retransmitinterval** - The time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 virtual link interface.

**transmit-delay** - The estimated time it takes to transmit a link state update packet over this interface.

**dead-interval** - The interval at which hello packets must not be seen before its neighbors declare the router down.

### Mode

Router Configuration Mode

### Defaults

hello-interval - 10

retransmit-interval - 20

transmit-delay - 1

dead-interval - 60

### Example:

```
SMIS(config-router)# area 1.1.1.1 virtual-link 20.0.0.3 1 hellointerval  
50 retransmit-interval 6 transmit-delay 6 dead-interval 100
```

Virtual links cannot be configured through stub areas.

hello-interval and dead-interval values must be the same for all routers on a specific network.

### Related Commands

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

**show ipv6 ospf virtual-links** – Displays the parameters and the current state of OSPFv3 virtual links

## 31.11 ASBR Router

This command configures the router as an ASBR. The “no” form of the command disables the ASBR status of the router.

**ASBR Router**

**no ASBR Router**

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# ASBR Router
```

Only when ASBR (Autonomous System Border Router) status is configured to enable, routes from other protocols are redistributed into OSPFv3 domain.

### Related Command

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process

## 31.12 area - range

This command creates the Internal Aggregation Address Range. The Internal Address Range is of two types:

- Type-3 Aggregation
- Type 7 Translation Aggregation

```
area <Area-ID> range <IPv6-Prefix> <Prefix-Length> [{ advertise |
notadvertise }] {summary | Type7} [tag <tag-value>]
```

### Syntax Description

**Area-ID** - A 32-bit integer

**range** - Internal Aggregation Address Range

**IPv6-Prefix** - The IPv6 address prefix of the range

**Prefix-Length** - The prefix length of the address range

**advertise** - Flushes out all the routes (LSAs) falling in the range and generates aggregated LSA for the range

**not-advertise** - Suppresses routes that match the prefix/prefix-length pair

**summary** - Summary LSA

**Type7** - Type-7 LSA

**tag** - Sets the tag value for the aggregated route

### Mode

Router Configuration Mode

### Defaults

tag - 0

### Example:

```
SMIS(config-router)# area 1.1.1.1 range 3ffe:5000:481d::5 80
advertise Type7 tag 20
```

When parameter summary is specified, the configured range is used for aggregating Type-3 LSA.

When parameter Type7 is specified, the configured range is used for aggregating Type-7 LSAs.

The optional parameter `tag` is used to set the tag value for the aggregated route. This is not used by the OSPFv3 protocol alone. It can be used to communicate information between AS boundary routers.

### **Related Command**

`show ipv6 ospf - area-range / summary-prefix` – Displays either the list of all area address ranges information or all external summary address configuration information



---

## 31.13 area - external summary address

This command enables route aggregation/filtering while importing routes in the OSPFv3 domain. The command configures Type-5 and Type-7 Address Range specifying whether Type-5/Type-7 LSAs are generated or not for the configured range for the particular area.

```
area <AreaID> summary-prefix <IPv6-Prefix> <Prefix-Length> [{ allowAll  
| denyAll | advertise | not-advertise}] [Translation { enabled |  
disabled }]
```

### Syntax Description

**AreaID** - A 32-bit integer

**summary-prefix** - Summary Prefix

**IPv6-Prefix** - The IPv6 address prefix of the range

**Prefix-Length** - The prefix length of the address range

**allowAll** - When set to allowAll and the associated areald is 0.0.0.0, aggregated Type-5 LSAs are generated for the specified range. In addition, aggregated Type-7 LSAs are generated in all the attached NSSAs for the specified range.

**denyAll** - When set to denyAll, neither Type-5 LSA nor Type-7 LSAs are generated for the specified range.

**advertise** - When set to advertise, and the associated areald is 0.0.0.0, aggregated Type-5 LSAs are generated. Otherwise, if the associated areald is x.x.x.x (other than 0.0.0.0), aggregated Type-7 LSA is generated in NSSA area x.x.x.x.

**not-advertise** - When set to doNotAdvertise, and the associated areald is 0.0.0.0, Type-5 LSA is not generated for the specified range, while all the NSSA LSAs within this range are flushed out and aggregated Type-7 LSA is generated in all attached NSSAs. If associated areald is x.x.x.x (other than 0.0.0.0), Type-7 LSA is not generated in NSSA x.x.x.x for the specified range.

**Translation** - When set to enabled, the P-Bit is set in the generated Type-7 LSA. When set to disabled, the P-Bit is cleared in the generated Type-7 LSA for the range.

### Mode

Router Configuration Mode

### Defaults

Translation – enabled advertise

**Example:**

```
SMIS(config-router)# area 0.0.0.0 summary-prefix  
3ffe:5000::481d::5 80 allowall Translation enabled
```

The Value allowAll/denyall is not valid for areald other than 0.0.0.0.

**Related Command**

**show ipv6 ospf - area-range / summary-prefix** – Displays either the list of all area address ranges information or all external summary address configuration information

## 31.14 redistribute

This command configures the protocol from which the routes have to be redistributed into OSPFv3. The “no” form of the command disables the redistribution of routes from the given protocol into OSPFv3.

```
redistribute {static | connected | ripng | bgp}
```

```
no redistribute {static | connected | ripng | bgp }
```

### Syntax Description

**static** - Advertises routes, configured statically in the OSPFv3 routing process

**connected** - Advertises directly connected networks routes in the OSPFv3 routing process

**ripng** - Advertises routes that are learnt by the RIP process in the OSPFv3 routing process

**bgp** - Advertises routes that are learnt by the BGP process in the OSPFv3 routing process

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# redistribute static
```

To configure Redistribution of routes from other protocols, the following steps must be performed.

1. Configure the router as ASBR.
2. Configure redistribution of routes from particular protocol.

The above order must be maintained and ASBR setting must be done before enabling redistribution.

### Related Commands

**ASBR Router** – Configures the router as an ASBR

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process

## 31.15 passive-interface

This command sets the global default passive interface status. All the interfaces created after executing this command become passive interfaces. The “no” form of the command resets the global default passive interface status. All the interfaces created after executing this command become non-passive interfaces.

**passive-interface**

**no passive-interface**

### Mode

Router Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-router)# passive-interface
```

### Related Command

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process

## 31.16 host - metric/area-id

This command configures a host entry with metric and/or area-id. The “no” form of the command deletes a host entry.

```
host <IPv6-Address> {metric <cost>} [area-id {<AreaID>}]
```

```
no host <IPv6-Address>
```

### Syntax Description

**IPv6-Address** - IPV6 address prefix

**metric** - Metric to be advertised

**area-id** - A 32-bit integer

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# host 3ffe:481d::5 metric 10 area-id 0.0.0.1
```

### Related Command

**show ipv6 ospf host** – Displays the Host Table information

## 31.17 no area

This command deletes an area and does any one of the following based on the optional parameter:

- converts stub/nss area to normal area
- deletes virtual link
- deletes stub cost
- deletes area-range or summary-prefix.

```
no area <area-id> [ { stub | nssa | virtual-link <router-id> | default-
metric | {range {summary | Type7} | summary-prefix} <IPv6-Prefix>
<Prefix-Length>} ]
```

### Syntax Description

**area-id** - A 32-bit integer

**stub** - Stub area

**nssa** - Not So Stubby Area

**virtual-link** - The Router ID of the virtual neighbor

**default-metric** - Cost for the default summary route in a stub/NSS area

**range** - Type-3 or Type-7 or External LSA range

**IPv6-Prefix** - The IPv6 address prefix of the range

**Prefix-Length** - The prefix length of the address range

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# no area 1.1.1.1
SMIS(config-router)# no area 1.1.1.1 stub
SMIS(config-router)# no area 1.1.1.1 default-metric
SMIS(config-router)# no area 1.1.1.1 virtual-link 20.0.0.3
SMIS(config-router)# no area 1.1.1.1 range summary
3ffe:3010:481d::5 80
```

Before deleting an area, it is necessary to delete all the interfaces attached to that area.

### Related Commands

**show ipv6 ospf areas** – Displays the Area Table

**show ipv6 ospf - area-range / summary-prefix** – Displays either the list of all area address ranges information or all external summary address configuration information

**no ipv6 ospf area** – Disables OSPFv3 routing protocol on the interface

## 31.18 nssaAsbrDfRtTrans

This command enables setting of the P bit in the default Type-7 LSA generated by an NSSA internal ASBR. The “no” form of the command disables setting of the P bit in the default Type-7 LSA generated by an NSSA internal ASBR.

**nssaAsbrDfRtTrans**

**no nssaAsbrDfRtTrans**

### Mode

Router Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-router)# nssaAsbrDfRtTrans
```

### Related Commands

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process



## 31.19 redist-config

This command configures the information to be applied to routes learnt from RTM. The “no” form of the command deletes the information applied to routes learnt from RTM.

```
redist-config <IPv6-Prefix> <Prefix-Length> [metric-value <metric>]  
[metric-type {asExtttype1 | asExtttype2}] [tag <tag-value>]
```

```
no redist-config <IPv6-Prefix> <Prefix-Length>
```

### Syntax Description

**IPv6-Prefix** - The IPv6 address prefix

**Prefix-Length** - The prefix length of the address

**metric-value** - The Metric value applied to the route before it is advertised into the OSPFv3 Domain

**metric-type** - The Metric Type applied to the route before it is advertised into the OSPFv3 Domain

**tag** - The Tag Type describes whether Tags will be automatically generated or will be manually configured

### Mode

Router Configuration Mode

### Example:

```
SMIS(config-router)# redist-config 3ffe:5000:481d::5 80 metricvalue  
30 metric-type asExtttype1 tag 12
```

### Related Command

**show ipv6 ospf redist-config** – Displays the configuration information to be applied to the routes learned from the RTM

## 31.20 as-external lsdb-limit

This command sets the maximum number of non-default AS-external-LSA entries that can be stored in the link-state database. If the value is -1, then there is no limit.

```
as-external lsdb-limit <lsdb-limit (-1 - 0x7fffffff)>
```

### Mode

Router Configuration Mode

### Defaults

lsdb-limit - -1

### Example:

```
SMIS(config-router)# as-external lsdb-limit 10
```

When the number of non-default AS-external-LSAs in a router's link-state database reaches the configured limit, the router enters Overflow- State. The router never holds more than the configured non-default AS-external-LSAs in its database.

The LSDB limit MUST be set identically in all routers attached to the OSPFv3 backbone and/or any regular OSPFv3 area. (i.e. OSPFv3 stub areas and NSSAs are excluded).

### Related Commands

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process

**exit-overflow-interval** – Sets the number of seconds after which a router will attempt to leave the Overflow State

## 31.21 exit-overflow-interval

This command sets the number of seconds after which a router will attempt to leave the Overflow State.

**exit-overflow-interval** <interval>

### Mode

Router Configuration Mode

### Defaults

interval - 0

### Example:

```
SMIS(config-router)# exit-overflow-interval 10
```

### Related Command

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process

## 31.22 demand-extensions

This command enables routing support for demand routing. The “no” form of the command disables routing support for demand routing.

**demand-extensions**

**no demand-extensions**

### Mode

Router Configuration Mode

### Defaults

Enabled

### Example:

```
SMIS(config-router)# demand-extensions
```

### Related Command

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process

## 31.23 reference-bandwidth

This command sets the reference bandwidth in kilobits per second for calculating the default interface metrics.

**reference-bandwidth <ref-bw>**

### Mode

Router Configuration Mode

### Defaults

ref-bw - 100,000 KBPS

### Example:

```
SMIS(config-router)# reference-bandwidth 1000000
```

### Related Command

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process

## 31.24 ipv6 ospf area

This command enables OSPFv3 for IPv6 on an interface. The “no” form of the command disables OSPFv3 routing protocol on the interface.

```
ipv6 ospf area <IPv4-Address>
```

```
no ipv6 ospf
```

### Syntax Description

**IPv4-Address** - A 32-bit integer

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# ipv6 ospf area 0.0.0.0
```

The no form of the command disables an interface and triggers flushing of selforiginated Link Scope LSAs, and deletes the Link Scope LSAs associated with this interface from the Link State Database. If there is a single interface in the associated area, then this command deletes its Area Scope LSAs from the Link State Database.

### Related Commands

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

## 31.25 ipv6 ospf demand-circuit

This command configures OSPFv3 to treat the interface as an OSPFv3 demand circuit. It indicates whether Demand OSPFv3 procedures (hello suppression to FULL neighbors and setting the DoNotAge flag on propagated LSAs) must be performed on the configured interface. The “no” form of the command disables the demand circuit on an interface.

```
ipv6 ospf demand-circuit
```

```
no ipv6 ospf demand-circuit
```

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# ipv6 ospf demand-circuit
```

The routing support for demand routing must have been enabled (using the `demandextensions` command) prior to the execution of this command.

### Related Commands

**demand-extensions** – Enables routing support for demand routing

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

## 31.26 ipv6 ospf retransmit-interval

This command sets the time between LSA retransmissions for adjacencies belonging to interface. The “no” form of the command sets the default retransmit interval for an interface.

```
ipv6 ospf retransmit-interval <interval>
```

```
no ipv6 ospf retransmit-interval
```

### Mode

Interface Configuration Mode

### Defaults

interval - 5

### Example:

```
SMIS(config-if)# ipv6 ospf retransmit-interval 10
```

The retransmit time interval is the number of seconds between the link-state advertisement retransmissions for adjacencies belonging to an interface. The retransmit-interval value is also used while retransmitting database description and linkstate request packets.

### Related Command

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information



## 31.27 ipv6 ospf transmit-delay

This command sets the estimated time taken to transmit LS update packet over a particular interface. The “no” form of the command sets the default transmit delay for an interface.

```
ipv6 ospf transmit-delay <1-1800>
```

```
no ipv6 ospf transmit-delay
```

### Mode

Interface Configuration Mode

### Defaults

delay - 1

### Example:

```
SMIS(config-if)# ipv6 ospf transmit-delay 10
```

### Related Command

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

## 31.28 ipv6 ospf priority

This command sets the router priority, which helps to determine the Designated Router for this network. The “no” form of the command sets the default router priority for an interface.

```
ipv6 ospf priority <1-255>
```

```
no ipv6 ospf priority
```

### Mode

Interface Configuration Mode

### Defaults

priority - 1

### Example:

```
SMIS(config-if)# ipv6 ospf priority 7
```

A priority value of 0 signifies that the router is not eligible to become the designated router on a particular network.

### Related Command

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

## 31.29 ipv6 ospf hello-interval

This command specifies the time interval between the OSPFv3 hello packets on a particular interface (the length of time, in seconds, between the Hello packets that the router sends on the interface). The “no” form of the command sets the default hello interval for an interface.

```
ipv6 ospf hello-interval <1-65535>
```

```
no ipv6 ospf hello-interval
```

### Mode

Interface Configuration Mode

### Defaults

interval - 10

### Example:

```
SMIS(config-if)# ipv6 ospf hello-interval 20
```

The hello interval value must be same for all routers attached to a common link.

### Related Command

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

## 31.30 ipv6 ospf dead-interval

This command configures the router dead interval. It is configured in seconds and indicates the time period for which the router waits for hello packet from the neighbor before declaring this neighbor down. The “no” form of the command sets the interface dead interval to default value.

```
ipv6 ospf dead-interval <1-65535>
```

```
no ipv6 ospf dead-interval
```

### Mode

Interface Configuration Mode

### Defaults

interval - 40

### Example:

```
SMIS(config-if)# ipv6 ospf dead-interval 50
```

This value must be a multiple of the Hello interval and must be same for all routers attached to a common link.

