

Dell™ PowerConnect™ 5400  
Systems

**CLI Reference Guide**

## Notes, Cautions, and Warnings



**NOTE:** A NOTE indicates important information that helps you make better use of your computer.



**CAUTION:** A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.



**WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

---

**Information in this document is subject to change without notice.**

© 2008 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: *Dell*, the *DELL* logo, *PowerConnect* are trademarks of Dell Inc.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

# Contents

1	Using the CLI . . . . .	25
	<b>CLI Command Modes . . . . .</b>	<b>25</b>
	Introduction . . . . .	25
	User EXEC Mode . . . . .	26
	Privileged EXEC Mode . . . . .	26
	Global Configuration Mode . . . . .	27
	Interface Configuration Mode and Specific Configuration Modes . . . . .	28
	<b>Starting the CLI . . . . .</b>	<b>28</b>
	<b>Editing Features . . . . .</b>	<b>29</b>
	<b>Setup Wizard . . . . .</b>	<b>30</b>
	Terminal Command Buffer . . . . .	30
	Negating the Effect of Commands . . . . .	30
	Command Completion . . . . .	31
	Keyboard Shortcuts . . . . .	31
	CLI Command Conventions . . . . .	32
2	Command Groups . . . . .	33
	<b>Introduction . . . . .</b>	<b>33</b>
	<b>Command Groups . . . . .</b>	<b>33</b>
	<b>ACL Commands . . . . .</b>	<b>35</b>
	<b>AAA Commands . . . . .</b>	<b>35</b>
	<b>Address Table Commands . . . . .</b>	<b>36</b>
	<b>Clock Commands . . . . .</b>	<b>37</b>
	<b>Configuration and Image Files Commands . . . . .</b>	<b>38</b>
	<b>DHCP Snooping Commands . . . . .</b>	<b>39</b>
	<b>Ethernet Configuration Commands . . . . .</b>	<b>39</b>
	<b>GVRP Commands . . . . .</b>	<b>41</b>

<b>IGMP Snooping Commands</b> . . . . .	<b>41</b>
<b>IP Addressing Commands</b> . . . . .	<b>42</b>
<b>IPv6 Addressing Commands</b> . . . . .	<b>43</b>
<b>iSCSI Commands</b> . . . . .	<b>44</b>
<b>LACP Commands</b> . . . . .	<b>44</b>
<b>Line Commands</b> . . . . .	<b>44</b>
<b>LLDP Commands</b> . . . . .	<b>45</b>
<b>Login Banner Commands</b> . . . . .	<b>46</b>
<b>Management ACL Commands</b> . . . . .	<b>46</b>
<b>PHY Diagnostics Commands</b> . . . . .	<b>47</b>
<b>Port Channel Commands</b> . . . . .	<b>47</b>
<b>Port Monitor Commands</b> . . . . .	<b>48</b>
<b>QoS Commands</b> . . . . .	<b>48</b>
<b>RADIUS Commands</b> . . . . .	<b>49</b>
<b>RMON Commands</b> . . . . .	<b>49</b>
<b>SNMP Commands</b> . . . . .	<b>50</b>
<b>Spanning Tree Commands</b> . . . . .	<b>51</b>
<b>SSH Commands</b> . . . . .	<b>53</b>
<b>Syslog Commands</b> . . . . .	<b>53</b>
<b>System Management Commands</b> . . . . .	<b>54</b>
<b>TACACS Commands</b> . . . . .	<b>55</b>
<b>TIC Commands</b> . . . . .	<b>55</b>
<b>Tunnel Commands</b> . . . . .	<b>56</b>
<b>User Interface Commands</b> . . . . .	<b>57</b>
<b>VLAN Commands</b> . . . . .	<b>57</b>
<b>Voice VLAN Commands</b> . . . . .	<b>59</b>



	<b>Web Server Commands</b> . . . . .	<b>59</b>
	<b>802.1x Commands</b> . . . . .	<b>60</b>
	<b>802.1x Advanced Commands</b> . . . . .	<b>62</b>
<b>3</b>	<b>Command Modes</b> . . . . .	<b>63</b>
	<b>GC (Global Configuration) Mode</b> . . . . .	<b>63</b>
	<b>IC (Interface Configuration) Mode</b> . . . . .	<b>67</b>
	<b>LC (Line Configuration) Mode</b> . . . . .	<b>70</b>
	<b>MA (Management Access-level) Mode</b> . . . . .	<b>70</b>
	<b>PE (Privileged User EXEC) Mode</b> . . . . .	<b>70</b>
	<b>SP (SSH Public Key) Mode</b> . . . . .	<b>72</b>
	<b>UE (User EXEC) Mode</b> . . . . .	<b>73</b>
	<b>VC (VLAN Configuration) Mode</b> . . . . .	<b>74</b>
<b>4</b>	<b>ACL Commands</b> . . . . .	<b>75</b>
	<b>ip access-list</b> . . . . .	<b>75</b>
	<b>mac access-list</b> . . . . .	<b>75</b>
	<b>permit (ip)</b> . . . . .	<b>76</b>
	<b>deny (IP)</b> . . . . .	<b>78</b>
	<b>permit (MAC)</b> . . . . .	<b>80</b>
	<b>deny (MAC)</b> . . . . .	<b>81</b>
	<b>service-acl</b> . . . . .	<b>82</b>
	<b>show access-lists</b> . . . . .	<b>83</b>
	<b>show interfaces access-lists</b> . . . . .	<b>84</b>

5	AAA Commands . . . . .	85
	<b>aaa authentication login</b> . . . . .	85
	<b>aaa authentication enable</b> . . . . .	86
	<b>login authentication</b> . . . . .	87
	<b>enable authentication</b> . . . . .	88
	<b>ip http authentication</b> . . . . .	89
	<b>ip https authentication</b> . . . . .	89
	<b>show authentication methods</b> . . . . .	90
	<b>password</b> . . . . .	92
	<b>enable password</b> . . . . .	92
	<b>username</b> . . . . .	93
	<b>show users accounts</b> . . . . .	94
6	Address Table Commands . . . . .	95
	<b>bridge address</b> . . . . .	95
	<b>bridge multicast filtering</b> . . . . .	96
	<b>bridge multicast address</b> . . . . .	97
	<b>bridge multicast forbidden address</b> . . . . .	98
	<b>bridge multicast unregistered</b> . . . . .	99
	<b>bridge multicast forward-all</b> . . . . .	100
	<b>bridge multicast forbidden forward-all</b> . . . . .	100
	<b>bridge aging-time</b> . . . . .	101
	<b>clear bridge</b> . . . . .	102
	<b>port security</b> . . . . .	103
	<b>port security mode</b> . . . . .	103
	<b>port security max</b> . . . . .	104
	<b>port security routed secure-address</b> . . . . .	105

	<b>show bridge address-table</b>	106
	<b>show bridge address-table static</b>	107
	<b>show bridge address-table count</b>	108
	<b>show bridge multicast address-table</b>	109
	<b>show bridge multicast filtering</b>	110
	<b>show ports security</b>	111
	<b>show ports security addresses</b>	113
7	<b>Login Banner</b>	115
	<b>banner exec</b>	115
	<b>banner login</b>	116
	<b>banner motd</b>	118
	<b>exec-banner</b>	119
	<b>login-banner</b>	120
	<b>motd-banner</b>	121
	<b>show banner</b>	121
8	<b>Clock</b>	123
	<b>clock set</b>	123
	<b>clock source</b>	123
	<b>clock timezone</b>	124
	<b>clock summer-time</b>	125
	<b>sntp authentication-key</b>	126
	<b>sntp authenticate</b>	127
	<b>sntp trusted-key</b>	128
	<b>sntp client poll timer</b>	129
	<b>sntp broadcast client enable</b>	129

<b>sntp anycast client enable</b> . . . . .	130
<b>sntp client enable</b> . . . . .	131
<b>sntp client enable (interface)</b> . . . . .	131
<b>sntp unicast client enable</b> . . . . .	132
<b>sntp unicast client poll</b> . . . . .	133
<b>sntp server</b> . . . . .	133
<b>show clock</b> . . . . .	135
<b>show sntp configuration</b> . . . . .	136
<b>show sntp status</b> . . . . .	138
9 Configuration and Image Files . . . . .	139
<b>dir</b> . . . . .	139
<b>more</b> . . . . .	140
<b>rename</b> . . . . .	141
<b>delete startup-config</b> . . . . .	142
<b>copy</b> . . . . .	143
<b>delete</b> . . . . .	146
<b>boot system</b> . . . . .	146
<b>show running-config</b> . . . . .	147
<b>show startup-config</b> . . . . .	148
<b>show bootvar</b> . . . . .	150
10 Ethernet Configuration Commands . . . . .	151
<b>interface ethernet</b> . . . . .	151
<b>interface range ethernet</b> . . . . .	151
<b>shutdown</b> . . . . .	152
<b>description</b> . . . . .	153