### Related Command

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

## 31.31 ipv6 ospf poll-interval

This command configures the larger time interval, in seconds, between the Hello packets sent to an inactive non-broadcast multi-access neighbor. The “no” form of the command sets the default poll interval for an interface.

```
ipv6 ospf poll-interval <1-65535>
```

```
no ipv6 ospf poll-interval
```

### Mode

Interface Configuration Mode

### Defaults

interval - 120

### Example:

```
SMIS(config-if)# ipv6 ospf poll-interval 30
```

### Related Command

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

## 31.32 ipv6 ospf metric

This command explicitly specifies the metric value for sending a packet on an interface. The “no” form of the command sets the default value for the interface metric.

```
ipv6 ospf metric <1-65535>
```

```
no ipv6 ospf metric
```

### Mode

Interface Configuration Mode

### Defaults

metric - 10

### Example:

```
SMIS(config-if)# ipv6 ospf metric 20
```

### Related Command

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

## 31.33 ipv6 ospf network

This command sets the network type for an interface. The “no” form of the command sets the default value for the network type.

```
ipv6 ospf network { broadcast | non-broadcast | point-to-multipoint |
pointto- point }
```

```
no ipv6 ospf network
```

### Syntax Description

**broadcast** - Networks supporting many (more than two) attached routers, together with the capability to address a single physical message to all of the attached routers (broadcast)

**non-broadcast** - Networks supporting many (more than two) routers, but having no broadcast capability

**point-to-multipoint** - Treats the non-broadcast network as a collection of point-to-point links

**point-to-point** - A network that joins a single pair of routers

### Mode

Interface Configuration Mode

### Defaults

broadcast

### Example:

```
SMIS(config-if)# ipv6 ospf network non-broadcast
```

If the Interface Network type is NBMA or Point-to-Multipoint, any neighbor must be configured. When there are few configured neighbors on the interface, then both the network type change command and the “no” form of the command will not succeed.

### Related Commands

**ipv6 ospf neighbor** – Configures a neighbor on non-broadcast networks and sets the priority value for the neighbor if specified

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

## 31.34 ipv6 ospf neighbor

This command configures a neighbor on non-broadcast networks and sets the priority value for the neighbor if specified. The “no” form of the command deletes a configured neighbor or sets the default priority value (if the priority option is specified).

```
ipv6 ospf neighbor <IPv6-Address> [priority <1-255>]
```

```
no ipv6 ospf neighbor <IPv6-Address> [priority]
```

### Syntax Description

**IPv6-Address** - IPv6 Address Prefix

**priority** - A number that specifies the router priority

### Mode

Interface Configuration Mode

### Defaults

priority <Number> - 1

### Example:

```
SMIS(config-if)# ipv6 ospf neighbor fe80::220:35ff:fe43:6020  
priority 2
```

- ➔ In the OSPFv3 protocol packets, the IPv6 address indicates the source address of the neighbor. The Link Local address of the neighbor must be used for this field.
- ➔ Neighbors can be configured only in NBMA networks and Point-to-Multipoint networks.

### Related Commands

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

**show ipv6 ospf neighbor** – Displays OSPFv3 neighbors information



## 31.35 ipv6 ospf passive-interface

This command configures an OSPFv3 interface to be Passive. The execution of the command results in suppressing OSPFv3 protocol packets traffic on this interface. The “no” form of the command configures an OSPFv3 interface to be non-passive.

```
ipv6 ospf passive-interface
```

```
no ipv6 ospf passive-interface
```

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# ipv6 ospf passive-interface
```

### Related Command

**show ipv6 ospf interface** – Displays the OSPFv3 related interface information

## 31.36 ipv6 ospf neighbor probing

This command enables neighbor probing on demand-circuit enabled interface. The “no” form of the command disables neighbor probing on demand-circuit enabled interface.

```
ipv6 ospf neighbor probing
```

```
no ipv6 ospf neighbor probing
```

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# ipv6 ospf neighbor probing
```

### Related Command

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

## 31.37 ipv6 ospf neighbor-probe retransmit-limit

This command sets the number of consecutive LSA retransmissions before the neighbor is deemed inactive. The “no” form of the command sets the default neighbor probe retransmission limit.

```
ipv6 ospf neighbor-probe retransmit-limit <retrans-limit>
```

```
no ipv6 ospf neighbor-probe retransmit-limit
```

### Mode

Interface Configuration Mode

### Defaults

retrans-limit - 10

### Example:

```
SMIS(config-if)# ipv6 ospf neighbor-probe retransmit-limit 30
```

### Related Command

```
show ipv6 ospf interface – Displays the OSPFv3-related interface information
```

## 31.38 ipv6 ospf neighbor-probe interval

This command sets the number of seconds, that indicates how often neighbor will be probed. The “no” form of the command sets the default neighbor probe interval.

```
ipv6 ospf neighbor-probe interval <interval>
```

```
no ipv6 ospf neighbor-probe interval
```

### Mode

Interface Configuration Mode

### Defaults

interval - 120

### Example:

```
SMIS(config-if)# ipv6 ospf neighbor-probe interval 200
```

### Related Command

**show ipv6 ospf interface** – Displays the OSPFv3-related interface information

## 31.39 debug ipv6 ospf

This command sets the trace levels. The “no” form of the command resets the trace levels.

```
debug ipv6 ospf [pkt ( [{high | low | hex}] [hp] [ddp] [lrq] [lsu]
[lsa] )] [level ( [fn_entry] [fn_exit] [critical] [mem_alloc_succ]
[mem_alloc_fail] )] [module ( [ppp] [rtm] [nssa] [rt_aggrg]
[adj_formation] [lsdb] [ism] [nsm] [rt_calc] [interface] [config] )]
```

```
no debug ipv6 ospf [ pkt ( [{high | low | hex}] [hp] [ddp] [lrq] [lsu]
[lsa] )] [level ( [fn_entry] [fn_exit] [critical] [mem_alloc_succ]
[mem_alloc_fail] )] [ module ( [ppp] [rtm] [nssa] [rt_aggrg]
[adj_formation] [lsdb] [ism] [nsm] [rt_calc] [interface] [config] ) ]
```

### Syntax Description

**pkt** - Packet High Level Dump debug messages

**high** - Packet High Level Dump Trace

**low** - Packet Low Level Dump Trace

**hex** - Packet Hex Dump Trace

**hp** - Hello packet Trace

**ddp** - DDP packet Trace

**lrq** - Link State Request Packet Trace

**lsu** - Link State Update Packet Trace

**lsa** - Link State Acknowledge Packet Trace

**level** - Trace Level Debug Messages

**fn\_entry** - Function Entry Trace

**fn\_exit** - Function Exit Trace

**critical** - Critical Trace

**mem\_alloc\_succ** - Memory Allocation Success Trace

**mem\_alloc\_fail** - Memory Allocation Failure Trace

**module** - OSPFv3 Module Debug Messages

**ppp** - Protocol Packet Processing Trace

**rtm** - RTM Module Trace

**nssa** - NSSA Trace

**rt\_aggrg** - Route Aggregation Trace

**adj\_formation** - Adjacency formation Trace

**lsdb** - Link State Database Trace  
**ism** - Interface State Machine Trace  
**nsm** - Neighbor State Machine Trace  
**rt\_calc** - Routing Table Calculation Trace  
**interface** - Interface Trace  
**config** - Configuration Trace

### **Mode**

Privileged EXEC Mode

### **Defaults**

Debugging is disabled by default.

### **Example:**

```
SMIS# debug ipv6 ospf pkt high hp level fn_entry module ppp
```

### **Related Command**

**show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process

## 31.40 show ipv6 ospf interface

This command displays the OSPFv3-related interface information.

```
show ipv6 ospf interface [ vlan <vlan-id(1-4069)> ]
```

### Syntax Description

**vlan** - VLAN Identifier

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf interface vlan 1
OSPFv3 Interface Information
Interface Name: vlan2 Interface Id: 1 Area Id: 0.0.0.0
Local Address: fe80::211:22ff:fe33:4412 Router Id: 11.0.0.2
Network Type: BROADCAST Cost: 10 State: WAITING
Designated Router Id: 0.0.0.0 local address: (null)
Backup Designated Router Id: 0.0.0.0 local address: (null)
Transmit Delay: 1 sec Priority: 1 IfOptions: 0x0
Timer intervals configured:
Hello: 10, Dead: 40, Retransmit: 5, Poll: 120
Demand Circuit: Disable Neighbor Probing: Disable
Nbr Probe Retrans Limit: 10 Nbr Probe Interval: 120
Hello due in 4 sec
Neighbor Count is: 1
Adjacent with the neighbor 11.0.0.1
```

### Related Commands

**area - virtual-link** – Sets the Virtual Link between Areas

**ipv6 ospf area** – Enables OSPFv3 for IPv6 on an interface

**ipv6 ospf demand-circuit** – Configures OSPFv3 to treat the interface as an OSPFV3 demand circuit

**ipv6 ospf retransmit-interval** – Sets the time between LSA retransmissions for adjacencies belonging to an interface

**ipv6 ospf transmit-delay** – Sets the estimated time taken to transmit LS update packet over a particular interface

**ipv6 ospf priority** – Sets the router priority, which helps to determine the Designated Router for this network

**ipv6 ospf hello-interval** – Specifies the time interval between the OSPFv3 hello packets on a particular interface

**ipv6 ospf dead-interval** – Configures the router dead interval

**ipv6 ospf poll-interval** – Configures the larger time interval, in seconds, between the Hello packets sent to an inactive non-broadcast multi-access neighbor

**ipv6 ospf metric** – Specifies the metric value for sending a packet on an interface

**ipv6 ospf network** – Sets the network type for an interface

**ipv6 ospf neighbor** – Configures a neighbor on non-broadcast networks and sets the priority value for the neighbor if specified

**ipv6 ospf passive-interface** – Configures an OSPFv3 interface to be Passive

**ipv6 ospf neighbor probing** – Enables neighbor probing on demand-circuit enabled interface

**ipv6 ospf neighbor-probe retransmit-limit** – Sets the number of consecutive LSA retransmissions before the neighbor is deemed inactive

**ipv6 ospf neighbor-probe interval** – Sets the number of seconds, that indicates how often neighbor will be probed



## 31.41 show ipv6 ospf neighbor

This command displays OSPFv3 neighbor information.

```
show ipv6 ospf neighbor [ <Neighbor-RouterID> ]
```

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf neighbor
```

```
ID Pri State Dead Address
```

```
Time
```

```
11.0.0.4 1 FULL/PTOP 31 fe80::211:22ff:fe33:4434
```

```
11.0.0.5 10 FULL/BACKUP 35 fe80::260:83ff:fe38:8aa2
```

### Related Command

**ipv6 ospf neighbor** – Configures a neighbor on non-broadcast networks and sets the priority value for the neighbor if specified

## 31.42 show ipv6 ospf - request/retrans-list

This command displays the list of all link state advertisements (LSAs) in request-list or in retransmission-list.

```
show ipv6 ospf { request-list | retrans-list } [ <Neighbor-RouterID> ]
```

### Syntax Description

**request-list** - The list of Link State Advertisements for which the neighbor has more up-to-date instances.

**retrans-list** - The list of Link State Advertisements that have been sent but not acknowledged.

**Neighbor-RouterID** - Neighbor router ID

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf retrans-list
NeighborId 20.0.0.3, Nbr Address fe80::220:35ff:fe43:6020
Type LsId AdvRtr SeqNo Age Checksum
0x2001 0.0.0.2 11.0.0.2 0x80000011 0 0xcddf
```

```
SMIS# show ipv6 ospf request-list
Neighbor 20.0.0.3, Address fe80::220:35ff:fe43:6020
Type LSID ADVRTR SeqNo Age Checksum
8193 0.0.0.1 11.0.0.3 0x80000002 6 0x1211
```

## 31.43 show ipv6 ospf virtual-links

This command displays the parameters and the current state of OSPFv3 virtual links.

```
show ipv6 ospf virtual-links
```

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf virtual-links
Interface State: PointToPoint, Neighbor State: FULL
Transit Area: 2.2.2.2, Virtual Neighbor: 11.0.0.7
Intervals Configured for the Virtual Interface:
Hello: 10, Dead: 60, Transit: 1, Retransmit : 20
```

### Related Command

**area - virtual-link** – Sets the Virtual Link between Areas

## 31.44 show ipv6 ospf border-routers

This command displays the internal OSPFv3 routing table entries to an ABR/ASBR.

**show ipv6 ospf border-routers**

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf border-routers
OSPFv3 Process Border Router Information
Destination Type NextHop Cost Rt Area
Type Id
11.0.0.2 ABR fe80::211:22ff:fe33:4412 10 intraArea 0.0.0.0
11.0.0.2 ABR fe80::211:22ff:fe33:4422 10 intraArea 0.0.0.1
11.0.0.2 ASBR fe80::211:22ff:fe33:4412 10 intraArea 0.0.0.0
11.0.0.2 ASBR fe80::211:22ff:fe33:4422 10 intraArea 0.0.0.0
```

### Related Commands

**abr-type** – Sets the ABR (Area Border Router) type

**ASBR Router** – Configures the router as an ASBR

## 31.45 show ipv6 ospf - area-range / summary-prefix

This command displays either the list of all area address ranges information or all external summary address configuration information.

```
show ipv6 ospf { area-range | summary-prefix }
```

### Syntax Description

**area-range** - Area associated with the OSPFv3 address range

**summary-prefix** - Aggregate addresses for OSPFv3

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf area-range
OSPFv3 Summary Address Configuration Information
Network Pfx LSA Area Effect Tag
Length Type
3ffe::100:0:0:0 80 Summary 0.0.0.0 advertise 0
3ffe::110:0:0:0 80 Summary 0.0.0.0 doNotAdvertise 0
3ffe::120:0:0:0 80 Summary 0.0.0.1 advertise 0
3ffe::130:0:0:0 80 Type7 0.0.0.1 advertise 0
```

```
SMIS# show ipv6 ospf summary-prefix
OSPFv3 External Summary Address Configuration Information
Prefix Pfx Area Effect TranslationState
Length
3ffe::200:0:0:0 80 0.0.0.0 advertise enabled
3ffe::210:0:0:0 80 0.0.0.0 advertise disabled
3ffe::220:0:0:0 80 0.0.0.0 doNotAdvertise enabled
3ffe::230:0:0:0 80 0.0.0.0 allowAll enabled
3ffe::240:0:0:0 80 0.0.0.0 denyAll enabled
```

### Related Commands

**area - range** - Creates the Internal Aggregation Address Range

**area - external summary address** – Enables route aggregation/filtering while importing routes in the OSPFv3 domain

**no area** – Deletes an area

## 31.46 show ipv6 ospf - General Information

This command displays general information about OSPFv3 routing process.

**show ipv6 ospf info**

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf info
Router Id: 11.0.0.1 ABR Type: Standard ABR
SPF schedule delay: 5 secs Hold time between two SPF's: 10
secs
Exit Overflow Interval: 0 Ref BW: 100000000 Ext Lsdb
Limit: -1
Trace Value: 0x00000800 As Scope Lsa: 0 Checksum
Sum: 0x0
Demand Circuit: Enable Passive Interface: Disable
Nssa Asbr Default Route Translation: Disable
It is an Area Border Router
Number of Areas in this router 2
Area 0.0.0.0
Number of interfaces in this area is 1
Number of Area Scope Lsa: 4 Checksum Sum: 0x1210e
Number of Indication Lsa: 0 SPF algorithm
executed: 6 times
Area 0.0.0.1
Number of interfaces in this area is 1
Number of Area Scope Lsa: 3 Checksum Sum: 0x18d41
Number of Indication Lsa: 0 SPF algorithm
executed: 2 times
```

### Related Commands

**router-id** – Sets a fixed router ID

**timers spf** – Configures the delay time and the hold time between two consecutive SPF

calculations

**abr-type** – Sets the ABR (Area Border Router) type

**ASBR Router** – Configures the router as an ASBR

**passive-interface** – Sets the global default passive interface status

**nssaAsbrDfRtTrans** – Enables setting of P bit in the default Type-7 LSA generated by an NSSA internal ASBR

**as-external lsdb-limit** – Sets the maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database

**exit-overflow-interval** – Sets the number of seconds after which a router will attempt to leave the Overflow State

**demand-extensions** – Enables routing support for demand routing

**reference-bandwidth** – Sets the reference bandwidth in kilobits per second for calculating the default interface metrics

**ipv6 ospf area** – Enables OSPFv3 for IPv6 on an interface

**debug ipv6 ospf** – Sets the trace levels



## 31.47 show ipv6 ospf - LSA Database

This command displays the LSA information.

```
show ipv6 ospf [area <AreaID>] database [{router|network|as-
external|interprefix| inter-router|intra-prefix|link|nssa}]
[{{detail|HEX}}]
```

### Syntax Description

**Area** - A 32-bit integer

**database** - Displays the number of each type of LSA for each area in the database

**router** - Router LSAs

**network** - Network LSAs

**as-external** - AS-External LSAs

**inter-prefix** - Inter-prefix LSAs

**inter-router** - Inter-router LSAs

**intra-prefix** - Intra-prefix LSAs

**link** - Link State LSAs

**nssa** - NSSA LSAs

**detail** - Displays the LSAs information in detail

**HEX** - Displays the LSAs information in hexadecimal format

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf database
AreaId RtrId LsaType Age Seq# Checksum
0.0.0.0 11.0.0.1 0x0008 300 0x80000002 0x323f
0.0.0.0 11.0.0.2 0x0008 300 0x80000001 0xa426
0.0.0.0 11.0.0.1 0x2001 1 0x80000003 0x3b9a
0.0.0.0 11.0.0.2 0x2001 0 0x80000006 0x2fa2
0.0.0.0 11.0.0.2 0x2002 0 0x80000001 0x6081
0.0.0.0 11.0.0.2 0x2009 0 0x80000002 0x504c
```

```
SMIS# show ipv6 ospf database detail
```

## Supermicro Intelligent Switch Command Line Interface User Guide

---

```
Age: 300 Seconds LS Type: Link Lsa
Link State Id: 0.0.0.1 Adv Rtr Id: 11.0.0.1
Sequence: 0x80000002 Checksum: 0x323f Length: 60
Router Priority: 1 Options: 0x33
Prefix: fe80::211:22ff:fe33:4411
#Prefixes; 1
Prefix Length (Bytes): 12 Prefix Options: 0x00
Prefix: 3ffe::100:0:0:0
```

```
SMIS# show ipv6 ospf database hex
00 00 00 08 00 00 00 02 0b 00 00 01 80 00 00 02 e9 d0 00 2c 01
00 00 33 fe 80 00
00 00 00 00 00 02 11 22 ff fe 33 44 21 00 00 00 00
00 07 00 08 00 00 00 02 0b 00 00 02 80 00 00 02 f9 be 00 2c 01
00 00 33 fe 80 00
00 00 00 00 00 02 11 22 ff fe 33 44 22 00 00 00 00
00 00 20 01 00 00 00 00 0b 00 00 01 80 00 00 01 fe e2 00 28 00
00 00 33 01 00 00
02 00 00 00 02 00 00 00 02 0b 00 00 02
00 06 20 01 00 00 00 00 0b 00 00 02 80 00 00 03 e7 f4 00 28 03
00 00 33 01 00 00
02 00 00 00 02 00 00 00 02 0b 00 00 01
```

## 31.48 show ipv6 ospf route

This command displays routes learned by the OSPFv3 process

**show ipv6 ospf route**

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf route
Dest/ NextHop/ Cost Rt.Type Area
Prefix-Length IfIndex
3ffe::10:0:0:0 fe80::290:69ff: 30 interArea 0.0.0.0
/80 fe90:b4bf /vlan1
3ffe::20:0:0:0 fe80::290:69ff: 20 interArea 0.0.0.0
/80 fe90:b4bf /vlan1
3ffe::30:0:0:0 :: /vlan1 10 intraarea 0.0.0.0
/80
3ffe::40:0:0:0 fe80::211:22ff: 20 intraArea 0.0.0.0
/80 fe33:4423 /vlan1
3ffe::40:0:0:5 fe80::211:22ff: 20 interArea 0.0.0.0
/128 fe33:4426 /vlan2
3ffe::40:0:0:5 fe80::211:22ff: 20 interArea 0.0.0.0
/128 fe33:4423 /vlan1
3ffe::50:0:0:0 :: /vlan2 10 intraArea 0.0.0.0
/80
3ffe::60:0:0:0 fe80::211:22ff: s20 interArea 0.0.0.0
/80 fe33:4426 /vlan2
3ffe::60:0:0:6 fe80::211:22ff: 10 interArea 0.0.0.0
/128 fe33:4426 /vlan2
```

### Related Commands

**ipv6 router ospf** – Enables the OSPFv3 routing protocol

**router-id** – Sets a fixed router ID

## 31.49 show ipv6 ospf areas

This command displays the Area Table.

**show ipv6 ospf areas**

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf areas
OSPFv3 AREA CONFIGURATION INFORMATION
AreaId: 0.0.0.0 Area Type: NORMAL AREA
Spf Calculation: 3 (times) Area Bdr Rtr Count: 1
As Bdr Rtr Count: 0 Area Summary: Send Summary
AreaId: 0.0.0.1 Area Type: NSS AREA
Spf Calculation: 0 (times) Area Bdr Rtr Count: 1
As Bdr Rtr Count: 0 Area Summary: Send Summary
Stub Metric: 0x1 Stub Metric Type: 1
Translator Role: Candidate Translator State: Disabled
Nssa Stability Interval: 40
```

### Related Commands

- area - stub/nssa** – Defines an area as a stub area or an NSSA (Not So Stubby Area)
- area - stability-interval** – Configures the stability interval (in seconds) for the NSSA
- area - translation-role** – Configures the translation role for NSSA
- no area** – Deletes an area

## 31.50 show ipv6 ospf host

This command displays the Host Table information.

```
show ipv6 ospf host
```

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf host
OSPFv3 HOST CONFIGURATION Information
Address AreaId StubMetric
3ffe::80:0:1 0.0.0.0 30
```

### Related Command

**host - metric/area-id** – Configures a host entry with metric and/or area-id

## 31.51 show ipv6 ospf redistrib-config

This command displays the configuration information to be applied to the routes learnt from the RTM.

```
show ipv6 ospf redistrib-config
```

### Mode

User/Privileged EXEC Mode

### Example:

```
SMIS# show ipv6 ospf redistrib-config
```

```
Address Prefix PfxLength MetricType Metric TagType TagValue  
3ffe:: 64 asExtType2 10 manual 10
```

### Related Command

**redistrib-config** – Configures the information to be applied to routes learnt from RTM

## 32 DiffServ (Differentiated Services)

DiffServ (Differentiated Services) is an architecture for providing different types or levels of service for network traffic. One key characteristic of Diffserv is that flows are aggregated in the network, so that core routers only need to distinguish a comparably small number of aggregated flows, even if those flows contain thousands or millions of individual flows.

Differentiated services are intended to provide a framework and building blocks to enable deployment of scalable service discrimination in the Internet. The differentiated services approach aims to speed deployment by separating the architecture into two major components, one of which is fairly wellunderstood and the other of which is just beginning to be understood. In this, we are guided by the original design of the Internet where the decision was made to separate the forwarding and routing components.

Packet forwarding is the relatively simple task that needs to be performed on a per-packet basis as quickly as possible. Forwarding uses the packet header to find an entry in a routing table that determines the packet's output interface. Routing sets the entries in that table and may need to reflect a range of transit and other policies as well as to keep track of route failures. Routing tables are maintained as a background process to the forwarding task.

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

[set qos](#)

[class-map](#)

[policy-map](#)

[match](#)

[class](#)

[set cos](#)

[police](#)

[cosq scheduling algorithm](#)

[traffic class](#)

[show policy-map](#)

[show class-map](#)

[show cosq algorithm](#)

[show cosq weights-bw](#)



## 32.1 set qos

This command enables differentiated services on the device. The “disable” option is used to disable the QoS feature on the device.

```
set qos { enable | disable }
```

### Syntax Description

**enable** - Enables differentiated services

**disable** - Disables differentiated services

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config)# set qos enable
```

QoS must be globally enabled prior to the execution of the class-map and policy-map mode commands.

When set as 'enabled', DiffServ Module programs the hardware and starts Protocol Operation.

When set as 'disabled', it stops protocol operation by deleting the hardware configuration.

### Related Commands

**show policy-map** - Displays the quality of service (QoS) policy maps

**show class-map** - Displays quality of service (QoS) class maps

## 32.2 class-map

This command creates a class map that is meant to be used for matching the packets to the class whose index is specified. This command is also used to enter the class-map configuration mode

The “no” form of this command is used to delete an existing class map and to return to global configuration mode

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

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

### Syntax Description

**class-map-number** - QoS class map number

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# class-map 5
```

Differentiated services must have been enabled in the device.

The class-map command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-interface basis.

The **match** command is available from the class-map configuration mode

### Related Command

**show class-map** - Displays quality of service (QoS) class maps

## 32.3 policy-map

This command is used to enter the policy-map configuration mode

In the policy-map configuration mode the user can create or modify a policy map. The “no” form of this command deletes an existing policy map and returns to the global configuration mode

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

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

### Syntax Description

**policy-map-number** - QoS Policy map number

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# policy-map 6
```

- ▶ Differentiated services must have been enabled in the device.  
The following two commands are available from the policy-map configuration mode
  - **class**
  - **exit** - Exits from the policy map configuration mode and returns to the global configuration mode

### Related Command

**show policy-map** - Displays quality of service (QoS) policy maps

## 32.4 match

This command specifies the fields in the incoming packets that are to be examined for the classification of the packets. The IP access group / MAC access group can be used as match criteria.

```
match access-group { mac-access-list | ip-access-list } <acl-index-num  
(1- 65535) >
```

### Syntax Description

**mac-access-list** - Access list created based on MAC addresses for non-IP traffic

**ip-access-list** - Access list created based on IP addresses. The IP-access list can either be defined as a standard IP-access list or an extended IP-access list.

**acl-index-num** - Specifies the ACL index range. The ACL index range for an IP standard ACL is 1 to 1000 and IP extended ACL is 1001 to 65535. The ACL index range for a MAC extended ACL is 1 to 65535.

### Mode

Class Map Configuration Mode

### Example:

```
iss (config-cmap)# match access-group mac-access-list 5
```

- ➔ Differentiated services must have been enabled in the device.  
MAC access list and IP access list must have been configured.

### Related Commands

**class-map** - Creates a class map to be used for matching the packets with the class whose name/index is specified

**show class-map** - Displays QoS Class maps

## 32.5 class

This command defines a traffic classification for the policy to act. The class-map-number that is specified in the policy map ties the characteristics for that class to the class map and its match criteria, as configured by using the class-map global configuration command. On execution of the class command, the switch enters the policy-map class configuration mode.

The “no” form of this command un-maps the class-map from the current policy-map configuration.

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

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

### Syntax Description

**class-map-number** - Class Map Number

### Mode

Policy-Map Configuration Mode

### Example:

```
iss (config-pmap)# class 5
```

- Differentiated services must have been enabled in the device.
- The policy-map global configuration command must be executed prior to using the class command. After a policy map is specified, the user can either configure a policy for new classes or modify a policy for any existing classes in that policy map.

The following configuration commands are available from the policy map class configuration mode

- **set cos**
- **police**

### Related Commands

**policy-map** - Enters the policy map configuration mode

**show policy-map** - Displays the QoS policy maps

## 32.6 set cos

This command defines the in-profile action by setting a class of service (CoS), Differentiated Services Code Point (DSCP), or IP-precedence value in the packet.

The “no” form of the command deletes the configured values.

```
set {cos <new-cos(0-7)> | ip dscp <new-dscp(0-63)> | ip precedence  
<newprecedence( 0-7)>}
```

```
no set {cos <new-cos(0-7)> | ip { dscp <new-dscp(0-63)> | precedence  
<newprecedence( 0-7)>}}
```

### Syntax Description

**cos** - New COS value assigned to the classified traffic

**ip dscp** - New DSCP value assigned to the classified traffic

**ip precedence** - New IP-precedence value assigned to the classified traffic

### Mode

Policy-Map Class Configuration Mode

### Example:

```
iss (config-pmap-c)# set cos 5
```

- ➔ To attach policy maps that contain the following elements to an ingress interface
  - set policy-map class configuration commands must be used. Moreover, the police policy-map class configuration command can be used to mark down (reduce) the DSCP value at the ingress interface.
  - Access control list (ACL) classification.
  - Per-port per-VLAN classification.

### Related Commands

**class**- Defines a traffic classification for the policy set

**policy-map** - Used to enter the policy map configuration mode

**class-map** - Creates a class map

**show policy-map** - Displays the QoS policy map configuration

## 32.7 police

This command defines a policer for the classified traffic. This command also specifies the action to be taken if the specified rate is exceeded or if there is no match for the policy configured.

```
police <rate-Kbps (64-1048572)> exceed-action {drop | policed-dscp-  
transmit <new-dscp (0-63)>}
```

### Syntax Description

**rate-Kbps** - Average traffic rate in kilo bits per second (Kbps)

**exceed-action** - Indicates the action of the switch when the specified rate is exceeded.

**drop** - drops the packet

**policed-dscp-transmit** - changes the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then sends the packet

### Mode

Policy-Map Class Configuration Mode

### Example:

```
iss (config-pmap-c)# police 128 exceed-action drop
```

Although the command-line help string displays a large range of values, the rate Kbps option cannot exceed the configured port speed. If a larger value is entered, then the switch rejects the policy map when attached to an interface.

### Related Commands

**class** - Defines a traffic classification for the policy to act

**policy-map** - Used to enter the policy map configuration mode

**class-map** - Creates a class map used for matching packets

**show policy-map** - Displays the QoS policy maps





## 32.8 cosq scheduling algorithm

This command sets the cosq scheduling algorithm. The “no” form of this command configures the scheduling algorithm to its default value strict.

```
cosq scheduling algorithm { strict | rr | wrr | deficit }
```

```
no cosq scheduling algorithm
```

### Syntax Description

**strict** - strict

**rr** - round robin

**wrr** - weighted round robin

**deficit** - deficit

### Mode

Interface Configuration mode

### Default

strict

### Example:

```
SMIS(config-if)# cosq scheduling algorithm strict
```

### Related Commands

**show cosq algorithm** - Displays the CoSq algorithm used for the interface.

**show cosq weights-bw** - Displays the CoSq weights and the bandwidth for the interface.

## 32.9 traffic class

This command sets weight and bandwidth for traffic classes.

The “no” form of this command removes the minimum and maximum bandwidth settings and resets the weight to the default value 1.

```
traffic-class <integer(0-7)> weight <integer(0-15)> [minbandwidth
<integer(64-16777152)>] [maxbandwidth <integer(64-16777152)>]
```

```
no traffic-class [<integer(0-7)>] [weight] [minbandwidth]
[maxbandwidth]
```

### Syntax Description

**traffic-class** - Configures cosq numbers

**weight** - Configures cosq weights

**minbandwidth** - Configures minimum bandwidth in kbps

**maxbandwidth** - Configures maximum bandwidth in kbps

### Mode

Interface Configuration mode

### Defaults

weight - 1

### Example:

```
SMIS(config-if)# traffic-class 1 weight 7 minbandwidth 1234
```

### Related Commands

**show cosq algorithm** - Displays the CoSq algorithm used for the interface.

**show cosq weights-bw** - Ddisplays the CoSq weights and the bandwidth for the interface.

## 32.10 show policy-map

This command displays the quality of service (QoS) policy maps, which defines the classification criteria for the incoming traffic. Policy maps can include polices that specify the bandwidth limitations and the action to take if the limits are exceeded.

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

### Syntax Description

**policy-map-num** - Policy map number

**class** - Class map number

### Mode

Privileged/User EXEC Mode

### Example:

```
SMIS# show policy-map 24
DiffServ Configurations:
-----
Quality of Service has been enabled
Policy Map 24 is not active
Class Map: 20
-----
Protocol : 255
In Profile Entry
-----
In profile action : policed-precedence 5
Out Profile Entry
-----
Metering on
burst bytes/token size : 6
Refresh count : 1000
Out profile action : drop
No Match Entry
-----
No match action : policed-precedence 5
```

### Related Commands

**policy-map** - Used to enter the policy map configuration mode

**class** - Defines a traffic classification for the policy to act

**set cos** - Defines the in-profile action by setting a CoS, DSCP or IP-precedence value in the packet

**police** - Defines a policer for the classified traffic

## 32.11 show class-map

This command displays quality of service (QoS) class maps, which defines the match criteria to classify traffic.