<b>speed</b> . . . . .	154
<b>duplex</b> . . . . .	154
<b>negotiation</b> . . . . .	155
<b>flowcontrol</b> . . . . .	156
<b>system flowcontrol</b> . . . . .	157
<b>mdix</b> . . . . .	157
<b>back-pressure</b> . . . . .	158
<b>port jumbo-frame</b> . . . . .	159
<b>clear counters</b> . . . . .	159
<b>set interface active</b> . . . . .	160
<b>show interfaces configuration</b> . . . . .	160
<b>show interfaces status</b> . . . . .	162
<b>show interfaces advertise</b> . . . . .	165
<b>show interfaces description</b> . . . . .	167
<b>show interfaces counters</b> . . . . .	168
<b>show ports jumbo-frame</b> . . . . .	172
<b>port storm-control include-multicast</b> . . . . .	173
<b>port storm-control broadcast enable</b> . . . . .	173
<b>port storm-control broadcast rate</b> . . . . .	174
<b>show ports storm-control</b> . . . . .	175
<b>show system flowcontrol</b> . . . . .	176
11 <b>DHCP Snooping</b> . . . . .	179
<b>ip dhcp snooping</b> . . . . .	179
<b>ip dhcp snooping vlan</b> . . . . .	179
<b>ip dhcp snooping trust</b> . . . . .	180
<b>ip dhcp snooping information option allowed-untrusted</b> . . . . .	180

<b>ip dhcp snooping verify</b> . . . . .	<b>181</b>
<b>ip dhcp snooping database</b> . . . . .	<b>182</b>
<b>ip dhcp snooping database update-freq.</b> . . . . .	<b>182</b>
<b>ip dhcp snooping binding</b> . . . . .	<b>183</b>
<b>clear ip dhcp snooping database</b> . . . . .	<b>184</b>
<b>show ip dhcp snooping</b> . . . . .	<b>184</b>
<b>show ip dhcp snooping binding</b> . . . . .	<b>185</b>
<b>12 GVRP Commands.</b> . . . . .	<b>187</b>
<b>gvrp enable (global)</b> . . . . .	<b>187</b>
<b>gvrp enable (interface).</b> . . . . .	<b>187</b>
<b>garp timer</b> . . . . .	<b>188</b>
<b>gvrp vlan-creation-forbid</b> . . . . .	<b>189</b>
<b>gvrp registration-forbid</b> . . . . .	<b>190</b>
<b>clear gvrp statistics</b> . . . . .	<b>191</b>
<b>show gvrp configuration.</b> . . . . .	<b>191</b>
<b>show gvrp statistics</b> . . . . .	<b>192</b>
<b>13 IGMP Snooping Commands</b> . . . . .	<b>195</b>
<b>ip igmp snooping (Global)</b> . . . . .	<b>195</b>
<b>ip igmp snooping (Interface).</b> . . . . .	<b>195</b>
<b>ip igmp snooping mrouter</b> . . . . .	<b>196</b>
<b>ip igmp snooping host-time-out</b> . . . . .	<b>197</b>
<b>ip igmp snooping mrouter-time-out</b> . . . . .	<b>197</b>
<b>ip igmp snooping leave-time-out</b> . . . . .	<b>198</b>
<b>ip igmp snooping querier enable</b> . . . . .	<b>199</b>
<b>ip igmp snooping querier address.</b> . . . . .	<b>200</b>

	<b>show ip igmp snooping mrouter</b> . . . . .	200
	<b>show ip igmp snooping interface</b> . . . . .	201
	<b>show ip igmp snooping groups</b> . . . . .	202
14	<b>IP Addressing Commands</b> . . . . .	205
	<b>clear host dhcp</b> . . . . .	205
	<b>ip address</b> . . . . .	205
	<b>ip address dhcp</b> . . . . .	206
	<b>ip default-gateway</b> . . . . .	207
	<b>show ip interface</b> . . . . .	208
	<b>arp</b> . . . . .	209
	<b>arp timeout</b> . . . . .	210
	<b>clear arp-cache</b> . . . . .	210
	<b>show arp</b> . . . . .	211
	<b>ip domain-lookup</b> . . . . .	212
	<b>ip domain-name</b> . . . . .	213
	<b>ip name-server</b> . . . . .	213
	<b>ip host</b> . . . . .	214
	<b>clear host</b> . . . . .	215
	<b>show hosts</b> . . . . .	215
15	<b>IPv6 Addressing</b> . . . . .	217
	<b>ipv6 enable</b> . . . . .	217
	<b>ipv6 address autoconfig</b> . . . . .	218
	<b>ipv6 icmp error-interval</b> . . . . .	218
	<b>show ipv6 icmp error-interval</b> . . . . .	219
	<b>ipv6 address</b> . . . . .	220

<b>ipv6 address link-local</b> . . . . .	221
<b>ipv6 unreachable</b> . . . . .	222
<b>ipv6 default-gateway</b> . . . . .	222
<b>ipv6 mld join-group</b> . . . . .	223
<b>ipv6 mld version</b> . . . . .	224
<b>show ipv6 interface</b> . . . . .	225
<b>show ipv6 route</b> . . . . .	227
<b>ipv6 nd dad attempts</b> . . . . .	228
<b>ipv6 host</b> . . . . .	229
<b>ipv6 neighbor</b> . . . . .	230
<b>ipv6 set mtu</b> . . . . .	231
<b>show ipv6 neighbors</b> . . . . .	232
<b>clear ipv6 neighbors</b> . . . . .	234
16 <b>iSCSI Commands</b> . . . . .	235
<b>iscsi enable</b> . . . . .	235
<b>iscsi target port</b> . . . . .	235
<b>iscsi cos</b> . . . . .	237
<b>iscsi aging time</b> . . . . .	237
<b>iscsi max connections</b> . . . . .	238
<b>show iscsi</b> . . . . .	239
<b>show iscsi sessions</b> . . . . .	240
17 <b>LACP Commands</b> . . . . .	243
<b>lacp system-priority</b> . . . . .	243
<b>lacp port-priority</b> . . . . .	243
<b>lacp timeout</b> . . . . .	244



<b>show lacp ethernet</b> . . . . .	245
<b>show lacp port-channel</b> . . . . .	245
<b>18 Line Commands</b> . . . . .	<b>247</b>
<b>line</b> . . . . .	<b>247</b>
speed . . . . .	247
<b>autobaud</b> . . . . .	<b>248</b>
exec-timeout . . . . .	249
<b>show line</b> . . . . .	<b>250</b>
<b>terminal history</b> . . . . .	<b>250</b>
<b>terminal history size</b> . . . . .	<b>251</b>
<b>19 LLDP Commands</b> . . . . .	<b>253</b>
<b>lldp enable (global)</b> . . . . .	<b>253</b>
<b>lldp enable (interface)</b> . . . . .	<b>253</b>
<b>lldp timer</b> . . . . .	<b>254</b>
<b>lldp hold-multiplier</b> . . . . .	<b>255</b>
<b>lldp reinit-delay</b> . . . . .	<b>256</b>
<b>lldp tx-delay</b> . . . . .	<b>256</b>
<b>lldp optional-tlv</b> . . . . .	<b>257</b>
<b>lldp management-address</b> . . . . .	<b>258</b>
<b>lldp med enable</b> . . . . .	<b>259</b>
<b>lldp med network-policy (global)</b> . . . . .	<b>259</b>
<b>lldp med network-policy (interface)</b> . . . . .	<b>260</b>
<b>lldp med location</b> . . . . .	<b>261</b>
<b>clear lldp rx</b> . . . . .	<b>262</b>
<b>show lldp configuration</b> . . . . .	<b>262</b>
<b>show lldp local</b> . . . . .	<b>263</b>

	<b>show lldp neighbors</b> . . . . .	265
	<b>show lldp med configuration</b> . . . . .	266
20	<b>Management ACL</b> . . . . .	269
	<b>management access-list</b> . . . . .	269
	<b>permit (management)</b> . . . . .	271
	<b>deny (management)</b> . . . . .	272
	<b>management access-class</b> . . . . .	273
	<b>show management access-list</b> . . . . .	273
	<b>show management access-class</b> . . . . .	274
21	<b>PHY Diagnostics Commands</b> . . . . .	275
	<b>test copper-port tdr</b> . . . . .	275
	<b>show copper-ports tdr</b> . . . . .	275
	<b>show copper-ports cable-length</b> . . . . .	276
	<b>show fiber-ports optical-transceiver</b> . . . . .	277
22	<b>Port Channel Commands</b> . . . . .	281
	<b>interface port-channel</b> . . . . .	281
	<b>interface range port-channel</b> . . . . .	281
	<b>channel-group</b> . . . . .	282
	<b>port-channel load-balance</b> . . . . .	283
	<b>show interfaces port-channel</b> . . . . .	284
23	<b>Port Monitor Commands</b> . . . . .	285
	<b>port monitor</b> . . . . .	285
	<b>show ports monitor</b> . . . . .	286

24	QoS Commands	289
	<b>qos</b>	289
	<b>show qos</b>	289
	<b>wrr-queue cos-map</b>	290
	<b>wrr-queue bandwidth</b>	291
	<b>priority-queue out num-of-queues</b>	292
	<b>traffic-shape</b>	293
	<b>rate-limit (Ethernet)</b>	293
	<b>show qos interface</b>	294
	<b>qos map dscp-queue</b>	296
	<b>qos trust (Global)</b>	296
	<b>qos trust (Interface)</b>	297
	<b>qos cos</b>	298
	<b>show qos map</b>	298
25	Radius Commands	301
	<b>radius-server host</b>	301
	<b>radius-server key</b>	302
	<b>radius-server retransmit</b>	303
	<b>radius-server source-ip</b>	304
	<b>radius-server source-ipv6</b>	304
	<b>radius-server timeout</b>	305
	<b>radius-server deadtime</b>	306
	<b>show radius-servers</b>	306