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

### Syntax Description

**class-map-num** - Displays the configured class map number

### Mode

Privileged/User EXEC Mode

### Example:

```
SMIS# show class-map
DiffServ Configurations:
-----
Class map 20
-----
Filter-ID : 3
Filter-Type : IP-Filter
```

### Related Commands

**class-map** - Creates a class map that is meant to be used for matching the packets to the class whose index is specified

**match** - Specifies the fields in the incoming packets that are to be examined for the classification of the packets

## 32.12 show cosq algorithm

This command displays the CoSq algorithm used for the interface.

```
show cosq algorithm [ interface <interface-type> <interface-id> ]
```

### Syntax Description

**interface-type** - Interface Type

**interface-id** - Interface ID

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# show cosq algorithm interface  
gigabitethernet 0/1
```

```
CoSq Algorithm
```

```
-----
```

```
Interface Algorithm
```

```
-----
```

```
Gi0/1 StrictPriority
```

```
.....
```

```
-----
```

## 32.13 show cosq weights-bw

This command displays the CoSq weights and the bandwidth for the interface.

```
show cosq weights-bw [ interface <interface-type> <interface-id> ]
```

### Syntax Description

**interface-type** - Interface Type

**interface-id** - Interface ID

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# show cosq weights-bw interface
```

```
gigabitethernet 0/1
```

```
CoSq Weights and Bandwidths
```

```
-----
```

Interface	CoSqId	CoSqWeight	MinBw	MaxBw	Flag
Gi0/1	0	1	0	0	2
Gi0/1	1	1	0	0	2
Gi0/1	2	1	0	0	2
Gi0/1	3	1	0	0	2
Gi0/1	4	1	0	0	2
Gi0/1	5	1	0	0	2
Gi0/1	6	1	0	0	2
Gi0/1	7	1	0	0	2
.....	.....	.....	.....	.....	.....

```
-----
```

## 33 ACL (Access Control Lists)

ACLs (Access Control Lists) filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. ACLs are used to block IP packets from being forwarded by a router.

The router examines each packet to determine whether to forward or drop or redirect the packet, based on the criteria specified within the access lists. Access list criteria can be the source address of the traffic, the destination address of the traffic, the upper-layer protocol or other information.

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

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

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

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

[ip access-list](#)

[mac access-list extended](#)

[permit - standard mode](#)

[deny - standard mode](#)

[redirect - standard mode](#)

[permit- ip/ospf/pim/protocol type](#)

[deny - ip/ospf/pim/protocol type](#)

[redirect - ip/ospf/pim/protocol type](#)

[permit tcp](#)

[deny tcp](#)



[redirect tcp](#)

[permit udp](#)

[deny udp](#)

[redirect udp](#)

[permit icmp](#)

[deny icmp](#)

[redirect icmp](#)

[ip access-group](#)

[mac access-group](#)

[permit](#)

[deny](#)

[redirect](#)

[show access-lists](#)

## 33.1 ip access-list

This command creates IP ACLs and enters the IP Access-list configuration mode.

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

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

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

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

```
ip access-list { standard { <access-list-number (1-32768)> | <access-
list-name> } | extended { <access-list-number (1-32768)> | <access-
lst-name> } }
```

```
no ip access-list { standard { <access-list-number (1-32768)> |
<access-list-name> } | extended { <access-list-number (1-32768)> |
<access-lst-name> } }
```

### Syntax Description

**standard** - Standard access-list number

**extended** - Extended access-list number

IP ACLs can be created with ACL numbers or with ACL names.

**access-list-number** – could be any number between 1 to 32768

**access-list-name** – could be any name string up to 32 characters.

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# ip access-list standard 1
```

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

### Related Commands

**permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters

**deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched

**redirect - standard mode** - Redirects traffic if the conditions defined in the redirect statement are matched

**permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched

**deny - ip/ospf/pim/protocol type**- Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched

**redirect - ip/ospf/pim/protocol type**- Redirects traffic for a particular protocol packet if the conditions defined in the redirect statement are matched

**permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters

**deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters

**redirect tcp** - Specifies the TCP packets to be redirected based on the associated parameters

**permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters

**deny udp** - Specifies the UDP packets to be rejected based on the associated parameters

**redirect udp** - Specifies the UDP packets to be redirected based on the associated parameters

**permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters

**deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters

**redirect icmp** - Specifies the ICMP packets to be redirected based on the IP address and associated parameters

**ip access-group** - Enables access control for the packets on the interface

**show access-lists** - Displays the access list configuration

## 33.2 mac access-list extended

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

```
mac access-list extended { <access-list-number (1-32768)> | <access-  
list-name> }
```

```
no mac access-list extended { <access-list-number (1-32768)> | <access-  
list-name> }
```

### Syntax Description

MAC ACLs can be created with ACL numbers or with ACL names.

access-list-number – could be any number from 1 to 32768

access-list-name – could be any name string up to 32 characters.

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# mac access-list extended 5
```

ACLs on the system perform both access control and layer 2 field classifications.

To define Layer 2 access lists, the mac access-list command must be used.

### Related Commands

**show access-lists**- Displays the access list configuration

**permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters

**deny**- Specifies the packets to be rejected based on the MAC address and the associated parameters

**redirect** - Specifies the packets to be redirected based on the MAC address and the associated parameters

## 33.3 permit - standard mode

This command specifies the packets to be forwarded depending upon the associated parameters.

Standard IP access lists use source addresses for matching operations.

```
permit { any | host <src-ip-address> | < src-ip-address> <mask> } [{  
any | host <dest-ip-address> | < dest-ip-address> <mask> } ]
```

### Syntax Description

**any|host <src-ip-address>| < src-ipaddress> <mask>** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or the host that the packet is from and the network mask to use with the source IP address

**any|host <dest-ip-address>| < dest-ip-address ><mask>** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or the host that the packet is destined for and the network mask to use with the destination IP address

### Mode

IP ACL Configuration (standard)

### Example:

```
SMIS(config-std-nacl)# permit host 100.0.0.10 host 10.0.0.1
```

### Related Commands

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched

**redirect - standard mode** - Redirects traffic if the conditions defined in the redirect statement are matched

**show access-lists-** Displays the access list configuration

## 33.4 deny - standard mode

This command denies traffic if the conditions defined in the deny statement are matched.

```
deny{ any | host <src-ip-address> | <src-ip-address> <mask> } [ { any |  
host <dest-ip-address> | <dest-ip-address> <mask> } ]
```

### Syntax Description

**any|host src-ip-address| <src-ip-address> <mask>** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source IP address

**any|host dest-ip-address| <dest-ipaddress><mask>** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination IP address

### Mode

IP ACL Configuration (standard)

### Example:

```
SMIS(config-std-nacl)# deny host 100.0.0.10 any
```

### Related Commands

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters

**redirect - standard mode** - Specifies the packets to be redirected depending upon the associated parameters

**show access-lists**-Displays the access list configuration

## 33.5 redirect - standard mode

This command redirects traffic if the conditions defined in the redirect statement are matched.

```
redirect <interface-type> <interface-id> { any | host <src-ip-address>
| <src-ip-address> <mask> } [ { any | host <dest-ip-address> | <dest-
ip-address> <mask> } ]
```

### Syntax Description

interface-type – may be any of the following:

gigabitethernet – gi

extreme-ethernet – ex

qx-ethernet – qx

interface-id - is in slot/port format for all physical interfaces

any|host src-ip-address| <src-ip-address> <mask> - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source IP address

any|host dest-ip-address| <dest-ipaddress><mask> - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination IP address

### Mode

IP ACL Configuration (standard)

### Example:

```
SMIS(config-std-nacl)# redirect gi 0/1 host 100.0.0.10 any
```

### Related Commands

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters

**deny - standard mode** - Specifies the packets to be denied depending upon the associated parameters

**show access-lists**-Displays the access list configuration

## 33.6 permit- ip/ospf/pim/protocol type

This command allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.

```
permit { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-  
ipaddress> | <src-ip-address> <mask> } { any | host <dest-ip-address> |  
<destip-address> <mask> } [ {tos <value (0-255)> | dscp <value (0-63)>}  
] [ priority <value (1-255)>]
```

### Syntax Description

**ip| ospf|pim| <protocol-type (1- 255)>** - Type of protocol for the packet. It can also be a protocol number.

**any| host <src-ip-address>| <src-ip-address> <mask>** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address.

**any|host <dest-ip-address>| <dest-ip-address> <mask>** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

**tos - Type of service. Can be of any number value from 0 to 255. This value will be matched against the value of "Type of Service" byte (2nd byte) in the IPv4 header.**

**Priority** - The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### Mode

ACL Extended Access List Configuration Mode

### Defaults

protocol-type - 255

priority - 1

### Example:

```
SMIS(config-ext-nacl)# permit 200 host 100.0.0.10 any tos 6
```



Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.

### Related Commands

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**show access-lists** - Displays the access list configuration

**deny - ip/ospf/pim/protocol type-** Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched

**redirect - ip/ospf/pim/protocol type-** Redirects traffic for a particular protocol packet if the conditions defined in the redirect statement are matched

---

## 33.7 deny - ip/ospf/pim/protocol type

This command denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.

```
deny { ip | ospf | pim | <protocol-type (1-255)> } { any | host <src-  
ipaddress> | <src-ip-address> <mask> } { any | host <dest-ip-address> |  
<destip-address> <mask> } [ {tos <value (0-255)> | dscp <value (0-63)>}  
] [ priority <value (1-255)>]
```

### Syntax Description

**ip| ospf|pim| <protocol-type (1-255)>** - Type of protocol for the packet. It can also be a protocol number.

**any| host <src-ip-address>| <src-ip-address> <mask>** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address

**any|host <dest-ip-address>| <dest-ip-address> <mask>** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

**tos** - **Type of service. Can be of any number value between 0 to 255. This value will be matched against the value of "Type of Service" byte (2nd byte) in the IPv4 header.**

**Priority** - The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### Mode

ACL Extended Access List Configuration Mode

### Defaults

protocol type - 255

priority - 1

### Example:

```
SMIS(config-ext-nacl)# deny ospf any host 10.0.0.1 tos 6
```

### Related Commands

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched

**redirect - ip/ospf/pim/protocol type-** Redirects traffic for a particular protocol packet if the conditions defined in the redirect statement are matched

**show access-lists** -Displays the access list configuration

## 33.8 redirect - ip/ospf/pim/protocol type

This command redirects traffic for a particular protocol packet if the conditions defined in the redirect statement are matched.

```
redirect <interface-type> <interface-id> { ip | ospf | pim | <protocol-
type (1-255)>} { any | host <src-ip-address> | <src-ip-address> <mask>
} { any | host <dest-ip-address> | <dest-ip-address> <mask> } [ {tos
<value (0-255)> | dscp <value (0-63)>} ] [priority <value (1-255)>]
```

### Syntax Description

interface-type – may be any of the following:

gigabitethernet – gi

extreme-ethernet – ex

qx-ethernet – qx

interface-id - is in slot/port format for all physical interfaces

ip| ospf|pim| <protocol-type (1-255)> - Type of protocol for the packet. It can also be a protocol number.

any| host <src-ip-address>| <src-ip-address> <mask> - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address

any|host <dest-ip-address>| <dest-ip-address> <mask> - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

tos - Type of service. Can be of any number value from 0 to 255. This value will be matched against the value of "Type of Service" byte (2nd byte) in the IPv4 header.

Priority - The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### Mode

ACL Extended Access List Configuration Mode

## Defaults

protocol type - 255

priority – 1

## Example:

```
SMIS(config-ext-nacl)# redirect gi 0/1 ospf any host 10.0.0.1 tos 6
```

## Related Commands

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched

**deny - ip/ospf/pim/protocol type**- Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched

**show access-lists** -Displays the access list configuration

## 33.9 permit tcp

This command specifies the TCP packets to be forwarded based on the associated parameters.

```
permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask>
} [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-
number (1- 65535)> | range <port-number (1-65535)> <port-number (1-
65535)>}] { any | host <dest-ip-address> | <dest-ip-address> <dest-
mask> } [{gt <port-number (1- 65535)> | lt <port-number (1-65535)> | eq
<port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-
65535)>}] [{ ack | rst }] [{tos <value (0-255)> |dscp <value (0-63)>}] [
priority <short (1-255)>]
```

### Syntax Description

**tcp** - Transport Control Protocol

**any| host <src-ip-address>| <src-ip-address> < src-mask >** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address

**port-number** - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.

eq=equal

lt=less than

gt=greater than

range=a range of ports; two different port numbers must be specified

**any|host <dest-ip-address> |<dest-ip-address> < dest-mask >** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

**ack** - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3).

**rst** - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3).

**tos** - Type of service. Can be of any number value from 0 to 255. This value will be matched against the value of "Type of Service" byte (2nd byte) in the IPv4 header.

**priority**

- The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### Mode

ACL Extended Access List Configuration Mode

### Defaults

tos-value - 0

ack - 'any' (3) [indicates that the TCP ACK bit will not be checked to decide the action]

rst - any' (3) [indicates that the TCP RST bit will not be checked to decide the action]

### Example:

```
SMIS(config-ext-nacl)# permit tcp any 10.0.0.1 255.255.255.255
```

### Related Commands

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**show access-lists** - Displays the access list configuration

**deny tcp** Specifies the TCP packets to be rejected based on the associated parameters

**redirect tcp** Specifies the TCP packets to be redirected based on the associated parameters

## 33.10 deny tcp

This command specifies the TCP packets to be rejected based on the associated parameters.

```
deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask>
} [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-
number (1- 65535)> | range <port-number (1-65535)> <port-number (1-
65535)>}] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask>
} [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-
number (1-65535)> |range <port-number (1-65535)> <port-number (1-
65535)>}] [{ ack | rst }] [{tos <value (0-255)> | dscp <value (0-63)>}] [
priority <short (1-255)>]
```

### Syntax Description

**Tcp** - Transmission control protocol

**any| host <src-ip-address>| <src-ip-address> <src-mask>** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address

**port-number** - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.

eq=equal

lt=less than

gt=greater than

range=a range of ports; two different port numbers must be specified

**any|host <dest-ip-address>| <dest-ip-address> <dest-mask>** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

**ack** - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3)

**rst** - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3)

**tos** - Type of service. Can be of any number value between 0 to 255.

**This value will be matched against the value of "Type of Service" byte (2nd byte) in the IPv4 header.**



**Priority** - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### **Mode**

ACL Extended Access List Configuration Mode

### **Defaults**

tos-value - 0

ack - 'any' (3) [indicates that TCP ACK bit will not be checked to decide the action]

rst - any' (3) [indicates that TCP RST bit will not be checked to decide the action]

### **Example:**

```
SMIS(config-ext-nacl)# deny tcp 100.0.0.10 255.255.255.0 eq 20 any
```

### **Related Commands**

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**show access-lists** - Displays the access list configuration

**permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters

**redirect tcp** Specifies the TCP packets to be redirected based on the associated parameters

## 33.11 redirect tcp

This command specifies the TCP packets to be redirected based on the associated parameters.

```
redirect <interface-type> <interface-id> tcp {any | host <src-ip-
address> | <src-ip-address> <src-mask> } [{gt <port-number (0-65535)> |
lt <port-number (1-65535)> |eq <port-number (0-65535)> | range <port-
number (0-65535)> <port-number (0-65535)>}] { any | host <dest-ip-
address> | <dest-ip-address> <dest-mask> } [{gt <port-number (0-65535)>
| lt <port-number (1-65535)> | eq <port-number (0-65535)> | range
<port-number (0-65535)> <port-number (0-65535)>}] [{ ack | rst }] [{tos
<value (0-255)> | dscp <value (0-63)>}] [ priority <short(1-255)>]
```

### Syntax Description

interface-type – may be any of the following:

gigabitethernet – gi

extreme-ethernet – ex

qx-ethernet – qx

interface-id - is in slot/port format for all physical interfaces

**Tcp** - Transmission control protocol

**any| host <src-ip-address>| <src-ip-address> <src-mask>** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address

**port-number** - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.

eq=equal

lt=less than

gt=greater than

range=a range of ports; two different port numbers must be specified

**any|host <dest-ip-address>| <dest-ip-address> <dest-mask>** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

**ack** - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3)

**rst** - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3)

**tos** - Type of service. Can be of any number value from 0 to 255. This value will be matched against the value of "Type of Service" byte (2nd byte) in the IPv4 header.

**Priority** - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### Mode

ACL Extended Access List Configuration Mode

### Defaults

tos-value - 0

ack - 'any' (3) [indicates that TCP ACK bit will not be checked to decide the action]

rst - any' (3) [indicates that TCP RST bit will not be checked to decide the action]

### Example:

```
SMIS(config-ext-nacl)# redirect gi 0/1 tcp 100.0.0.10 255.255.255.0 eq  
20 any
```

### Related Commands

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**show access-lists** - Displays the access list configuration

**permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters

**deny tcp** Specifies the TCP packets to be denied based on the associated parameters

## 33.12 permit udp

This command specifies the UDP packets to be forwarded based on the associated parameters.

```
permit udp { any | host <src-ip-address> | <src-ip-address> <src-
mask> } [ { gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq
<port-number (1- 65535)> | range <port-number (1-65535)> <port-number
(1-65535)> } ] { any | host <dest-ip-address> | <dest-ip-address> <dest-
mask> } [ { gt <port-number (1- 65535)> | lt <port-number (1-65535)> | eq
<port-number (1-65535)> | range <portnumber (1-65535)> <port-number (1-
65535)> } ] [ { tos <value (0-255)> | dscp <value (0-63)> } ] [ priority
<short (1-255)> ]
```

### Syntax Description

**udp** - User Datagram Protocol

**any| host <src-ip-address>| <src-ip-address> <src-mask>** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address

**port-number** - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.

eq=equal

lt=less than

gt=greater than

range=a range of ports; two different port numbers must be specified

**any|host <dest-ip-address>| <dest-ip-address> <dest-mask>** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

**tos** - **Type of service**. Can be of any number value from 0 to 255. This value will be matched against the value of "Type of Service" byte (2nd byte) in the IPv4 header.

**Priority** - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### Mode

ACL Extended Access List Configuration Mode

**Example:**

```
SMIS(config-ext-nacl)# permit udp any gt 65000 any dscp 1
```

**Related Commands**

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**show access-lists** - Displays the access list configuration

**deny udp** - Specifies the UDP packets to be rejected based on the associated parameters

**redirect udp** - Specifies the UDP packets to be redirected based on the associated parameters

## 33.13 deny udp

This command specifies the UDP packets to be rejected based on the associated parameters.

```
deny udp { any | host <src-ip-address> | <src-ip-address> <src-
mask> } [ { gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq
<port-number (1- 65535)> | range <port-number (1-65535)> <port-number
(1-65535)> } ] [ { any | host <dest-ip-address> | <dest-ip-address> <dest-
mask> } ] [ { gt <port-number (1- 65535)> | lt <port-number (1-65535)> | eq
<port-number (1-65535)> | range <portnumber (1-65535)> <port-number (1-
65535)> } ] [ { tos <value (0-255)> | dscp <value (0-63)> } ] [ priority <short
(1-255)> ]
```

### Syntax Description

**udp** - User Datagram Protocol

**any| host <src-ip-address>| <src-ip-address> <src-mask>** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address

**port-number** - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.

eq=equal

lt=less than

gt=greater than

range=a range of ports; two different port numbers must be specified

**any|host <dest-ip-address> |<dest-ip-address> <dest-mask>** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

**tos** - **Type of service**. Can be of any number value from 0 to 255. This value will be matched against the value of "Type of Service" byte (2nd byte) in the IPv4 header.

**Priority** - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### Mode

ACL Extended Access List Configuration Mode

**Example:**

```
SMIS(config-ext-nacl)# deny udp host 10.0.0.1 any eq 20
```

**Related Commands**

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**show access-lists** - Displays the access list configuration

**permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters

**redirect udp** - Specifies the UDP packets to be redirected based on the associated parameters

## 33.14 redirect udp

This command specifies the UDP packets to be redirected based on the associated parameters.

```
redirect <interface-type> <interface-id> udp { any | host <src-ip-
address> | <src-ip-address> <src-mask>} [{gt <port-number (0-65535)> |
lt <port-number (1-65535)> | eq <port-number (0-65535)> | range <port-
number (0-65535)> <port-number (0-65535)>}] { any | host <dest-ip-
address> | <dest-ip-address> <dest-mask> } [{ gt <port-number (0-
65535)> | lt <port-number (1-65535)> | eq <port-number (0-65535)> |
range <port-number (0-65535)> <port-number (0-65535)>}] [{tos <value
(0-255)> | dscp <value (0-63)>}] [ priority <(1-255)>]
```

### Syntax Description

interface-type – may be any of the following:

gigabitethernet – gi

extreme-ethernet – ex

qx-ethernet – qx

interface-id - is in slot/port format for all physical interfaces

udp - User Datagram Protocol

**any| host <src-ip-address>| <src-ip-address> <src-mask>** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address

**port-number** - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.

eq=equal

lt=less than

gt=greater than

range=a range of ports; two different port numbers must be specified

**any|host <dest-ip-address> |<dest-ip-address> <dest-mask>** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

**tos** - **Type of service**. Can be of any number value from 0 to 255. This value will be matched against the value of "Type of Service" byte (2nd byte) in the IPv4 header.



**Priority** - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

**Mode**

ACL Extended Access List Configuration Mode

**Example:**

```
SMIS(config-ext-nacl)# redirect gi 0/1 udp host 10.0.0.1 any eq 20
```

**Related Commands**

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**show access-lists** - Displays the access list configuration

**permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters

**deny udp** - Specifies the UDP packets to be denied based on the associated parameters

## 33.15 permit icmp

This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.

```
permit icmp {any |host <src-ip-address>|<src-ip-address> <mask>}{any |  
host <dest-ip-address> | <dest-ip-address> <mask> }[<message-type (0-  
255)>] [<message-code (0-255)>] [ priority <value (1-255)>]
```

### Syntax Description

**icmp** - Internet Control Message Protocol

**any| host <src-ip-address> |<src-ip-address> <mask>** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address

**any|host <dest-ip-address>| <dest-ip-address> <mask>** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

**message-type** - Message type

**message-code** - ICMP Message code

**priority** - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### Mode

ACL Extended Access List Configuration Mode

### Defaults

message-type/message code - 255

### Example:

```
SMIS(config-ext-nacl)# permit icmp any any
```

The ICMP message type can be one of the following:

### Value ICMP type

0 Echo reply

3 Destination unreachable

4 Source quench

5 Redirect

- 8 Echo request
- 11 Time exceeded
- 12 Parameter problem
- 13 Timestamp request
- 14 Timestamp reply
- 15 Information request
- 16 Information reply
- 17 Address mask request
- 18 Address mask reply
- 155 No ICMP type

The ICMP code can be any of the following:

**- Value ICMP code**

- 0 Network unreachable
- 1 Host unreachable
- 2 Protocol unreachable
- 3 Port unreachable
- 4 Fragment need
- 5 Source route fail
- 6 Destination network unknown
- 7 Destination host unknown
- 8 Source host isolated
- 9 Destination network administratively prohibited
- 10 Destination host administratively prohibited
- 11 Network unreachable TOS
- 12 Host unreachable TOS
- 255 No ICMP code

**Related Commands**

**ip access-list** - Created IP ACLs and enters the IP Access-list configuration mode

**show access-lists** - Displays the access list configuration

**deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters

**redirect icmp** - Specifies the ICMP packets to be redirected based on the IP address and associated parameters



## 33.16 deny icmp

This command specifies the ICMP packets to be rejected based on the IP address and associated parameters.

```
deny icmp {any |host <src-ip-address>|<src-ip-address> <mask>}{any |  
host <dest-ip-address> | <dest-ip-address> <mask> }[<message-type (0-  
255)>] [<message-code (0-255)>] [ priority <value (1-255)>]
```

### Syntax Description

**icmp** - Internet Control Message Protocol

**any| host <src-ip-address>| <src-ip-address> <mask>** - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address

**any|host <dest-ip-address>| <dest-ip-address> <mask>** - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

**message-type** - Message type

**message-code** - ICMP Message code

**priority** - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### Mode

ACL Extended Access List Configuration Mode

### Defaults

message-type / message code - 255

### Example:

```
Smis(config-ext-nacl)# deny icmp host 100.0.0.10 10.0.0.1  
255.255.255.255
```

The ICMP message type can be one of the following:

### Value ICMP type

0 Echo reply

3 Destination unreachable

4 Source quench

5 Redirect  
8 Echo request  
11 Time exceeded  
12 Parameter problem  
13 Timestamp request  
14 Timestamp reply  
15 Information request  
16 Information reply  
17 Address mask request  
18 Address mask reply  
155 No ICMP type

The ICMP code can be any of the following:

**Value ICMP code**

0 Network unreachable  
1 Host unreachable  
2 Protocol unreachable  
3 Port unreachable  
4 Fragment need  
5 Source route fail  
6 Destination network unknown  
7 Destination host unknown  
8 Source host isolated  
9 Destination network administratively prohibited  
10 Destination host administratively prohibited  
11 Network unreachable TOS  
12 Host unreachable TOS  
255 No ICMP code

**Related Commands**

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**show access-lists** - Displays the access list configuration

**permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters

**redirect icmp** - Specifies the ICMP packets to be redirected based on the IP address and associated parameters

## 33.17 redirect icmp

This command specifies the ICMP packets to be redirected based on the IP address and associated parameters.

```
redirect <interface-type> <interface-id> icmp {any | host <src-ip-  
address>|<src-ip-address> <mask>} {any | host <dest-ip-address> |  
<dest-ip-address> <mask> } [<message-type (0-255)>] [<message-code (0-  
255)>] [priority <(1-255)>]
```

### Syntax Description

interface-type – may be any of the following:

gigabitethernet – gi

extreme-ethernet – ex

qx-ethernet – qx

interface-id - is in slot/port format for all physical interfaces

icmp - Internet Control Message Protocol

any| host <src-ip-address>| <src-ip-address> <mask> - Source IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is from and the network mask to use with the source address

any|host <dest-ip-address>| <dest-ip-address> <mask> - Destination IP address can be 'any' or the word 'host' and the dotted decimal address or number of the network or the host that the packet is destined for and the network mask to use with the destination address

message-type - Message type

message-code - ICMP Message code

priority - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rule. A higher value of 'filter priority' implies a higher priority.

### Mode

ACL Extended Access List Configuration Mode

### Defaults

message-type / message code - 255

### Example:

```
Smis(config-ext-nacl)# deny icmp host 100.0.0.10 10.0.0.1  
255.255.255.255
```

The ICMP message type can be one of the following:

**Value ICMP type**

- 0 Echo reply
- 3 Destination unreachable
- 4 Source quench
- 5 Redirect
- 8 Echo request
- 11 Time exceeded
- 12 Parameter problem
- 13 Timestamp request
- 14 Timestamp reply
- 15 Information request
- 16 Information reply
- 17 Address mask request
- 18 Address mask reply
- 155 No ICMP type

The ICMP code can be any of the following:

**Value ICMP code**

- 0 Network unreachable
- 1 Host unreachable
- 2 Protocol unreachable
- 3 Port unreachable
- 4 Fragment need
- 5 Source route fail
- 6 Destination network unknown
- 7 Destination host unknown
- 8 Source host isolated
- 9 Destination network administratively prohibited
- 10 Destination host administratively prohibited
- 11 Network unreachable TOS
- 12 Host unreachable TOS
- 255 No ICMP code

**Related Commands**

`ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode



**show access-lists** - Displays the access list configuration

**permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters

**deny icmp** - Specifies the ICMP packets to be denied based on the IP address and associated parameters

## 33.18 ip access-group

This command enables access control for the packets on the interface. It controls access to a Layer 2 or Layer 3 interface. The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out.

```
ip access-group <access-list-number (1-32768)> {in | out}
```

```
no ip access-group [<access-list-number (1-32768)>] {in | out}
```

### Syntax Description

**access-list-number** - IP access control list number

**in** - Inbound packets

**out** - Outbound packets

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# ip access-group 1 in
```

### Related Commands

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**show access-lists** - Displays the access list configuration

## 33.19 mac access-group

This command applies a MAC access control list (ACL) to a Layer 2 interface. The no form of this command can be used to remove the MAC ACLs from the interface.

```
mac access-group <access-list-number (1-32768)> {in | out}
```

```
no mac access-group [<access-list-number (1-32768)>] {in | out}
```

### Syntax Description

**access-list-number** - Access List Number

**in** - Inbound packets

**out** - Outbound packets

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# mac access-group 5 in
```

MAC access list must have been created.

### Related Commands

**mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user

**show access-lists** - Displays the access list statistics

## 33.20 permit

This command specifies the packets to be forwarded based on the MAC address and the associated parameters, that is, this command allows non-IP traffic to be forwarded if the conditions are matched.

```
permit { any | host <mac_addr> } { any | host <mac_addr> } [ { aarp |
amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |
etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps |
netbios | vines-echo | vines-ip | xns-id | <short (0-65535)> } ] [
encaptype <integer (1-65535)> ] [vlan <vlan-id (1-4069)>] [ priority
<short (1-255)>]
```

### Syntax Description

**<mac\_addr>** - Source and Destination MAC address to be matched with the packet

**Aarp** - Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address

**Amber** - EtherType DEC-Amber

**dec-spanning** - EtherType Digital Equipment Corporation (DEC) spanning tree

**decent-iv** - EtherType DECnet Phase IV protocol

**diagnostic** - EtherType DEC-Diagnostic

**dsm** - EtherType DEC-DSM/DDP

**etype-6000** - EtherType 0x6000

**etype-8042** - EtherType 0x8042

**lat** - EtherType DEC-LAT

**lavc-sca** - EtherType DEC-LAVC-SCA

**mop-console** - EtherType DEC-MOP Remote Console

**mop-dump** - EtherType DEC-MOP Dump

**msdos** - EtherType DEC-MSDOS

**mumps** - EtherType DEC-MUMPS

**netbios** - EtherType DEC- Network Basic Input/Output System (NETBIOS)

**vines-echo** - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems

**vines-ip** - EtherType VINES IP

**xns-id** - EtherType Xerox Network Systems (XNS) protocol suite

**encaptype** - Encapsulation Type

**vlan** - VLAN ID to be filtered

**priority** - The priority of the L2 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority

### Mode

ACL MAC Configuration Mode

### Defaults

vlan-id - 0

priority - 1

### Example:

```
SMIS(config-ext-macl)# permit host 00:11:22:33:44:55 any  
arp priority 10
```

MAC access list must have been created.

### Related Commands

**mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user

**mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface

**deny** - Specifies the packets to be rejected based on the MAC address and the associated parameters

**redirect** - Specifies the packets to be redirected based on the MAC address and the associated parameters

**show access-lists** - Displays the access list statistics

## 33.21 deny

This command specifies the packets to be rejected based on the MAC address and the associated parameters.

```
deny { any | host <mac_addr> } { any | host <mac_addr> } [ { aarp |
amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |
etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps |
netbios | vines-echo | vines-ip | xns-id | <short (0-65535)> } ] [
encaptype <integer (1-65535)> ] [ vlan <vlan-id (1-4069)>] [ priority
<short (1-255)>]
```

### Syntax Description

**any | host <mac\_addr>** - Source MAC address to be matched with the packet

**any | host <mac\_addr>** - Destination MAC address to be matched with the packet

**aarp** - Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address

**amber** - EtherType DEC-Amber

**dec-spanning** - EtherType Digital Equipment Corporation (DEC) spanning tree

**decent-iv** - EtherType DECnet Phase IV protocol

**diagnostic** - EtherType DEC-Diagnostic

**dsm** - EtherType DEC-DSM/DDP

**etype-6000** - EtherType 0x6000

**etype-8042** - EtherType 0x8042

**lat** - EtherType DEC-LAT

**lavc-sca** - EtherType DEC-LAVC-SCA

**mop-console** - EtherType DEC-MOP Remote Console

**mop-dump** - EtherType DEC-MOP Dump

**msdos** - EtherType DEC-MSDOS

**mumps** - EtherType DEC-MUMPS

**netbios** - EtherType DEC- Network Basic Input/Output System (NETBIOS)

**vines-echo** - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems

**vines-ip** - EtherType VINES IP

**xns-id** - EtherType Xerox Network Systems (XNS) protocol suite

**encaptype** - Encapsulation Type

**vlan** - VLAN ID to be filtered

**priority** - The priority of the L2 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### Mode

ACL MAC Configuration Mode

### Defaults

vlan-id - 0

priority - 1

### Example:

```
SMIS(config-ext-macl)# deny any host 00:11:22:33:44:55
priority 200
```

MAC access list must have been created.