26	RMON Commands . . . . .	309
	<b>show rmon statistics</b> . . . . .	309
	<b>rmon collection history</b> . . . . .	311
	<b>show rmon collection history</b> . . . . .	312
	<b>show rmon history</b> . . . . .	314
	<b>rmon alarm</b> . . . . .	317
	<b>show rmon alarm-table</b> . . . . .	318
	<b>show rmon alarm</b> . . . . .	319
	<b>rmon event</b> . . . . .	321
	<b>show rmon events</b> . . . . .	322
	<b>show rmon log</b> . . . . .	323
	<b>rmon table-size</b> . . . . .	325
27	SNMP Commands . . . . .	327
	<b>snmp-server community</b> . . . . .	327
	<b>snmp-server view</b> . . . . .	328
	<b>snmp-server filter</b> . . . . .	329
	<b>snmp-server contact</b> . . . . .	330
	<b>snmp-server location</b> . . . . .	331
	<b>snmp-server enable traps</b> . . . . .	331
	<b>snmp-server trap authentication</b> . . . . .	332
	<b>snmp-server host</b> . . . . .	332
	<b>snmp-server set</b> . . . . .	334
	<b>snmp-server group</b> . . . . .	335
	<b>snmp-server user</b> . . . . .	336
	<b>snmp-server v3-host</b> . . . . .	337
	<b>snmp-server engineID local</b> . . . . .	339

<b>show snmp engineid</b> . . . . .	341
<b>show snmp</b> . . . . .	341
<b>show snmp views</b> . . . . .	342
<b>show snmp groups</b> . . . . .	343
<b>show snmp filters</b> . . . . .	344
<b>show snmp users</b> . . . . .	345
<b>28 Spanning-Tree Commands</b> . . . . .	<b>347</b>
<b>spanning-tree</b> . . . . .	347
<b>spanning-tree mode</b> . . . . .	347
<b>spanning-tree forward-time</b> . . . . .	348
<b>spanning-tree hello-time</b> . . . . .	349
<b>spanning-tree max-age</b> . . . . .	350
<b>spanning-tree priority</b> . . . . .	350
<b>spanning-tree disable</b> . . . . .	351
<b>spanning-tree cost</b> . . . . .	352
<b>spanning-tree port-priority</b> . . . . .	352
<b>spanning-tree portfast</b> . . . . .	353
<b>spanning-tree link-type</b> . . . . .	354
<b>spanning-tree mst priority</b> . . . . .	354
<b>spanning-tree mst max-hops</b> . . . . .	355
<b>spanning-tree mst port-priority</b> . . . . .	356
<b>spanning-tree mst cost</b> . . . . .	356
<b>spanning-tree mst configuration</b> . . . . .	357
<b>instance (mst)</b> . . . . .	358
<b>name (mst)</b> . . . . .	359
<b>revision (mst)</b> . . . . .	359

<b>show (mst)</b> . . . . .	<b>360</b>
<b>exit (mst)</b> . . . . .	<b>361</b>
<b>abort (mst)</b> . . . . .	<b>361</b>
<b>spanning-tree pathcost method</b> . . . . .	<b>362</b>
<b>spanning-tree bpdu</b> . . . . .	<b>362</b>
<b>clear spanning-tree detected-protocols</b> . . . . .	<b>363</b>
<b>show spanning-tree</b> . . . . .	<b>364</b>
<b>Spanning-tree guard root</b> . . . . .	<b>376</b>
<b>29 SSH Commands</b> . . . . .	<b>377</b>
<b>ip ssh port</b> . . . . .	<b>377</b>
<b>ip ssh server</b> . . . . .	<b>377</b>
<b>crypto key generate dsa</b> . . . . .	<b>378</b>
<b>crypto key generate rsa</b> . . . . .	<b>379</b>
<b>ip ssh pubkey-auth</b> . . . . .	<b>379</b>
<b>crypto key pubkey-chain ssh</b> . . . . .	<b>380</b>
<b>user-key</b> . . . . .	<b>380</b>
<b>key-string</b> . . . . .	<b>381</b>
<b>show ip ssh</b> . . . . .	<b>382</b>
<b>show crypto key mypubkey</b> . . . . .	<b>384</b>
<b>show crypto key pubkey-chain ssh</b> . . . . .	<b>385</b>
<b>30 Syslog Commands</b> . . . . .	<b>387</b>
<b>logging on</b> . . . . .	<b>387</b>
<b>logging</b> . . . . .	<b>387</b>
<b>logging console</b> . . . . .	<b>389</b>
<b>logging buffered</b> . . . . .	<b>389</b>

<b>logging buffered size.</b> . . . . .	390
<b>clear logging.</b> . . . . .	391
<b>logging file.</b> . . . . .	391
<b>clear logging file.</b> . . . . .	392
<b>aaa logging.</b> . . . . .	392
<b>file-system logging.</b> . . . . .	393
<b>management logging.</b> . . . . .	394
<b>show logging.</b> . . . . .	394
<b>show logging file.</b> . . . . .	396
<b>show syslog-servers.</b> . . . . .	398
<b>31 System Management.</b> . . . . .	<b>401</b>
<b>ping.</b> . . . . .	401
<b>traceroute.</b> . . . . .	403
<b>telnet.</b> . . . . .	405
<b>resume.</b> . . . . .	408
<b>reload.</b> . . . . .	409
<b>hostname.</b> . . . . .	409
<b>service cpu-utilization.</b> . . . . .	410
<b>show cpu utilization.</b> . . . . .	411
<b>show users.</b> . . . . .	411
<b>show sessions.</b> . . . . .	412
<b>show system.</b> . . . . .	413
<b>set system.</b> . . . . .	414
<b>show system mode.</b> . . . . .	415

<b>show version</b> . . . . .	415
<b>asset-tag</b> . . . . .	416
<b>show system id</b> . . . . .	417
<b>32 TACACS Commands</b> . . . . .	419
<b>tacacs-server host</b> . . . . .	419
<b>tacacs-server key</b> . . . . .	420
<b>tacacs-server timeout</b> . . . . .	420
<b>tacacs-server source-ip</b> . . . . .	421
<b>show tacacs</b> . . . . .	422
<b>33 TIC Commands</b> . . . . .	423
<b>passwords min-length</b> . . . . .	423
<b>password-aging</b> . . . . .	424
<b>passwords aging</b> . . . . .	424
<b>passwords history</b> . . . . .	425
<b>passwords history hold-time</b> . . . . .	426
<b>passwords lockout</b> . . . . .	426
<b>aaa login-history file</b> . . . . .	427
<b>set username active</b> . . . . .	428
<b>set line active</b> . . . . .	428
<b>set enable-password active</b> . . . . .	429
<b>show passwords configuration</b> . . . . .	429
<b>show users login-history</b> . . . . .	431



34	Tunnel . . . . .	433
	<b>interface tunnel</b> . . . . .	433
	<b>tunnel mode ipv6ip</b> . . . . .	433
	<b>tunnel isatap router</b> . . . . .	434
	<b>tunnel source</b> . . . . .	435
	<b>tunnel isatap query-interval</b> . . . . .	436
	<b>tunnel isatap solicitation-interval</b> . . . . .	436
	<b>tunnel isatap robustness</b> . . . . .	437
	<b>show ipv6 tunnel</b> . . . . .	438
35	User Interface . . . . .	441
	<b>enable</b> . . . . .	441
	<b>disable</b> . . . . .	441
	<b>login</b> . . . . .	442
	<b>configure</b> . . . . .	443
	<b>exit(configuration)</b> . . . . .	443
	<b>exit(EXEC)</b> . . . . .	444
	<b>end</b> . . . . .	444
	<b>help</b> . . . . .	445
	<b>history</b> . . . . .	445
	<b>terminal datadump</b> . . . . .	446
	<b>history size</b> . . . . .	447
	<b>debug-mode</b> . . . . .	447
	<b>show history</b> . . . . .	448
	<b>show privilege</b> . . . . .	449
	<b>do</b> . . . . .	449

36	VLAN Commands . . . . .	451
	<b>vlan database</b> . . . . .	451
	<b>vlan</b> . . . . .	451
	<b>interface vlan</b> . . . . .	452
	<b>interface range vlan</b> . . . . .	453
	<b>name</b> . . . . .	453
	<b>switchport access vlan</b> . . . . .	454
	<b>switchport trunk allowed vlan</b> . . . . .	455
	<b>switchport trunk native vlan</b> . . . . .	455
	<b>switchport general allowed vlan</b> . . . . .	456
	<b>switchport general pvid</b> . . . . .	457
	<b>switchport general ingress-filtering disable</b> . . . . .	458
	<b>switchport general acceptable-frame-type tagged-only</b> . . . . .	458
	<b>switchport forbidden vlan</b> . . . . .	459
	<b>switchport mode</b> . . . . .	460
	<b>switchport customer vlan</b> . . . . .	460
	<b>map protocol protocols-group</b> . . . . .	461
	<b>switchport general map protocols-group vlan</b> . . . . .	462
	<b>switchport protected</b> . . . . .	463
	<b>ip internal-usage-vlan</b> . . . . .	463
	<b>show vlan</b> . . . . .	464
	<b>show vlan internal usage</b> . . . . .	465
	<b>show vlan protocols-groups</b> . . . . .	466
	<b>show interfaces switchport</b> . . . . .	467

37	Voice VLAN. . . . .	469
	<b>voice vlan id</b> . . . . .	469
	<b>voice vlan oui-table</b> . . . . .	469
	<b>voice vlan cos</b> . . . . .	471
	<b>voice vlan aging-timeout</b> . . . . .	471
	<b>voice vlan enable</b> . . . . .	472
	<b>voice vlan secure</b> . . . . .	473
	<b>show voice vlan</b> . . . . .	473
38	Web Server. . . . .	477
	<b>ip http server</b> . . . . .	477
	<b>ip http port</b> . . . . .	477
	<b>ip http exec-timeout</b> . . . . .	478
	<b>ip https server</b> . . . . .	479
	<b>ip https port.</b> . . . . .	479
	<b>ip https exec-timeout</b> . . . . .	480
	<b>crypto certificate generate</b> . . . . .	481
	<b>crypto certificate request</b> . . . . .	482
	<b>crypto certificate import.</b> . . . . .	483
	<b>ip https certificate</b> . . . . .	485
	<b>crypto certificate import pkcs12.</b> . . . . .	485
	<b>show crypto certificate mycertificate.</b> . . . . .	487
	<b>show ip http</b> . . . . .	488
	<b>show ip https.</b> . . . . .	488

39	802.1x Commands	491
	<b>aaa authentication dot1x</b>	491
	<b>dot1x system-auth-control</b>	492
	<b>dot1x port-control</b>	492
	<b>dot1x re-authentication</b>	493
	<b>dot1x timeout re-authperiod</b>	494
	<b>dot1x re-authenticate</b>	495
	<b>dot1x timeout quiet-period</b>	495
	<b>dot1x timeout tx-period</b>	496
	<b>dot1x max-req</b>	497
	<b>dot1x timeout supp-timeout</b>	498
	<b>dot1x timeout server-timeout</b>	498
	<b>dot1x send-async-request-id</b>	499
	<b>show dot1x</b>	500
	<b>show dot1x users</b>	502
	<b>show dot1x statistics</b>	503
	<b>ADVANCED FEATURES</b>	505
	<b>dot1x auth-not-req</b>	505
	<b>dot1x multiple-hosts</b>	506
	<b>dot1x single-host-violation</b>	506
	<b>dot1x guest-vlan</b>	507
	<b>dot1x guest-vlan enable</b>	508
	<b>dot1x mac-authentication</b>	509
	<b>dot1x traps mac-authentication failure</b>	509
	<b>dot1x radius-attributes vlan</b>	510
	<b>show dot1x advanced</b>	511

# Using the CLI

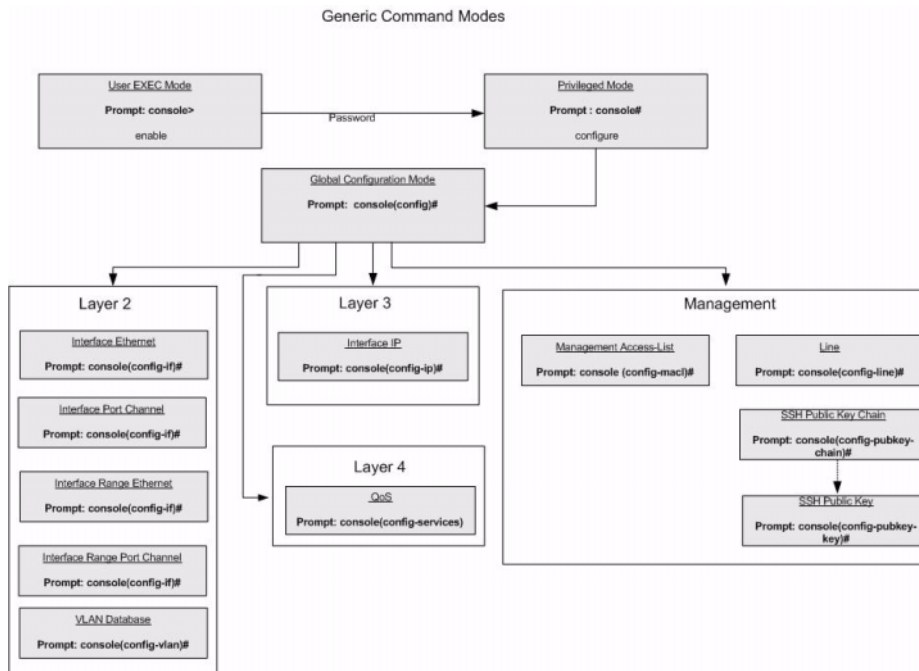
This chapter describes how to start using the CLI and describes implemented command editing features to assist in using the CLI.

## CLI Command Modes

### Introduction

To assist in configuring devices, the CLI (Command Line Interface) is divided into different command modes. Each command mode has its own set of specific commands. Entering a question mark "?" at the system prompt (console prompt) displays a list of commands available for that particular command mode.

From each mode a specific command is used to navigate from one command mode to another. The standard order to access the modes is as follows: *User EXEC mode*, *Privileged EXEC mode*, *Global Configuration mode*, and *Interface Configuration mode*. The following figure illustrates the command mode access path.



When starting a session, the initial mode is the User EXEC mode. Only a limited subset of commands are available in User EXEC Mode. This level is reserved for tasks that do not change the configuration. To enter the next level, the Privileged EXEC mode, a password is required.

The Privileged mode gives access to commands that are restricted on EXEC mode and provides access to the device Configuration mode.

The Global Configuration mode manages the device configuration on a global level.

The Interface Configuration mode configures specific interfaces in the device.

## User EXEC Mode

After logging into the device, the user is automatically in User EXEC command mode unless the user is defined as a privileged user. In general, the User EXEC commands allow the user to perform basic tests, and list system information.

The user-level prompt consists of the device "host name" followed by the angle bracket (>).

```
console>
```

The default host name is "Console" unless it has been changed using the **hostname** command in the Global Configuration mode.

## Privileged EXEC Mode

Privileged access is password protected to prevent unauthorized use because many of the privileged commands set operating system parameters: The password is not displayed on the screen and is case sensitive.

Privileged users enter directly into the Privileged EXEC mode. To enter the Privileged EXEC mode from the User EXEC mode, perform the following steps:

- 1 At the prompt enter the command **enable** and press <Enter>. A password prompt is displayed.
- 2 Enter the password and press <Enter>. The password is displayed as "\*". The Privileged EXEC mode prompt is displayed. The Privileged EXEC mode prompt consists of the device "host name" followed by "#".

```
console#
```

To return from Privileged Exec mode to User EXEC mode, type the **disable** command at the command prompt.

The following example illustrates how to access Privileged Exec mode and return back to the User EXEC mode:

```
console>enable
Enter Password: *****
console#
console#disable
console>
```

The Exit command is used to return from any mode to the previous mode except when returning to User EXEC mode from the Privileged EXEC mode. For example, the Exit command is used to return from the Interface Configuration mode to the Global Configuration mode

### Global Configuration Mode

Global Configuration mode commands apply to features that affect the system as a whole, rather than just a specific interface. The Privileged EXEC mode command **configure** is used to enter the Global Configuration mode.

To enter the Global Configuration mode perform the following steps:

- 1 At the Privileged EXEC mode prompt enter the command **configure** and press <Enter>. The Global Configuration mode prompt is displayed. The Global Configuration mode prompt consists of the device "host name" followed by the word "(config)" and "#".

```
console(config)#
```

- 2 Use one of the following commands to return from the Global Configuration mode to the Privileged EXEC mode:
  - **exit**
  - **end**
  - **Ctrl+Z**

The following example illustrates how to access Global Configuration mode and returns to the Privileged EXEC mode:

```
console#
console#configure
console(config)#exit
console#
```

## Interface Configuration Mode and Specific Configuration Modes

Interface Configuration mode commands are to modify specific interface operations. The following are the Interface Configuration modes:

- **Line Interface** — Contains commands to configure the management connections. These include commands such as line speed, timeout settings, etc. The Global Configuration mode command line is used to enter the Line Configuration command mode.
- **VLAN Database** — Contains commands to create a VLAN as a whole. The Global Configuration mode command vlan database is used to enter the VLAN Database Interface Configuration mode.
- **Management Access List** — Contains commands to define management access-lists. The Global Configuration mode command management access-list is used to enter the Management Access List Configuration mode.
- **Ethernet** — Contains commands to manage port configuration. The Global Configuration mode command interface ethernet is used to enter the Interface Configuration mode to configure an Ethernet type interface.
- **Port Channel** — Contains commands to configure port-channels, for example, assigning ports to a VLAN or port-channel. Most of these commands are the same as the commands in the Ethernet interface mode, and are used to manage the member ports as a single entity. The Global Configuration mode command interface port-channel is used to enter the Port Channel Interface Configuration mode.
- **SSH Public Key-chain** — Contains commands to manually specify other device SSH public keys. The Global Configuration mode command crypto key pubkey-chain ssh is used to enter the SSH Public Key-chain Configuration mode.
- **Interface** — Contains commands that configure the interface. The Global Configuration mode command interface ethernet is used to enter the Interface Configuration mode.
- **QoS** — Contains commands related to service definitions. The Global Configuration mode command qos config-services is used to enter the QoS services configuration mode.