### Related Commands

**mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user

**mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface

**permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters

**redirect** - Specifies the packets to be redirected based on the MAC address and the associated parameters

**show access-lists** - Displays the access list statistics

## 33.22 redirect

This command specifies the packets to be redirected based on the MAC address and the associated parameters.

```
redirect <interface-type> <interface-id> { any | host <src-mac-
address> } { any | host <dest-mac-address> } [aarp | amber | dec-spanning
| decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-
sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo |
vines-ip | xns-id | <protocol (0-65535)>] [ encapsype <value (1-
65535)>] [ Vlan <vlan-id (1-4069)>] [priority <value (1-255)>]
```

### Syntax Description

interface-type – may be any of the following:

gigabitethernet – gi

extreme-ethernet – ex

qx-ethernet – qx

interface-id - is in slot/port format for all physical interfaces

**any | host <mac\_addr>** - Source MAC address to be matched with the packet

**any | host <mac\_addr>** - Destination MAC address to be matched with the packet

**aarp** - EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address

**amber** - EtherType DEC-Amber

**dec-spanning** - EtherType Digital Equipment Corporation (DEC) spanning tree

**decent-iv** - EtherType DECnet Phase IV protocol

**diagnostic** - EtherType DEC-Diagnostic

**dsm** - EtherType DEC-DSM/DDP

**etype-6000** - EtherType 0x6000

**etype-8042** - EtherType 0x8042

**lat** - EtherType DEC-LAT

**lavc-sca** - EtherType DEC-LAVC-SCA

**mop-console** - EtherType DEC-MOP Remote Console

**mop-dump** - EtherType DEC-MOP Dump

**msdos** - EtherType DEC-MSDOS

**mumps** - EtherType DEC-MUMPS

**netbios** - EtherType DEC- Network Basic Input/Output System (NETBIOS)



**vines-echo** - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems

**vines-ip** - EtherType VINES IP

**xns-id** - EtherType Xerox Network Systems (XNS) protocol suite

**encaptype** - Encapsulation Type

**vlan** - VLAN ID to be filtered

**priority** - The priority of the L2 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

### Mode

ACL MAC Configuration Mode

### Defaults

vlan-id - 0

priority - 1

### Example:

```
SMIS(config-ext-macl)# redirect gi 0/1 any host 00:11:22:33:44:55
priority 200
```

MAC access list must have been created.

### Related Commands

**mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user

**mac access-group** - Applies a MAC access control list (ACL) to a Layer 2 interface

**permit** - Specifies the packets to be forwarded based on the MAC address and the associated parameters

**deny** - Specifies the packets to be denied based on the MAC address and the associated parameters

**show access-lists** - Displays the access list statistics

## 33.23 show access-lists

This command displays the access lists configuration.

```
show access-lists [{ip | mac}] <access-list-number (1-32768)> ]
```

### Syntax Description

**ip** - IP Access List

**mac** - MAC Access List

### Mode

Privileged/User EXEC Mode

### Example:

```
SMIS# show access-lists
SMIS# show access-lists ip 1
SMIS# show access-lists mac 1
```

### Related Commands

**ip access-list** - Creates IP ACLs and enters the IP Access-list configuration mode

**mac access-list extended** - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user

**permit - standard mode** - Specifies the packets to be forwarded depending upon the associated parameters

**deny - standard mode** - Denies traffic if the conditions defined in the deny statement are matched

**redirect - standard mode** - Redirects traffic if the conditions defined in the redirect statement are matched

**permit- ip/ospf/pim/protocol type** - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched

**deny - ip/ospf/pim/protocol type** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched

**redirect - ip/ospf/pim/protocol type** - Redirects traffic for a particular protocol packet if the conditions defined in the redirect statement are matched

**permit tcp** - Specifies the TCP packets to be forwarded based on the associated parameters

**deny tcp** - Specifies the TCP packets to be rejected based on the associated parameters

**redirect tcp** - Specifies the TCP packets to be redirected based on the associated parameters

**permit udp** - Specifies the UDP packets to be forwarded based on the associated parameters

**deny udp** - Specifies the UDP packets to be rejected based on the associated parameters

**redirect udp** - Specifies the UDP packets to be redirected based on the associated parameters

**permit icmp** - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters

**deny icmp** - Specifies the ICMP packets to be rejected based on the IP address and associated parameters

**redirect icmp** - Specifies the ICMP packets to be redirected based on the IP address and associated parameters

**ip access-group** - Enables access control for the packets on the interface

## 34 Loop protection

Loop protection feature helps to detect and prevent network loops caused by unmanaged network devices. This loop protection feature is independent of the spanning tree protocol. This can be used when the switches are connected to unmanaged devices where spanning tree cannot prevent network loops.

This feature detects networks loops by transmitting Ethernet control packets. The User can configure to disable the loop detected ports for a specific period.

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

[loop-protect](#)

[loop\\_protect - interface](#)

[loop-protect disable-period](#)

[loop-protect receive-action](#)

[loop-protect transmit-interval](#)

[show loop-protect](#)

## 34.1 loop-protect

This command enables or disables the loop protection feature globally on the switch. To enable loop protection on ports, the loop protect command needs to be configured on the corresponding port interfaces also. To enable loop protection on ports, refer to the section [loop protect – interface](#).

Loop protection feature is disabled by default.

```
loop-protect {enable | disable}
```

### Syntax Description

enable – Enables the loop protection feature

disable – Disables the loop protection feature

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config)# loop-protect enable
```

### Related Commands

show loop-protect – Displays the loop protection feature status.

## 34.2 loop-protect - interface

This command enables the loop protection feature on the port interface. The “no” form of this command disables the loop protection feature on the port interface.

To use the loop protection feature on any ports, this feature need to be enabled globally also on the switch. To enable the loop protection feature globally, refer the section [loop protect](#).

Loop protection feature is disabled by default on all ports.

**loop-protect**

**no loop-protect**

### **Mode**

Interface Configuration Mode

### **Defaults**

disable

### **Example:**

```
SMIS(config-if)# loop-protect enable
```

### **Related Commands**

show loop-protect – Displays the loop protection feature status.

## 34.3 loop-protect disable-period

Switch disables (shuts down) the loop detected ports.

This command configures the disable period for which the loop detected ports are kept down.

By default disable period value is 0 which means the loop detected ports are kept down until user enables it manually.

The no form of this command removes the configured disable period value and reset it to the default value 0.

```
loop-protect disable-period <integer(0-604800)>
```

```
no loop-protect disable-period
```

### Syntax Description

**disable-period** - number of seconds the loop detected ports are kept down.

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config)# loop-protect disable-period 30
```

### Related Commands

show loop-protect – Displays the loop protection disable period information.

## 34.4 loop-protect receive-action

When a loop is detected switch disables the port from which the loop protection packets originated. This command can be used to configure not to disable the port when loop is detected.

The no form of this command resets the receive action to the default value send-disable.

```
loop-protect receive-action {send-disable| no-disable}
```

```
no loop-protect receive-action
```

### Syntax Description

send-disable – disables the port from which the loop protection packets originated are getting looped

no-disable – loop detected ports are not disabled

### Mode

Global Configuration Mode

### Defaults

send-disable

### Example:

```
SMIS(config)# loop-protect receive-action no-disable
```

### Related Commands

show loop-protect – Displays the loop protection receive action information.



## 34.5 loop-protect transmit-interval

When loop protection feature is enabled, switch transmits Ethernet control frames periodically to detect the network loops. By default Ethernet control frames are sent once every 5 seconds. This command helps to configure the period on which the Ethernet control frames are transmitted.

The “no” form of this command resets the transmit interval period to the default value of 5 seconds.

```
loop-protect transmit-interval <integer(1-10)>
```

```
no loop-protect transmit-interval
```

### Syntax Description

Transmit-interval – number of seconds between subsequent Ethernet control frames sent out

### Mode

Global Configuration Mode

### Defaults

5

### Example:

```
SMIS(config)# loop-protect transmit-interval 10
```

### Related Commands

show loop-protect – Displays the loop protection transmit interval information.

## 34.6 show loop-protect

This command displays the loop protection configuration information.

**show loop-protect**

**Mode**

Privileged/User EXEC Mode

**Example:**

```
SMIS# show loop-protect
```

```
Loop Protection      : Enabled
Transmit Interval   : 5 seconds
Receive action      : send-disable
Disable Period      : 0 (Keep Disabled)
```

Loop Protection Configured Interfaces

Interface	Status	Loop-Detected
Gi0/1	Down	No
Gi0/2	Down	No

**Related Commands**

loop-protect – Enable or disable the loop protection feature

loop-protect - interface – Enable or disable the loop protection feature on port interfaces

loop-protect disable-period – Configures the time for which the loop detected ports are kept down

loop-protect receive-action – Configures the action to be taken when loop a loop is detected

loop-protect transmit-interval – Configures the interval on which loop detection packets are sent

## 35 Link Status Tracking

Link status tracking feature helps to control the link status of downstream interfaces based on the link status of upstream interfaces.

The interfaces connected to servers and other end devices are called downstream interfaces. And the uplink interfaces of the switches are referred as upstream interfaces.

The link status tracking feature dynamically changes the link status of downstream interfaces depending on the link status of upstream interfaces. When the link status of one or more of the upstream interfaces is “up”, it maintains the link status of all the dependent downstream interfaces as “up”. When all the upstream interfaces are “down”, it brings down all the dependent downstream interfaces. This helps servers to choose alternate interfaces to send traffic.

User can configure multiple groups of upstream and downstream interfaces for independent link status tracking among different groups.

The list of CLI commands for the configuration of link status tracking is as follows:

[link-status-tracking](#)

[link-status-tracking group](#)

[link-status-tracking group – interface](#)

[show link-status-tracking](#)

## 35.1 link-status-tracking

This command enables or disables the link status tracking feature.

Link status tracking feature is disabled by default.

```
link-status-tracking {enable | disable}
```

### Syntax Description

enable – Enables the link status tracking feature

disable – Disables the link status tracking feature

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config)# link-status-tracking enable
```

### Related Commands

show link-status-tracking – Displays the link status tracking feature information.

## 35.2 link-status-tracking group

This command creates the link status tracking groups. The “no” form of this command removes the configured link status tracking groups.

```
link-status-tracking group <short(1-1024)>
```

```
no link-status-tracking group <short(1-1024)>
```

### Syntax Description

group – Any number between 1 to 1024

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# link-status-tracking group 1
```

### Related Commands

show link-status-tracking – Displays the link status tracking feature information.

## 35.3 link-status-tracking group - interface

This command adds the interfaces as either downstream or upstream interfaces to the link status tracking groups.

The “no” form of this command removes the interfaces from the link status tracking groups.

```
link-status-tracking group <short(1-1024)> {upstream | downstream}
```

```
no link-status-tracking
```

### Syntax Description

group – Any number between 1 to 1024

upstream – configure this interface as the upstream interface for the given group

downstream - configure this interface as the downstream interface for the given group

### Mode

Interface Configuration Mode

### Example:

```
SMIS(config-if)# link-status-tracking group 1 upstream
```

### Related Commands

show link-status-tracking – Displays the link status tracking feature information.

## 35.4 show link-status-tracking

This command displays the link status tracking configuration information.

If the group number given it displays the information specific to the given groups. If group is not given, it displays the information for all the configured groups.

**show link-status-tracking [group <short(1-1024)>]**

### Syntax Description

group – Any number between 1 to 1024

### Mode

Privileged/User EXEC Mode

### Example:

```
SMIS# show link-status-tracking
```

```
Link Status Tracking is Enabled
```

```
Group :1 down
```

```
Upstream Interfaces:
```

```
Ex0/1 (down)
```

```
Downstream Interfaces:
```

```
Gi0/1 (Dis)      Gi0/2 (Dis)      Gi0/3 (Dis)      Gi0/4 (Dis)      Gi0/5 (Dis)
Gi0/6 (Dis)      Gi0/7 (Dis)      Gi0/8 (Dis)      Gi0/9 (Dis)      Gi0/10 (Dis)
Gi0/11 (Dis)     Gi0/12 (Dis)     Gi0/13 (Dis)     Gi0/14 (Dis)     Gi0/15 (Dis)
Gi0/16 (Dis)     Gi0/17 (Dis)     Gi0/18 (Dis)     Gi0/19 (Dis)     Gi0/20 (Dis)
```

```
Group :2 down
```

```
Upstream Interfaces:
```

```
Ex0/2 (down)
```

```
Downstream Interfaces:
```

### Related Commands

link-status-tracking – enables or disables the link status tracking feature

link-status-tracking group – creates or deletes the link status tracking groups

link-status-tracking group – interface – adds or removes the interfaces in to link status tracking groups.



## 36 Data Center Bridging

Data Center Bridging (DCB) provides lossless Ethernet connectivity for SAN (Storage Area Network) applications. This is achieved by using the Data Center Bridging eXchange (DCBX) protocol, in the form of LLDP TLVs, exchanged between the link partners to create a lossless Ethernet link. Supermicro's DCBX-capable switch products support the CEE standard, widely supported by many DCB devices.

Since DCBX protocol messages are encapsulated in LLDP PDUs, DCBX link stability relies on a well-configured LLDP environment. DCBX requires exactly one LLDP link partner to be a DCBX peer, multiple LLDP neighbours advertising DCBX TLVs are disallowed.

This feature is supported only on the following switch models

SBM-XEM-X10SM

SSE-X24S/R

The DCBX configuration can be divided into two parts:

1. CEE-Map configurations
2. Interface configurations

The first, CEE-Map is a set of DCBX settings. It consists of the following elements:

1. Priority to Priority Group (PG) mapping,
2. Bandwidth percentage for each PG, and
3. PFC for each priority and PG

Up to 4 CEE-Maps can be defined, each DCBX-capable interface can choose to associate with any one of the CEE-Maps, the settings in the associated CEE-Map will be encapsulated in the form of LLDP TLVs, and sent to the peer side for DCBX configurations.

The second is interface configuration mode. The advertisement, willing bit, and enable bit of DCBX TLVs can be controlled here. The commands of this part are described in LLDP section. This section lists the CEE-Map commands:

Priority Group (PG) Declaration and Bandwidth Allocation

[group](#)

[group-bandwidth](#)

Priority-to-PG Mapping Manipulations

[priority](#)

[pri2pg](#)

Priority-based Flow Control (PFC) Settings

[pfc group](#)

[pfc priority](#)

and related commands in interface configuration mode:

[cee](#)

[dcbx cee](#)

## 36.1 group

This command sets a description string to the specified group, and the “no” form of this command resets to default.

```
group <id(0-7,15)> description {<string(63)>}
no group <id(0-7,15)>
```

### Syntax Description

<id> - The priority-group ID (PGID)  
 <string> - The description string

### Mode

Config-CEE-Map mode

### Example:

```
SMIS(config)# cee-map 2
SMIS(config-cee-map)# group 4 description SAN-2
SMIS(config-cee-map)# end
SMIS# show cee-map 2
```

```
...
Group Bandwidht(%) PFC Description
-----
0      10 No LAN
1      11 Yes SAN
2      12 No
3      11 No
4      13 No SAN-2
5      11 No
6      14 No
7      18 No
15     MAX No
```

### Defaults

"LAN" for PG 0, "SAN" for PG 1, and empty string for the others.

### Related Commands

show cee-map - displays the CEE-MAP settings

## 36.2 group-bandwidth

This command allocates the maximum egress bandwidth as a percentage for each priority-group (PG). The no form of this command resets to the default allocation. Note that the sum of all bandwidth percentages must be 100. A PG can utilize all of the egress bandwidth if other PGs don't reach their allocated maximum percentage, hence any PG assigned 0% will not necessarily stop transmission, it can still use any unused bandwidth.

```
group-bandwidth <pg0_bw> <pg1_bw> <pg2_bw> <pg3_bw> <pg4_bw> <pg5_bw>
<pg6_bw> <pg7_bw>
no group-bandwidth
```

### Syntax Description

<pg0\_bw> - The percentage (0-100) of egress bandwidth for PG 0.  
 <pg1\_bw> - The percentage (0-100) of egress bandwidth for PG 1.  
 <pg2\_bw> - The percentage (0-100) of egress bandwidth for PG 2.  
 <pg3\_bw> - The percentage (0-100) of egress bandwidth for PG 3.  
 <pg4\_bw> - The percentage (0-100) of egress bandwidth for PG 4.  
 <pg5\_bw> - The percentage (0-100) of egress bandwidth for PG 5.  
 <pg6\_bw> - The percentage (0-100) of egress bandwidth for PG 6.  
 <pg7\_bw> - The percentage (0-100) of egress bandwidth for PG 7.