## Starting the CLI

The switch can be managed over a direct connection to the switch console port, or via a Telnet connection. The switch is managed by entering command keywords and parameters at the prompt. Using the switch command-line interface (CLI) is very similar to entering commands on a UNIX system.

If access is via a Telnet connection, ensure the device has an IP address defined, corresponding management access is granted, and the workstation used to access the device is connected to the device prior to using CLI commands.



**NOTE:** The following steps are for use on the console line only.



To start using the CLI, perform the following steps:

- 1 Start the device and wait until the startup procedure is complete.  
The User Exec mode is entered, and the prompt "Console>" is displayed.
- 2 Configure the device and enter the necessary commands to complete the required tasks.
- 3 When finished, exit the session with the **quit** or **exit** command.

When a different user is required to log onto the system, in the Privileged EXEC mode command mode the login command is entered. This effectively logs off the current user and logs on the new user.

## Editing Features

### Entering Commands

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "**show interfaces status ethernet g5**," **show**, **interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **g5** specifies the port.

To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)# username admin password smith
```

When working with the CLI, the command options are not displayed. The command is not selected from a menu but is manually entered. To see what commands are available in each mode or within an Interface Configuration, the CLI does provide a method of displaying the available commands, the command syntax requirements and in some instances parameters required to complete the command. The standard command to request help is?

There are two instances where the help information can be displayed:

- **Keyword lookup** — The character ? is entered in place of a command. A list of all valid commands and corresponding help messages are displayed.
- **Partial keyword lookup** — A command is incomplete and the character ? is entered in place of a parameter. The matched parameters for this command are displayed.

To assist in using the CLI, there is an assortment of editing features. The following features are described:

- Terminal Command Buffer
- Command Completion
- Keyboard Shortcuts

## Setup Wizard

The CLI supports a Setup Wizard. This is an easy-to-use user interface which quickly guides the user in setting up basic device information, so that the device can be easily managed from a Web Based Interface. Refer to the **Getting Started Guide** and **User Guide** for more information on the Setup Wizard.

### Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a *First In First Out (FIFO)* basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets.

Keyword	Source or destination
Up-arrow key Ctrl+P	Recalls commands in the history buffer, beginning with the most recent command. Repeats the key sequence to recall successively older commands.
Down-arrow key	Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence will recall successively more recent commands.

By default, the history buffer system is enabled, but it can be disabled at any time. For information about the command syntax to enable or disable the history buffer, see `history`.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 256. By configuring 0, the effect is the same as disabling the history buffer system. For information about the command syntax for configuring the command history buffer, see `history size`.

To display the history buffer, see `show history`.

### Negating the Effect of Commands

For many configuration commands, the prefix keyword `no` can be entered to cancel the effect of a command or reset the configuration to the default value. This guide describes the negation effect for all applicable commands.

## Command Completion

If the command entered is incomplete, invalid, or has missing or invalid parameters, then the appropriate error message is displayed. This assists in entering the correct command. By pressing the <Tab> button, an incomplete command is entered. If the characters already entered are not enough for the system to identify a single matching command, press "?" to display the available commands matching the characters already entered.

Incorrect or incomplete commands are automatically re-entered next to the cursor. If a parameter must be added, the parameter can be added to the basic command already displayed next to the cursor. The following example indicates that the command interface ethernet requires a missing parameter.

```
(config)#interface ethernet
%missing mandatory parameter
(config)#interface ethernet
```

## Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The following table describes the CLI shortcuts.

Keyboard Key	Description
Up-arrow key	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-arrow key	Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+Z / End	Returns back to the Privileged EXEC mode from any mode.
Backspace key	Moves the cursor back one space.

## CLI Command Conventions

When entering commands there are certain command entry standards that apply to all commands. The following table describes the command conventions.

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry.
{ }	In a command line, curly brackets indicate a selection of compulsory parameters separated by the   character. One option must be selected. For example: <b>flowcontrol {auto on off}</b> means that for the <b>flowcontrol</b> command either <b>auto</b> , <b>on</b> or <b>off</b> must be selected.
<i>Italic font</i>	Indicates a parameter.
<Enter>	Any individual key on the keyboard. For example click <Enter>.
Ctrl+F4	Any combination keys pressed simultaneously on the keyboard.
Screen Display	Indicates system messages and prompts appearing on the console.
all	When a parameter is required to define a range of ports or parameters and <b>all</b> is an option, the default for the command is <b>all</b> when no parameters are defined. For example, the command <b>interface range port-channel</b> has the option of either entering a range of channels, or selecting <b>all</b> . When the command is entered without a parameter, it automatically defaults to <b>all</b> .

# Command Groups

## Introduction

The Command Language Interface (CLI) is a network management application operated through an ASCII terminal without the use of a Graphic User Interface (GUI) driven software application. By directly entering commands, you have greater configuration flexibility. The CLI is a basic command-line interpreter similar to the UNIX C shell.

A device can be configured and maintained by entering commands from the CLI, which is based solely on textual input and output with commands being entered from a terminal keyboard and the output displayed as text via a terminal monitor. The CLI can be accessed from a VT100 terminal connected to the console port of the device or through a Telnet connection from a remote host.

The first time you use the CLI from the console a Setup Wizard is invoked. The Setup Wizard guides you in setting up a minimum configuration, so that the device can be managed from the Web Based Interface. Refer to the Getting Started Guide and User Guide for more information on the Setup Wizard.

This guide describes how the Command Line Interface (CLI) is structured, describes the command syntax, and describes the command functionality.

This guide also provides information for configuring the Dell™ PowerConnect™ switch, details the procedures and provides configuration examples. Basic installation configuration is described in the *User's Guide* and must be completed before using this document.

## Command Groups

The system commands can be broken down into the functional groups shown below.

<b>Command Group</b>	<b>Description</b>
ACL Commands	Configures and displays ACL configuration and information.
AAA Commands	Configures connection security including authorization and passwords.
Address Table Commands	Configures bridging address tables.
Configuration and Image Files Commands	Manages the device Configuration files.
Clock Commands	Configures clock commands on the device.
DHCP Snooping Commands	Configures DHCP snooping and displays DHCP configuration and DHCP information.

Ethernet Configuration	Configures all port configuration options for example ports, storm control, port speed and auto-negotiation.
GVRP Commands	Configures and displays GVRP configuration and information.
IGMP Snooping Commands	Configures IGMP snooping and displays IGMP configuration and IGMP information.
IP Addressing Commands	Configures and manages IP addresses on the device.
IPv6 Addressing Commands	Configures and manages IPv6 addresses on the device.
iSCSI Commands	Configures and manages Internet Small Computer Interface System Information (iSCSI).
LACP Commands	Configures and displays LACP information.
Line Commands	Configures the console and remote Telnet connection.
Login Banner Commands	Configures customizable login banners on the device.
Management ACL Commands	Configures and displays management access-list information.
PHY Diagnostics Commands	Diagnoses and displays the interface status.
Port Channel Commands	Configures and displays Port channel information.
Port Monitor Commands	Monitors activity on specific target ports.
QoS Commands	Configures and displays QoS information.
RADIUS Commands	Configures and displays RADIUS information.
RMON Commands	Displays RMON statistics.
SNMP Commands	Configures SNMP communities, traps and displays SNMP information.
Spanning Tree Commands	Configures and reports on Spanning Tree protocol
SSH Commands	Configures SSH authentication.
Syslog Commands	Manages and displays syslog messages.
System Management Commands	Configures the device clock, name and authorized users.
TACACS Commands	Configures TACACS commands
TIC Commands	Configures password access and control.
Tunnel Commands	Configures tunnel routing configurations.
User Interface Commands	Describes user commands used for entering CLI commands.
VLAN Commands	Configures VLANs and displays VLAN information.
Voice VLAN Commands	Configures Voice VLANs and displays Voice VLAN information.
Web Server Commands	Configures Web based access to the device.
802.1x Commands	Configures commands related to 802.1x security protocol.

## ACL Commands

Command Group	Description	Access Mode
ip access-list	Defines an IPv4 Access List and places the device in IPv4 Access List Configuration mode.	Global Configuration
mac access-list	Enables the MAC-Access List Configuration mode and creates Layer 2 ACLs.	Global Configuration
permit (ip)	Permits traffic if the conditions defined in the <i>permit</i> statement match.	IP-Access List Configuration
deny (IP)	Denies traffic if the conditions defined in the <i>deny</i> statement match.	IP-Access List Configuration
permit (MAC)	Defines permit conditions of an MAC ACL.	MAC-Access List Configuration
deny (MAC)	Denies traffic if the conditions defined in the <i>deny</i> statement match.	MAC-Access List Configuration
service-acl	Applies an ACL to the input interface.	Interface Configuration (Ethernet, port-channel)
show access-lists	Displays access control lists (ACLs) defined on the device.	Privileged EXEC
show interfaces access-lists	Displays access lists applied on interfaces.	Privileged EXEC

## AAA Commands

Command Group	Description	Access Mode
aaa authentication login	Defines login authentication.	Global Configuration
aaa authentication enable	Defines authentication method lists for accessing higher privilege levels.	Global Configuration
enable authentication	Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console.	Line Configuration
ip http authentication	Specifies authentication methods for http.	Global Configuration
ip https authentication	Specifies authentication methods for https.	Global Configuration
show authentication methods	Displays information about the authentication methods.	Privileged User EXEC

password	Specifies a password on a line.	Line Configuration
enable password	Sets a local password to control access to normal and privilege levels.	Global Configuration
username	Establishes a username-based authentication system.	Global Configuration
show users accounts	Displays information about the local user database.	Privileged User EXEC

## Address Table Commands

Command Group	Description	Access Mode
bridge address	Adds a static MAC-layer station source address to the bridge table.	VLAN Configuration
bridge multicast filtering	Enables filtering of Multicast addresses.	Global Configuration
bridge multicast address	Registers MAC-layer Multicast addresses to the bridge table, and adds static ports to the group.	VLAN Configuration
bridge multicast forbidden address	Forbids adding a specific Multicast address to specific ports.	VLAN Configuration
bridge multicast unregistered	Configures the forwarding state of unregistered multicast addresses.	Interface Configuration
bridge multicast forward-all	Enables forwarding of all Multicast frames on a port.	VLAN Configuration
bridge multicast forbidden forward-all	Enables forbidding forwarding of all Multicast frames to a port.	VLAN Configuration
bridge aging-time	Sets the address table aging time.	Global Configuration
clear bridge	Removes any learned entries from the forwarding database.	Privileged User EXEC
port security	Disables new address learning on an interface.	Interface Configuration
port security routed secure-address	Adds MAC-layer secure addresses to a routed port.	Interface Configuration
show bridge address-table	Displays dynamically created entries in the bridge-forwarding database.	Privileged User EXEC
show bridge address-table static	Displays statically created entries in the bridge-forwarding database.	Privileged User EXEC



show bridge address-table count	Displays the number of addresses present in all or at a specific VLAN.	Privileged User EXEC
show bridge multicast address-table	Displays statically created entries in the bridge-forwarding database.	Privileged User EXEC
show bridge multicast filtering	Displays the Multicast filtering configuration.	Privileged User EXEC
show ports security	Displays the port-lock status.	Privileged User EXEC
show ports security addresses	Displays the current dynamic addresses in locked ports.	Privileged User EXEC

## Clock Commands

Command Group	Description	Access Mode
clock set	Manually sets the system clock.	Privileged User EXEC
clock source	Configures an external time source for the system clock.	Privileged User EXEC
clock timezone	Sets the time zone for display purposes.	Global Configuration
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).	Global Configuration
sntp authentication-key	Defines an authentication key for Simple Network Time Protocol (SNTP).	Global Configuration
sntp authenticate	Grants authentication for received Network Time Protocol (NTP) traffic from servers.	Global Configuration
sntp trusted-key	Authenticates the identity of a system to which SNTP will synchronize.	Global Configuration
sntp client poll timer	Sets the polling time for the SNTP client.	Global Configuration
sntp broadcast client enable	Enables the SNTP Broadcast clients.	Global Configuration
sntp anycast client enable	Enables Anycast clients.	Global Configuration
sntp client enable (interface)	Enables the SNTP client on an interface.	Interface Configuration

sntp unicast client enable	Enables the device to use the SNTP to request and accept NTP traffic from servers.	Global Configuration
sntp unicast client poll	Enables polling for the SNTP predefined Unicast clients.	Global Configuration
sntp server	Specifies SNTP UDP port of the SNTP server	Global Configuration
show clock	Displays the time and date from the system clock.	User EXEC
show sntp configuration	Shows the configuration of the SNTP.	Privileged User EXEC
show sntp status	Shows the status of the SNTP.	Privileged User EXEC

## Configuration and Image Files Commands

Command Group	Description	Access Mode
dir	Displays list of files on a flash file system	Privileged User EXEC
more	Displays a file	Privileged EXEC
rename	Renames a file.	Privileged User EXEC
delete startup-config	Deletes the startup-config file.	Privileged User EXEC
copy	Copies files from a source to a destination.	Privileged User EXEC
delete	Deletes a file from a Flash memory device.	Privileged User EXEC
boot system	Specifies the system image that the device loads at startup.	Privileged User EXEC
show running-config	Displays the contents of the currently running configuration file.	Privileged User EXEC
show startup-config	Displays the startup configuration file contents.	Privileged User EXEC
show bootvar	Displays the active system image file that the device loads at startup.	Privileged EXEC

## DHCP Snooping Commands

Command Group	Description	Access Mode
ip dhcp snooping	Globally enables Dynamic Host Configuration Protocol (DHCP) snooping	Global Configuration
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN.	Global Configuration
ip dhcp snooping trust	Configures a port as trusted for DHCP snooping purposes.	Interface Configuration (Ethernet, port-channel)
ip dhcp snooping information option allowed-untrusted	Configures a switch to accept DHCP packets with option-82 information from an untrusted port.	Global Configuration
ip dhcp snooping verify	Configures the switch to verify that on an untrusted port the source MAC address in a DHCP packet matches the client hardware address.	Global Configuration