### Mode

Config-CEE-Map mode

### Example:

```
SMIS(config)#
SMIS(config)# cee-map 2
SMIS(config-cee-map)# group-bandwidth 10 11 12 13 14 15 16 9
SMIS(config-cee-map)# end
SMIS# show cee-map 2
```

```
...
Group Bandwidht(%) PFC Description
-----
 0      10 No LAN
 1      11 Yes SAN
 2      12 No
 3      13 No
 4      14 No
 5      15 No
 6      16 No
 7       9 No
15     MAX No
...
```

### Defaults

20% egress bandwidth for PG0, and 80% for PG1.

### Related Commands

show cee-map - displays the CEE-MAP settings

## 36.3 pfc priority

This command is used to declare a priority is PFC-enabled or disabled.

Note that if a priority is PFC-disabled, but it joined a PFC-enabled PG, then the PFC function of this priority is automatically enabled. Alternatively,, if a priority joined a PG that does not require enabling PFC, the priority can still enable the PFC function individually.

```
pfc priority <pri(0-7)> {enable|disable}
```

### Syntax Description

<pri> - The priority ID  
 enable - Enable PFC function on this priority.  
 disable - Disable PFC function on this priority.

### Mode

Config-CEE-Map mode

### Example:

```
SMIS# show cee-map 2
```

```
...
Priority Group PFC Description
-----
0 0 No LAN
1 0 No
2 0 No
3 1 Yes FCoE/FIP
4 0 No
5 0 No
6 0 No
7 0 No
```

```
...
SMIS# configure terminal
SMIS(config)# cee-map 2
SMIS(config-cee-map)# pfc priority 1 enable
SMIS(config-cee-map)# pfc priority 2 enable
SMIS(config-cee-map)# exit
SMIS(config)# exit
SMIS# show cee-map 2
```

```
...
Priority Group PFC Description
-----
0 0 No LAN
1 0 Yes
2 0 Yes
3 1 Yes FCoE/FIP
4 0 No
5 0 No
6 0 No
7 0 No
```

...

**Defaults**

Enabled for priority 3, and disabled for the others.

**Related Commands**

show cee-map - displays the CEE-MAP settings

## 36.4 pri2pg

This command maps priorities to priority groups (PGs). The “no” form of this command resets to default mapping. Priorities within a PG share the same egress bandwidth portion.

```
pri2pg <pri0_pg> <pri1_pg> <pri2_pg> <pri3_pg> <pri4_pg> <pri5_pg>
<pri6_pg> <pri7_pg>
no pri2pg [{priority <id(0-7)>| all}]
```

### Syntax Description

<pri0\_pg> - The PG that priority 0 maps to.  
 <pri1\_pg> - The PG that priority 1 maps to.  
 <pri2\_pg> - The PG that priority 2 maps to.  
 <pri3\_pg> - The PG that priority 3 maps to.  
 <pri4\_pg> - The PG that priority 4 maps to.  
 <pri5\_pg> - The PG that priority 5 maps to.  
 <pri6\_pg> - The PG that priority 6 maps to.  
 <pri7\_pg> - The PG that priority 7 maps to.  
 <id> - The priority ID.

### Mode

Config-CEE-Map mode

### Example:

```
SMIS(config)# cee-map 2
SMIS(config-cee-map)# group-bandwidth 20 50 30 0 0 0 0
SMIS(config-cee-map)# pri2pg 0 0 0 1 2 2 2
SMIS(config-cee-map)# group 2 description AUDIO_SERVICE
SMIS(config-cee-map)# priority 0 description INTERNET
SMIS(config-cee-map)# priority 1 description DATA_BASE
SMIS(config-cee-map)# priority 2 description DATA_BASE_CONTROL
SMIS(config-cee-map)# priority 4 description AUDIO_DATA_1
SMIS(config-cee-map)# priority 5 description AUDIO_DATA_2
SMIS(config-cee-map)# priority 6 description AUDIO_SYNC
SMIS(config-cee-map)# priority 7 description AUDIO_CONTROL
SMIS(config-cee-map)# end
SMIS# show cee-map 2
```

```
...
Priority Group PFC Description
-----
 0 0 No INTERNET
 1 0 No DATA_BASE
 2 0 No DATA_BASE_CONTROL
 3 1 Yes FCoE/FIP
 4 2 No AUDIO_DATA_1
 5 2 No AUDIO_DATA_2
 6 2 No AUDIO_SYNC
 7 2 No AUDIO_CONTROL
```

```
Group Bandwidth(%) PFC Description
-----
```

0	20	No	LAN
1	50	Yes	SAN
2	30	No	AUDIO_SERVICE
3	0	No	
4	0	No	
5	0	No	
6	0	No	
7	0	No	
15	MAX	No	

...

## Defaults

Priority 3 mapped to PG 1 (SAN), and all others are mapped to PG 0 (LAN).

## Related Commands

show cee-map - displays the CEE-MAP settings

## 36.5 pfc group

This command is used to declare whether a priority group (PG) is required to enable PFC or not. If a PG is declared "PFC-enabled", all the priorities mapped to this PG are PFC-enabled automatically. If a PG is declared "PFC-disabled", then the priorities mapped to this PG can choose to or not to enable PFC individually.

**pfc group <id(0-7)> {enable|disable}**

### Syntax Description

<id> - The priority-group ID (PGID)  
 enable - The PG asks all its priorities to enable PFC.  
 disable - The PG does not ask its priorities to enable PFC.

### Mode

Config-CEE-Map mode

### Example:

SMIS# show cee-map 2

```

...
Group Bandwidht(%) PFC Description
-----
 0      20 No LAN
 1      80 Yes SAN
 2       0 No
 3       0 No
 4       0 No
 5       0 No
 6       0 No
 7       0 No
 15     MAX No
    
```

```

...
SMIS# configure terminal
SMIS(config)# cee-map 2
SMIS(config-cee-map)# pfc group 0 enable
SMIS(config-cee-map)# end
SMIS# show cee-map 2
    
```

```

...
Group Bandwidht(%) PFC Description
-----
 0      20 Yes LAN
 1      80 Yes SAN
 2       0 No
 3       0 No
 4       0 No
 5       0 No
 6       0 No
 7       0 No
 15     MAX No
    
```

### Defaults



"LAN" for PG 0, and "SAN" for PG 1.

## **Related Commands**

show cee-map - displays the CEE-MAP settings

## 36.6 pfc priority

This command is used to declare a priority is PFC-enabled or disabled.

Note that, if a priority is PFC-disabled, but it joined a PFC-enabled PG, then the PFC function of this priority is automatically enabled. Alternatively, if a priority joined a PG that does not require enabling PFC, the priority can still enable the PFC function individually.

**pfc priority <pri(0-7)> {enable|disable}**

### Syntax Description

<pri> - The priority ID  
 enable - Enable PFC function on this priority.  
 disable - Disable PFC function on this priority.

### Mode

Config-CEE-Map mode

### Example:

SMIS# show cee-map 2

```
...
Priority Group PFC Description
-----
 0  0  No LAN
 1  0  No
 2  0  No
 3  1  Yes FCoE/FIP
 4  0  No
 5  0  No
 6  0  No
 7  0  No
```

```
...
SMIS# configure terminal
SMIS(config)# cee-map 2
SMIS(config-cee-map)# pfc priority 1 enable
SMIS(config-cee-map)# pfc priority 2 enable
SMIS(config-cee-map)# exit
SMIS(config)# exit
SMIS# show cee-map 2
```

```
...
Priority Group PFC Description
-----
 0  0  No LAN
 1  0  Yes
 2  0  Yes
 3  1  Yes FCoE/FIP
 4  0  No
 5  0  No
 6  0  No
 7  0  No
```

**Defaults**

Enabled for priority 3, and disabled for the others.

**Related Commands**

show cee-map - displays the CEE-MAP settings

## 36.7 cee

This command associates an interface with a CEE-Map. The “no” form of this command disassociate from any CEE-Map. For an interface which is performing DCBX, to disassociate the CEE-Map, please execute "no dcbx cee" prior to executing "no cee".

```
cee <cee-map-id(1-4)>>  
no cee
```

### Syntax Description

<cee-map-id> - The CEE-Map identifier to associate.

### Mode

Interface configuration mode.

### Example:

```
SMIS# configure terminal  
SMIS(config)# interface extreme-ethernet 0/1  
SMIS(config-if)# cee 1  
SMIS(config-if)#
```

### Defaults

There is no CEE-Map associated.

### Related Commands

cee-map - Create, modify, or delete a cee-map.  
dcbx cee - Start DCBX protocol  
no dcbx cee - Stop DCBX protocol

## 36.8 dcbx cee

This command starts the DCBX protocol in CEE mode on an interface that is associated with a CEE-Map, and the “no” form of this command stops the CEE mode of the DCBX protocol.

**dcbx cee**  
**no dcbx cee**

### Syntax Description

dcbx cee - Encapsulates DCBX TLVs in the LLDP message, starts DCBX.  
no dcbx cee - Stops encapsulating DCBX TLVs in the LLDP message, stop DCBX.

### Mode

Interface configuration mode.

### Example:

```
SMIS# configure terminal
SMIS(config)# interface extreme-ethernet 0/1
SMIS(config-if)# cee 1
SMIS(config-if)# dcbx cee
```

### Defaults

There is no CEE-Map associated.

### Related Commands

cee-map - Create, modify, or delete a cee-map.  
dcbx cee - Start DCBX protocol  
no dcbx cee - Stop DCBX protocol  
show lldp dcbx interface - Show DCBX interface status

## 37 LLDP

Link layer discovery protocol (LLDP) helps to learn information about the other devices on the local network. LLDP enabled devices send out information about their identity and capabilities periodically. To share different information LLDP supports many types of TLVs.

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

[set lldp](#)

[lldp chassis-id-subtype](#)

[lldp holdtime-multiplier](#)

[lldp notification interval](#)

[lldp reinitialization-delay](#)

[lldp transmit-interval](#)

[lldp tx-delay](#)

[clear lldp counters](#)

[clear lldp table](#)

[lldp notification](#)

[lldp port-id-subtype](#)

[lldp tlv-select basic-tlv](#)

[lldp tlv-select dot1tlv](#)

[lldp tlv-select dot3tlv](#)

[lldp transmit | receive](#)

[debug lldp](#)

[show lldp](#)

[show lldp errors](#)

[show lldp interface](#)

[show lldp local](#)

[show lldp neighbors](#)

[show lldp statistics](#)

[show lldp traffic](#)

## 37.1 set lldp

This command enables or disables the LLDP feature.

LLDP feature is disabled by default.

```
set lldp {enable | disable}
```

### Syntax Description

enable – Enables the LLDP feature

disable – Disables the LLDP feature

### Mode

Global Configuration Mode

### Defaults

disable

### Example:

```
SMIS(config)# set lldp enable
```

### Related Commands

show lldp – Displays the LLDP feature information.



## 37.2 lldp chassis-id-subtype

This command configures chassis identifier type. Chassis identifier can be any one of the following:

- Chassis Component - Chassis component string
- Interface Alias - Interface alias
- Port Component - Port component string
- MAC Address - MAC address of the switch
- Network Address - Network address of the switch
- Interface Name - Interface name
- Locally Assigned - Any user defined local string

```
lldp chassis-id-subtype { chassis-comp <string(255)> | if-alias | port-comp <string(255)> | mac-addr | nw-addr | if-name | local <string(255)> }
```

### Syntax Description

- chassis-comp** - Chassis component string
- if-alias** - Interface alias. To use the if-alias option, the management interface must have been configured with valid description.
- port-comp** - Port component string
- mac-addr** - MAC address of the switch
- nw-addr** - Network address of the switch
- if-name** - Interface name
- local** - Any user defined local string

### Mode

Global Configuration Mode

### Defaults

MAC address of the switch

### Example:

```
SMIS(config)# lldp chassis-id-subtype chassis-comp abcd
```

### Related Commands

show lldp – Displays the LLDP feature information.



## 37.3 lldp holdtime-multiplier

This command helps to configure the time-to-live of LLDP information. The LLDP devices hold the received LLDP information for the time advertised as time-to-live information.

This time-to-live value is calculated as below:

time-to-live = holdtime multiplier X transmit interval

This command helps to configure this holdtime multiplier. The “no” form of this command resets this hold time multiplier to its default 4.

```
lldp holdtime-multiplier <value(2-10)>
```

```
no lldp holdtime-multiplier
```

### Syntax Description

holdtime-multiplier – any number between 2 to 10

### Mode

Global Configuration Mode

### Defaults

4

### Example:

```
SMIS(config)# lldp holdtime-multiplier 5
```

### Related Commands

show lldp – Displays the LLDP feature information.

## 37.4 lldp notification interval

This command configures the time interval on which LLDP traps are sent to SNMP managers when LLDP information is changed.

The “no” form of this command resets the notification interval to its default value 5 seconds.

```
lldp notification-interval <seconds(5-3600)>
```

```
no lldp notification-interval
```

### Syntax Description

notification-interval – any number between 5 to 3600

### Mode

Global Configuration Mode

### Defaults

5 seconds

### Example:

```
SMIS(config)# lldp notification-interval 300
```

### Related Commands

show lldp – Displays the LLDP feature information.

## 37.5 lldp reinitialization-delay

This command configures time delay used to initialize LLDP on any interface.

The “no” form of this command resets the time delay to its default value 2 seconds.

```
lldp reinitialization-delay <seconds(1-10)>
```

```
no lldp reinitialization-delay
```

### Syntax Description

reinitialization-delay – any number between 1 to 10

### Mode

Global Configuration Mode

### Defaults

2 seconds

### Example:

```
SMIS(config)# lldp reinitialization-delay 8
```

### Related Commands

show lldp – Displays the LLDP feature information.

## 37.6 lldp transmit-interval

This command configures the time interval on which LLDP update messages are sent.

The “no” form of this command resets the transmit interval to its default value 30 seconds.

```
lldp transmit-interval <seconds(5-32768)>
```

```
no lldp transmit-interval
```

### Syntax Description

transmit-interval – any number between 5 to 32768

### Mode

Global Configuration Mode

### Defaults

30 seconds

### Example:

```
SMIS(config)# lldp transmit-interval 180
```

### Related Commands

show lldp – Displays the LLDP feature information.

## 37.7 lldp tx-delay

This command configures the minimum time interval maintained between any two subsequent LLDP messages sent out.

The “no” form of this command resets this transmit delay to its default value 2 seconds.

```
lldp tx-delay <seconds(1-8192)>
```

```
no lldp tx-delay
```

### Syntax Description

tx-delay – any number between 1 to 8192

### Mode

Global Configuration Mode

### Defaults

2 seconds

### Example:

```
SMIS(config)# lldp tx-delay 15
```

### Related Commands

show lldp – Displays the LLDP feature information.

## 37.8 clear lldp counters

This command resets the LLDP traffic counters.

```
clear lldp counters
```

### **Mode**

Global Configuration Mode

### **Example:**

```
SMIS(config)# clear lldp counters
```

### **Related Commands**

show lldp traffic – Displays the LLDP traffic counters.



## 37.9 clear lldp table

This command resets all the LLDP neighbor information learned.

clear lldp table

### Mode

Global Configuration Mode

### Example:

```
SMIS(config)# clear lldp table
```

### Related Commands

show lldp neighbors – Displays the LLDP neighbor information.

## 37.10 lldp notification

This command configures the lldp notification status and notification types on the interface.

The “no” form of this command disables the notification on the interface.

lldp notification [remote-table-chg][mis-configuration]

no lldp notification

### Syntax Description

remote-table-chg – configures to send SNMP notification when remote table changes

mis-configuration – configures to send SNMP notification when incorrect configuration detected in the switch

When no options given this command enables lldp notification on the interface.