ip dhcp snooping database	Configures the DHCP snooping binding file.	Global Configuration
ip dhcp snooping database update-freq	Configures the update frequency of the DHCP snooping binding file.	Global Configuration
ip dhcp snooping binding	Configures the DHCP snooping binding database and to add binding entries to the database.	Privileged EXEC
clear ip dhcp snooping database	Clears the DHCP binding database.	Privileged EXEC
show ip dhcp snooping	Displays the DHCP snooping configuration.	EXEC
show ip dhcp snooping binding	Display the DHCP snooping binding database and configuration information for all interfaces on a switch.	EXEC

## Ethernet Configuration Commands

Command Group	Description	Access Mode
interface ethernet	Enters the Interface Configuration mode to configure an Ethernet type interface.	Global Configuration
interface range ethernet	Enters the Interface Configuration mode to configure multiple Ethernet type interfaces.	Global Configuration
shutdown	Disables interfaces.	Interface Configuration

description	Adds a description to an interface.	Interface Configuration
speed	Configures the speed of a given Ethernet interface when not using auto-negotiation.	Interface Configuration
duplex	Configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation.	Interface Configuration
negotiation	Enables auto-negotiation operation for the speed and duplex parameters of a given interface.	Interface Configuration
flowcontrol	Configures the Flow Control on a given interface.	Interface Configuration
system flowcontrol	Enables flow control on cascade ports.	Interface Configuration
mdix	Enables automatic crossover on a given interface.	Interface Configuration
back-pressure	Enables Back Pressure on a given interface.	Interface Configuration
port jumbo-frame	Enables jumbo frames for the device.	Global Configuration
clear counters	Clears statistics on an interface.	User EXEC
set interface active	Reactivates an interface that was suspended by the system.	Privileged User EXEC
show interfaces configuration	Displays the configuration for all configured interfaces.	User EXEC
show interfaces status	Displays the status for all configured interfaces.	User EXEC
show interfaces description	Displays the description for all configured interfaces.	User EXEC
show interfaces counters	Displays traffic seen by the physical interface.	User EXEC
show ports jumbo-frame	Displays the jumbo frames configuration.	User EXEC
port storm-control include-multicast	Enables the device to count Multicast packets.	Global Configuration
port storm-control broadcast enable	Enables Broadcast storm control.	Interface Configuration
port storm-control broadcast rate	Configures the maximum Broadcast rate.	Interface Configuration
show ports storm-control	Displays the storm control configuration.	Privileged User EXEC
show system flowcontrol	Displays the flow control state on cascade ports.	Privileged User EXEC

## GVRP Commands

Command Group	Description	Mode
gvrp enable (global)	Enables GVRP globally.	Global Configuration
gvrp enable (interface)	Enables GVRP on an interface.	Interface Configuration
garp timer	Adjusts the GARP application join, leave, and leaveall GARP timer values.	Interface Configuration
gvrp vlan-creation-forbid	Enables or disables dynamic VLAN creation.	Interface Configuration
gvrp registration-forbid	De-registers all VLANs, and prevents dynamic VLAN registration on the port.	Interface Configuration
clear gvrp statistics	Clears all the GVRP statistics information.	Privileged User EXEC
show gvrp configuration	Displays GVRP configuration information.	User EXEC
show gvrp statistics	Displays GVRP statistics.	User EXEC

## IGMP Snooping Commands

Command Group	Description	Access Mode
ip igmp snooping (Global)	Enables Internet Group Management Protocol (IGMP) snooping.	Global Configuration
ip igmp snooping (Interface)	Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN.	VLAN Configuration
ip igmp snooping mrouter	Enables automatic learning of Multicast router ports in the context of a specific VLAN.	VLAN Configuration
ip igmp snooping host-time-out	Configures the host-time-out.	VLAN Configuration
ip igmp snooping mrouter-time-out	Configures the mrouter-time-out.	VLAN Configuration
ip igmp snooping leave-time-out	Configures the leave-time-out.	VLAN Configuration
show ip igmp snooping mrouter	Displays information on dynamically learned Multicast router interfaces.	User EXEC
show ip igmp snooping interface	Displays IGMP snooping configuration.	User EXEC
show ip igmp snooping groups	Displays Multicast groups learned by IGMP snooping.	User EXEC

## IP Addressing Commands

Command Group	Description	Access Mode
clear host dhcp	Sets an IP address on the device.	Interface Configuration
ip address	Sets an IP address	Interface Configuration
ip address dhcp	Acquires an IP address on an interface from the DHCP server.	Interface Configuration
ip default-gateway	Defines a default gateway (router)	Global Configuration
show ip interface	Displays the usability status of interfaces configured for IP.	User EXEC
arp	Adds a permanent entry in the ARP cache.	Global Configuration
arp timeout	Configures how long an entry remains in the ARP cache	Global Configuration
clear arp-cache	Deletes all dynamic entries from the ARP cache.	Privileged User EXEC
show arp	Displays entries in the ARP table.	Privileged User EXEC
ip domain-lookup	Enables the IP Domain Naming System (DNS)-based host name-to-address translation.	Global Configuration
ip domain-name	Defines a default domain name, that the software uses to complete unqualified host names.	Global Configuration
ip name-server	Sets the available name servers.	Global Configuration
ip host	Defines static host name-to-address mapping in the host cache.	Global Configuration
clear host	Deletes entries from the host name-to-address cache	Privileged User EXEC
show hosts	Displays the default domain name, a list of name server hosts, the static and cached list of host names and addresses.	User EXEC

## IPv6 Addressing Commands

Command Group	Description	Access Mode
ipv6 enable	Enables IPv6 processing on an interface.	Interface Configuration
ipv6 address autoconfig	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface.	Interface Configuration
ipv6 icmp error-interval	Configures the rate limit interval and bucket size parameters for IPv6 ICMP error messages.	Global Configuration
show ipv6 icmp error-interval	Displays the IPv6 ICMP error interval setting	Privileged EXEC
ipv6 address	Configures an IPv6 address for an interface.	Interface Configuration
ipv6 address link-local	Configures an IPv6 link-local address for an interface.	Interface Configuration
ipv6 unreachable	Enables the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface.	Interface Configuration
ipv6 default-gateway	Defines an IPv6 default gateway.	Global Configuration
ipv6 mld join-group	Configures Multicast Listener Discovery (MLD) reporting for a specified group.	Interface Configuration
ipv6 mld version	Changes the Multicast Listener Discovery Protocol (MLD) version.	Interface Configuration
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.	Privileged EXEC
show ipv6 route	Displays the current state of the IPv6 routing table.	Privileged EXEC
ipv6 nd dad attempts	Configures the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the unicast IPv6 addresses of the interface.	Interface Configuration
ipv6 host	Defines a static host name-to-address mapping in the host name cache.	Global Configuration
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache.	Global Configuration
ipv6 set mtu	Sets the MTU size of IPv6 packets sent on an interface.	Privileged EXEC
show ipv6 neighbors	Displays IPv6 neighbor discovery cache informatio.	Privileged EXEC
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.	Privileged EXEC

## iSCSI Commands

Command Group	Description	Access Mode
iscsi enable	Globally enables iSCSI awareness.	Global Configuration
iscsi target port	Configures iSCSI port(s), target address and name.	Global Configuration
iscsi cos	Sets the quality of service profile applied to iSCSI flows.	Global Configuration
iscsi aging time	Sets aging time for iSCSI sessions.	Global Configuration
iscsi max connections	Sets the maximum number of iSCSI connections that can be supported	Global Configuration
show iscsi	Displays the iSCSI settings	Privileged User EXEC
show iscsi sessions	Display the iSCSI sessions	Privileged EXEC

## LACP Commands

Command Group	Description	Access Mode
lacp system-priority	Configures the system LACP priority.	Global Configuration
lacp port-priority	Configures the priority value for physical ports.	Interface Configuration
lacp timeout	Assigns an administrative LACP timeout.	Interface Configuration
show lacp ethernet	Displays LACP information for Ethernet ports.	User EXEC
show lacp port-channel	Displays LACP information for a port-channel.	User EXEC

## Line Commands

Command Group	Description	Access Mode
line	Identifies a specific line for configuration and enters the Line Configuration command mode.	Global Configuration
speed	Sets the line baud rate.	Line Configuration
autobaud	Sets the line for automatic baud rate detection	Line Configuration



exec-timeout	Configures the interval that the system waits until user input is detected.	Line Configuration
show line	Displays line parameters.	User EXEC
terminal history	Enables the command history function for the current terminal session.	User EXEC
terminal history size	Configures the history buffer size for the current terminal session.	User EXEC

## LLDP Commands

Command Group	Description	Access Mode
lldp enable (global)	Enables Link Layer Discovery Protocol.	Interface Configuration (Ethernet)
lldp enable (interface)	Enables Link Layer Discovery Protocol (LLDP) on an interface.	Interface Configuration (Ethernet)
lldp timer	Specifies how often the software sends LLDP updates.	Global Configuration
lldp hold-multiplier	Specifies the amount of time the receiving device should hold a Link Layer Discovery Protocol packet before discarding it.	Global Configuration
lldp reinit-delay	Specifies the minimum time an LLDP port will wait before reinitializing LLDP transmission.	Global Configuration
lldp tx-delay	Specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.	Global Configuration
lldp optional-tlv	Specifies which optional TLVs from the basic set should be transmitted.	Interface Configuration (Ethernet)
lldp management-address	Specifies the management address to be advertised from an interface.	Interface Configuration (Ethernet)
lldp med enable	Enables LLDP Media Endpoint Discovery (MED) on an interface.	Interface Configuration (Ethernet)
lldp med network-policy (global)	Defines LLDP MED network policy.	Global Configuration

lldp med network-policy (interface)	Attaches a LLDP MED network policy to a port.	Interface Configuration (Ethernet)
lldp med location	Configures location information for the LLDP MED for an interface.	Interface Configuration (Ethernet)
clear lldp rx	Restarts the LLDP RX state machine and clearing the neighbors table.	Privileged EXEC
show lldp configuration	Displays the LLDP configuration.	Privileged EXEC
show lldp local	Displays the LLDP information that is advertised from a specific port.	Privileged EXEC
show lldp neighbors	Displays information about neighboring devices discovered using LLDP.	Privileged EXEC
show lldp med configuration	Displays the LLDP MED configuration.	Privileged EXEC

## Login Banner Commands

Command Group	Description	Access Mode
banner exec	Specifies and enables a message to be displayed when an EXEC process is created.	Global Configuration
banner login	Enables a message to be displayed before the username and password login prompts.	Global Configuration
banner motd	Specifies and enables a message-of-the-day banner..	Global Configuration
exec-banner	Enables the display of exec banners.	Line Configuration
login-banner	Enables the display of login banners.	Line Configuration
motd-banner	Enables the display of message-of-the-day banners.	Line Configuration
show banner	Displays the banners configuration.	Privileged EXEC

## Management ACL Commands

Command Group	Description	Access Mode
management access-list	Defines a management access-list, and enters the access-list for configuration.	Global Configuration
permit (management)	Defines a permit rule.	Management Access-level

deny (management)	Defines a deny rule.	Management Access-level
management access-class	Defines which management access-list is used.	Global Configuration
show management access-list	Displays management access-lists.	Privileged User EXEC
show management access-class	Displays the active management access-list.	Privileged User EXEC

## PHY Diagnostics Commands

Command Group	Description	Access Mode
test copper-port tdr	Diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.	Privileged User EXEC