### Mode

Interface Configuration Mode

### Defaults

Notification status - disabled

Notification type – mis configuration

### Example:

```
SMIS(config-if)# lldp notification remote-table-chg
```

### Related Commands

show lldp interface – Displays the LLDP feature interface configuration.

## 37.11 lldp port-id-subtype

This command configures the port identifier type. An LLDP port identifier can be any one of the following:

Interface Alias - Interface alias

Port Component - Port component string

MAC Address - MAC address of the switch

Interface Name - Interface name

Locally Assigned - Any user defined local string

```
lldp port-id-subtype { if-alias | port-comp <string(255)> | mac-addr |  
if-name | local <string(255)> }
```

### Syntax Description

**if-alias** - Interface alias. The if-alias option can be used only for the interfaces which have valid description configured.

**port-comp** - Port component string up to 255 characters

**mac-addr** - MAC address of the switch

**if-name** - Interface name

**local** - Any user defined local string up to 255 characters

### Mode

Interface Configuration Mode

### Defaults

Interface name

### Example:

```
SMIS(config-if)# lldp port-id-subtype mac-addr
```

### Related Commands

show lldp local – Displays the LLDP interface information.

## 37.12 lldp tlv-select basic-tlv

This command configures basic tlv transmission on interface. It enables the transmission of given tlv on any interface.

The “no” form of this command disables the transmission of given tlv on any interface.

```
lldp tlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-  
capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6 <ip6_addr>}]}
```

```
no lldp tlv-select basic-tlv { [port-descr] [sys-name] [sys-descr]  
[sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6 <ip6_addr>}]}
```

### Syntax Description

**port-descr** - Enables port description tlv transmission

**sys-name** - Enables system name tlv transmission

**sys-descr** - Enables system description tlv transmission

**sys-capab** - Enables system capabilities tlv transmission

**mgmt-addr all** - Enables transmission of all management address information

**mgmt-addr ipv4** - Enables transmission of given IPv4 management address information

**mgmt-addr ipv6** - Enables transmission of given IPv6 management address information

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# lldp tlv-select basic-tlv sys-name sys-descr sys-capab
```

### Related Commands

show lldp local – Displays the LLDP local interface information.

## 37.13 lldp tlv-select dcbx-cee-pfc

For DCBX-capable switch products, this command configures the PFC (Priority-based Flow Control) feature sub-TLV included in the DCBX TLV. PFC sub-TLV is used to inform the link partner about the PFC settings. By default, the setting is for host CNA (Converged Network Adapter) connectivity, so the "willing" control bit is zero to ask the host to follow the switch side PFC settings.

Moreover, if the port is connected to a FC/FCoE switch (FCF), the "willing" bit might need to be set to 1 to ask the switch to follow FCF's PFC setting. Whether or not to change the willing bit is dependent on the FCF configuration.

Note that flowcontrol (both send and receive) should be turned off, otherwise it will impact PFC operations.

The "no" form of this command resets to the default values.

```
lldp tlv-select dcbx-cee-pfc [advertise {on|off}] [willing {0|1}]
[enable {0|1}]
no lldp tlv-select dcbx-cee-pfc
```

This feature is supported only on the following switch models

SBM-XEM-X10SM

SSE-X24SR

### Syntax Description

advertise on - Let DCBX TLV carry PFC sub-TLV.  
 advertise off - Let DCBX TLV does not carry PFC sub-TLV.  
 willing 0 - Clear the willing control bit, insists using local PFC settings.  
 willing 1 - Set the willing control bit, will follow peer's PFC settings.  
 enable 0 - Advertise that local side disabled PFC feature.  
 enable 1 - Advertise that local side enabled PFC feature.

### Mode

Interface Configuration Mode

### Defaults

Advertise on, willing 0, and enable 1.

### Related Commands

show lldp dcbx interface - displays the current DCBX status of specified interface  
 show cee-map - displays the CEE-MAP settings

## 37.14 lldp tlv-select dcbx-cee-pg

For DCBX-capable switch products, this command configures the PG (Priority Group) feature sub-TLV included in the DCBX TLV. PG sub-TLV is used to inform the link partner about the relationship between priorities and priority groups (PGs). By default, the setting is for host CNA (Converged Network Adapter) connectivity, so the "willing" control bit is zero to ask the host follow switch side PG settings. Moreover, if the port is connected to a FC/FCoE switch (FCF), the "willing" bit might need to be set to 1 to ask the switch to follow FCF's PG setting. Whether or not to change the willing bit is dependent on the FCF configuration.

The "no" form of this command reset to the default values.

```
lldp tlv-select dcbx-cee-pg [advertise {on|off}] [willing {0|1}]
[enable {0|1}]
no lldp tlv-select dcbx-cee-pg
```

This feature is supported only on the following switch models

SBM-XEM-X10SM

SSE-X24SR

### Syntax Description

advertise on - Let DCBX TLV carries PG sub-TLV.

advertise off - Let DCBX TLV does not carry PG sub-TLV.

willing 0 - Clear the willing control bit, insists using local PG settings.

willing 1 - Set the willing control bit, will follow peer's PG settings.

enable 0 - Advertise that local side disabled PG feature.

enable 1 - Advertise that local side enabled PG feature.

### Mode

Interface Configuration Mode

### Defaults

Advertise on, willing 0, and enable 1.

### Related Commands

show lldp dcbx interface - displays the current DCBX status of specified interface

show cee-map - displays the CEE-MAP settings

## 37.15 lldp tlv-select dot1tlv

This command configures 802.1 VLAN tlv transmission on interface. It enables the transmission of given tlv on any interface.

The “no” form of this command disables the transmission of given tlv on any interface.

```
lldp tlv-select dot1tlv {[port-vlan-id] [protocol-vlan-id {all | <vlan-id>}] [vlan-name {all | <vlan-id>}]}
```

```
no lldp tlv-select dot1tlv {[port-vlan-id] [protocol-vlan-id {all | <vlan-id>}] [vlan-name {all | <vlan-id>}]}
```

### Syntax Description

**port-vlan-id** – Enables transmission of port vlan identifier tlv

**protocol-vlan-id all** - Enables transmission of all protocol vlan identifiers tlv

**protocol-vlan-id <vlan-id>** - Enables transmission of the given protocol vlan identifier tlv

**vlan-name all** - Enables transmission of all vlan names tlv

**vlan-name <vlan-id>** - Enables transmission of the given vlan name tlv

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# lldp tlv-select dot1tlv port-vlan-id protocol-vlan-id  
all
```

### Related Commands

show lldp local – Displays the LLDP local interface information.

## 37.16 lldp tlv-select dot3tlv

This command configures 802.3 standard tlv transmission on interface. It enables the transmission of given tlv on any interface.

The “no” form of this command disables the transmission of given tlv on any interface.

```
lldp tlv-select dot3tlv { [macphy-config] [link-aggregation] [max-framesize] }
```

```
no lldp tlv-select dot3TLV { [macphy-config] [link-aggregation] [max-framesize] }
```

### Syntax Description

**macphy-config** – Enables transmission of MAC and phy configuration and status tlv

**link-aggregation** - Enables transmission of link aggregation information tlv

**max-framesize** - Enables transmission of max frame size information tlv

### Mode

Interface Configuration Mode

### Defaults

Disabled

### Example:

```
SMIS(config-if)# lldp tlv-select dot3tlv macphy-config link-aggregation
```

### Related Commands

show lldp local – Displays the LLDP local interface information.



## 37.17 lldp transmit | receive

This command enables the transmit and receive of LLDP messages on any interface.

The “no” form of this command disables the transmit and receive of LLDP messages on any interface.

```
lldp {transmit | receive}
```

```
no lldp {transmit | receive}
```

### Syntax Description

**transmit** – Enables transmission of LLDP messages

**receive** - Enables receive of LLDP messages

### Mode

Interface Configuration Mode

### Defaults

Both transmit and receive enabled

### Example:

```
SMIS(config-if)# lldp transmit
```

### Related Commands

show lldp interface – Displays the LLDP interface information.

## 37.18 debug lldp

This command enables the display of LLDP debug messages.

The “no” form of this command disables the display of LLDP debug messages.

```
debug lldp [{all | [init-shut] [mgmt] [data-path] [ctrl] [pkt-dump]
[resource] [all-fail] [buf] [neigh-add] [neigh-del] [neigh-updt]
[neigh-drop] [neigh-ageout] [critical][tlv {all | [chassis-id][port-id]
[ttl] [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr]
[port-vlan] [ppvlan] [vlan-name] [proto-id] [mac-phy] [pwr-mdi] [lagg]
[max-frame] [dcbx]}]]}]
```

```
no debug lldp [{all | [init-shut] [mgmt] [data-path] [ctrl] [pkt-dump]
[resource] [all-fail] [buf] [neigh-add] [neigh-del] [neigh-updt]
[neigh-drop] [neigh-ageout] [critical][tlv {all | [chassis-id][port-id]
[ttl] [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr]
[port-vlan] [ppvlan] [vlan-name] [proto-id] [mac-phy] [pwr-mdi] [lagg]
[max-frame] [dcbx]}]]}]
```

### Syntax Description

**all** – displays all debug messages

**init-shut** – displays initialization and shutdown messages

**mgmt** – displays management messages

**data-path** – displays all data path messages

**ctrl** – displays all control messages

**pkt-dump** – displays the contents of all LLDP packets

**resource** – displays the resources (like memory) utilization debug messages

**all-fail** – displays all failure events

**neigh-add** – displays all neighbor addition events

**neigh-del** – displays all neighbor deletion events

**neigh-updt** – displays all neighbor update events

**neigh-drop** – displays all neighbor drop events

**neigh-ageout** – displays all neighbor aging out events

**critical** – displays all critical event messages

**tlv all** – displays all TLV information

**tlv chassis-id** – displays chassis identifier TLV information  
**tlv port-id** – displays port identifier TLV information  
**tlv ttl** – displays time to live TLV information  
**tlv port-descr** – displays port description TLV information  
**tlv sys-name** – displays system name TLV information  
**tlv sys-descr** – displays system description TLV information  
**tlv sys-capab** – displays system capabilities TLV information  
**tlv mgmt-addr** – displays management address TLV information  
**tlv port-vlan** – displays port VLAN TLV information  
**tlv ppvlan** – displays protocol VLAN TLV information  
**tlv vlan-name** – displays VLAN name TLV information  
**tlv proto-id** – displays protocol identifier TLV information  
**tlv mac-phy** – displays MAC and phy TLV information  
**tlv pwr-mdi** – displays power mdi TLV information  
**tlv lagg** – displays link aggregation TLV information  
**tlv max-frame** – displays max frame size TLV information  
**tlv dcbx** – for DCBX-capable products, displays DCBX information

### Mode

Privileged/User EXEC Mode

### Defaults

Disabled

### Example:

```
SMIS# debug lldp init-shut mgmt data-path pkt-dump
```

### Related Commands

## 37.19 show lldp

This command displays LLDP configuration information.

**show lldp**

### Syntax Description

#### Mode

Privileged/User EXEC Mode

#### Defaults

#### Example:

```
SMIS# show lldp
```

#### Related Commands

show lldp errors – Displays the LLDP errors

show lldp interface – Displays the LLDP interface configuration information

show lldp local – Displays the LLDP local interface information

show lldp neighbor – Displays the LLDP neighbor table

show lldp statistics – Displays the LLDP statistics

show lldp traffic – Displays the LLDP traffic counters

## 37.20 show lldp dcbx

This command displays the status of a DCBX TLV exchange, for switch products that support DCBX.

```
show lldp dcbx interface [<interface-type> <interface-id>]
```

This feature is supported only on the following switch models

SBM-XEM-X10SM

SSE-X24SR

### Syntax Description

interface-type - Interface type, only for DCBX-capable ports.

interface-id - Physical interface ID including slot and port number.

### Mode

Privileged/User EXEC Mode

### Defaults

### Related Commands

lldp tlv-select dcbx-cee-pfc jV Configures the PFC feature sub-TLV

lldp tlv-select dcbx-cee-pg - Configures the PG feature sub-TLV

## 37.21 show lldp errors

This command displays LLDP error counters.

```
show lldp errors
```

### Syntax Description

#### Mode

Privileged/User EXEC Mode

#### Defaults

#### Example:

```
SMIS# show lldp errors
```

#### Related Commands

show lldp – Displays the LLDP information

show lldp interface – Displays the LLDP interface configuration information

show lldp local – Displays the LLDP local interface information

show lldp neighbor – Displays the LLDP neighbor table

show lldp statistics – Displays the LLDP statistics

show lldp traffic – Displays the LLDP traffic counters

## 37.22 show lldp interface

This command displays LLDP interface information.

```
show lldp interface [<interface-type> <interface-id>]
```

### Syntax Description

**interface-type** - Interface type, can either be a gi, ex or qx

**interface-id** - Physical interface ID including slot and port number.

### Mode

Privileged/User EXEC Mode

### Defaults

### Example:

```
SMIS# show lldp interface gi 0/1
```

### Related Commands

show lldp – Displays the LLDP information

show lldp errors – Displays the LLDP errors

show lldp local – Displays the LLDP local interface information

show lldp neighbor – Displays the LLDP neighbor table

show lldp statistics – Displays the LLDP statistics

show lldp traffic – Displays the LLDP traffic counters

## 37.23 show lldp local

This command displays LLDP interface configuration and TLV information.

```
show lldp local {[<interface-type> <interface-id>] | [mgmt-addr]}
```

### Syntax Description

**interface-type** - Interface type, can either be a gi, ex or qx

**interface-id** - Physical interface ID including slot and port number.

**mgmt-addr** - Management address

### Mode

Privileged/User EXEC Mode

### Defaults

### Example:

```
SMIS# show lldp local gi 0/1
```

### Related Commands

show lldp – Displays the LLDP information

show lldp errors – Displays the LLDP errors

show lldp interface – Displays the LLDP interface information

show lldp neighbor – Displays the LLDP neighbor table

show lldp statistics – Displays the LLDP statistics

show lldp traffic – Displays the LLDP traffic counters



## 37.24 show lldp neighbors

This command displays LLDP neighbor information.

```
show lldp neighbors [chassis-id <string(255)> port-id <string(255)>]
[<interface-type> <interface-id>][detail]
```

### Syntax Description

**chassis-id** - chassis identifier

**port-id** - port identifier

**interface-type** - Interface type, can either be a gi, ex or qx

**interface-id** - Physical interface ID including slot and port number.

**detail** - displays more detailed information

### Mode

Privileged/User EXEC Mode

### Defaults

### Example:

```
SMIS# show lldp neighbors gi 0/1
```

### Related Commands

show lldp – Displays the LLDP information

show lldp errors – Displays the LLDP errors

show lldp interface – Displays the LLDP interface information

show lldp local – Displays the LLDP local interface information

show lldp statistics – Displays the LLDP statistics

show lldp traffic – Displays the LLDP traffic counters

## 37.25 show lldp statistics

This command displays LLDP statistics.

```
show lldp statistics
```

### Syntax Description

#### Mode

Privileged/User EXEC Mode

#### Defaults

#### Example:

```
SMIS# show lldp statistics
```

#### Related Commands

show lldp – Displays the LLDP information

show lldp errors – Displays the LLDP errors

show lldp interface – Displays the LLDP interface information

show lldp local – Displays the LLDP local interface information

show lldp neighbors – Displays the LLDP neighbor table

show lldp traffic – Displays the LLDP traffic counters

## 37.26 show lldp traffic

This command displays LLDP traffic counters.

```
show lldp traffic [<iftype> <ifnum>]
```

### Syntax Description

**iftype** - Interface type, can either be a gi, ex or qx

**ifnum** - Physical interface ID including slot and port number.

### Mode

Privileged/User EXEC Mode

### Defaults

### Example:

```
SMIS# show lldp traffic gi 0/1
```

### Related Commands

show lldp – Displays the LLDP information

show lldp errors – Displays the LLDP errors

show lldp interface – Displays the LLDP interface information

show lldp local – Displays the LLDP local interface information

show lldp neighbors – Displays the LLDP neighbor table

show lldp statistics – Displays the LLDP statistics