show copper-ports tdr	Displays the last TDR (Time Domain Reflectometry) tests on specified ports.	Privileged User EXEC
show copper-ports cable-length	Displays the estimated copper cable length attached to a port.	Privileged User EXEC
show fiber-ports optical-transceiver	Displays the optical transceiver diagnostics.	Privileged User EXEC

## Port Channel Commands

Command Group	Description	Access Mode
interface port-channel	Enters the Interface Configuration mode of a specific port-channel.	Global Configuration
interface range port-channel	Enters the Interface Configuration mode to configure multiple port-channels.	Global Configuration
channel-group	Associates a port with a port-channel.	Interface Configuration
port-channel load-balance	Configures the load balancing policy of the port channeling	User EXEC
show interfaces port-channel	Displays port-channel information.	User EXEC

## Port Monitor Commands

Command Group	Description	Access Mode
port monitor	Starts a port monitoring session.	Interface Configuration
show ports monitor	Displays the port monitoring status.	User EXEC

## QoS Commands

Command Group	Description	Access Mode
qos	Enables quality of service (QoS) on the device and enters QoS basic or advance mode.	Global Configuration
show qos	Displays the QoS status.	User EXEC
wrr-queue cos-map	Maps assigned CoS values to select one of the egress queues.	Global Configuration
wrr-queue bandwidth	Assigns Weighted Round Robin (WRR) weights to egress queues.	Interface Configuration
priority-queue out num-of-queues	Enables the egress queues to be expedite queues.	Global Configuration
traffic-shape	Sets the shaper on an egress port.	Interface Configuration
rate-limit (Ethernet)	Limits the rate of the incoming traffic.	Interface Configuration (Ethernet, Port-Channel)
show qos interface	Displays interface QoS data.	User EXEC
qos map dscp-queue	Modifies the DSCP to CoS map.	Global Configuration
qos trust (Global)	Configures the system to basic mode and the "trust" state.	Global Configuration
qos trust (Interface)	Enables each port trust state	Interface Configuration
qos cos	Configures the default port CoS value.	Interface Configuration
show qos map	Displays all the maps for QoS.	User EXEC

## RADIUS Commands

Command Group	Description	Access Mode
radius-server host	Specifies a RADIUS server host.	Global Configuration
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.	Global Configuration
radius-server retransmit	Specifies the number of times the software searches the list of RADIUS server hosts.	Global Configuration
radius-server source-ip	Specifies the source IP address used for communication with RADIUS servers.	Global Configuration
radius-server source-ipv6	Specifies the source IPv6 address used for the IPv6 communication with RADIUS servers.	Global Configuration
radius-server timeout	Sets the interval for which a router waits for a server host to reply.	Global Configuration
radius-server deadtime	Improves RADIUS response times when servers are unavailable.	Global Configuration
show radius-servers	Displays the RADIUS server settings.	Privileged User EXEC

## RMON Commands

Command Group	Description	Mode
show rmon statistics	Displays RMON Ethernet Statistics.	User EXEC
rmon collection history	Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.	Interface Configuration (Ethernet, port-channel)s
show rmon collection history	Displays the requested history group configuration.	User EXEC
show rmon history	Displays RMON Ethernet Statistics history.	User EXEC
rmon alarm	Configures alarm conditions.	Global Configuration
show rmon alarm-table	Displays the alarms summary table.	User EXEC
show rmon alarm	Displays alarm configurations.	User EXEC
rmon event	Configures a RMON event.	Global Configuration

show rmon events	Displays the RMON event table.	User EXEC
show rmon log	Displays the RMON logging table.	User EXEC
rmon table-size	Configures the maximum RMON tables sizes.	Global Configuration

## SNMP Commands

Command Group	Description	Access Mode
snmp-server community	the community access string to permit access to SNMP protocol.	Global Configuration
snmp-server view	Creates or update a view entry,	Global Configuration
snmp-server contact	Sets up a system contact.	Global Configuration
snmp-server location	Sets up the information on where the device is located.	Global Configuration
snmp-server enable traps	Enables the switch to send SNMP traps or SNMP notifications.	Global Configuration
snmp-server trap authentication	Enables the switch to send Simple Network Management Protocol traps when authentication failed.	Global Configuration
snmp-server host	Specifies the recipient of Simple Network Management Protocol notification operation,	Global Configuration
snmp-server set	Sets SNMP MIB value by the CLI.	Global Configuration
snmp-server group	Configures a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views.	Global Configuration
snmp-server user	Configure a new SNMP Version 3 user.	Global Configuration
snmp-server v3-host	Specifies the recipient of Simple Network Management Protocol Version 3 notifications.	Global Configuration
snmp-server engineID local	Specifies the Simple Network Management Protocol (SNMP) engineID on the local device.	Global Configuration
show snmp engineid	Displays the ID of the local Simple Network Management Protocol (SNMP) engine	Privileged User EXEC
show snmp	Displays the SNMP status.	Privileged User EXEC

show snmp views	Displays the configuration of views.	Privileged EXEC
show snmp groups	Displays the configuration of groups.	Privileged EXEC
show snmp filters	Displays the configuration of filters	Privileged EXEC
show snmp users	Displays the configuration of groups.	Privileged EXEC

## Spanning Tree Commands

Command Group	Description	Access Mode
spanning-tree	Enables spanning tree functionality.	Global Configuration
spanning-tree mode	Configures the spanning tree protocol.	Global Configuration
spanning-tree forward-time	Configures the spanning tree bridge forward time.	Global Configuration
spanning-tree hello-time	Configures the spanning tree bridge Hello Time.	Global Configuration
spanning-tree max-age	Configures the spanning tree bridge maximum age.	Global Configuration
spanning-tree priority	Configures the spanning tree priority.	Global Configuration
spanning-tree disable	Disables spanning tree on a specific port.	Interface Configuration
spanning-tree cost	Configures the spanning tree path cost for a port.	Interface Configuration
spanning-tree port-priority	Configures port priority.	Interface Configuration
spanning-tree portfast	Enables PortFast mode.	Interface Configuration
spanning-tree link-type	Overrides the default link-type setting.	Interface Configuration (Ethernet, port-channel)
spanning-tree mst priority	Configures the device priority for the specified spanning-tree instance	Global Configuration
spanning-tree mst max-hops	Configures the number of hops in an MST region before the BPDU is discarded and the port information is aged out.	Global Configuration

spanning-tree mst priority	Configures port priority for the specified MST instance	Interface Configuration
s spanning-tree mst cost	Configures the path cost for multiple spanning tree (MST) calculations.	Interface Configuration
spanning-tree mst configuration	Enables configuring an MST region by entering the Multiple Spanning Tree (MST) mode.	Global Configuration
instance (mst)	Maps VLANs to an MST instance.	MST Configuration mode
name (mst)	Defines the configuration name.	MST Configuration mode
revision (mst)	Defines the configuration revision number.	MST Configuration mode
show (mst)	Displays the current or pending MST region configuration.	MST Configuration mode
exit (mst)	Exits the MST Configuration mode and applies all configuration changes.	MST Configuration mode
abort (mst)	Exits the MST Configuration mode without applying the configuration changes	MST Configuration mode
spanning-tree pathcost method	Sets the default path cost method.	Global Configuration
spanning-tree bpdu	Defines BPDU handling when spanning-tree is disabled on an interface.	Global Configuration
clear spanning-tree detected-protocols	Restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.	Privileged EXEC mode
show spanning-tree	Displays spanning-tree configuration.	Privileged EXEC mode
Spanning-tree guard root	Configure the switch to convert STP/RSTP packets to MSTP instances.	Global Configuration
Spanning-tree guard root	enables root guard on all the spanning tree instances on that interface.	Interface Configuration



## SSH Commands

Command Group	Description	Access Mode
ip ssh port	Specifies the port to be used by the SSH server.	Global Configuration
ip ssh server	Enables the device to be configured from a SSH server.	Global Configuration
crypto key generate dsa	Generates DSA key pairs.	Global Configuration
crypto key generate rsa	Generates RSA key pairs.	Global Configuration
ip ssh pubkey-auth	Enables public key authentication for incoming SSH sessions.	Global Configuration
crypto key pubkey-chain ssh	Enters SSH Public Key-chain Configuration mode.	Global Configuration
user-key	Specifies which SSH public key is manually configured and enters the SSH public key-string configuration command.	SSH Public Key
key-string	Manually specifies a SSH public key.	SSH Public Key
show ip ssh	Displays the SSH server configuration.	Privileged User EXEC
show crypto key mypubkey	Displays the SSH public keys stored on the device.	Privileged User EXEC
show crypto key pubkey-chain ssh	Displays SSH public keys stored on the device.	Privileged User EXEC

## Syslog Commands

Command Group	Description	Access Mode
logging on	Controls error messages logging.	Global Configuration
logging	Logs messages to a syslog server.	Global Configuration
logging console	Limits messages logged to the console based on severity.	Global Configuration
logging buffered	Limits syslog messages displayed from an internal buffer based on severity.	Global Configuration

logging buffered size	Changes the number of syslog messages stored in the internal buffer.	Global Configuration
clear logging	Clears messages from the internal logging buffer.	Privileged User EXEC
logging file	Limits syslog messages sent to the logging file based on severity.	Global Configuration
clear logging file	Clears messages from the logging file.	Privileged User EXEC
aaa logging	Controls logging of AAA events.	Global Configuration
file-system logging	Controls logging file system events.	Global Configuration
management logging	Controls logging of management access lists events.	Global Configuration
show logging	Displays the state of logging and the syslog messages stored in the internal buffer.	Privileged User EXEC
show logging file	Displays the state of logging and the syslog messages stored in the logging file.	Privileged User EXEC
show syslog-servers	Displays the syslog servers settings.	Privileged User EXEC

## System Management Commands

Command Group	Description	Access Mode
ping	Sends ICMP echo request packets to another node on the network.	User EXEC
tracert	Discovers the routes that packets will actually take when traveling to their destination.	User EXEC
telnet	Logs in to a host that supports Telnet.	User EXEC
resume	Switches to another open Telnet session	User EXEC
reload	Reloads the operating system	Privileged User EXEC
hostname	Specifies or modifies the device host name.	Global Configuration
service cpu-utilization	Allows the software to measure CPU utilization.	Global Configuration
show cpu utilization	Displays information about the active users.	User EXEC

show users	Lists the open Telnet sessions.	User EXEC
show sessions	Lists the open Telnet sessions	User EXEC
show system	Displays system information.	User EXEC
set system	Activates/deactivates specified features.	Privileged EXEC
show system mode	Displays information on features control	User EXEC
show version	Displays the system version information.	User EXEC
asset-tag	Specifies the device asset-tag.	Global Configuration
show system id	Displays the service ID information.	User EXEC

## TACACS Commands

Command Group	Description	Mode
tacacs-server host	Specifies a TACACS+ host.	Global Configuration
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon.	Global Configuration
tacacs-server source-ip	Specifies the source IP address that will be used for the communication with TACACS servers.	Global Configuration
show tacacs	Displays configuration and statistics for a TACACS+ servers.	Privileged User EXEC

## TIC Commands

Command Group	Description	Access Mode
The following example displays the local users configured with access to the system. passwords min-length	Configures the minimal length required for passwords in the local database.	Global Configuration
passwords aging	Configures the aging time of line passwords.	Line Configuration
passwords aging	Configures the aging time of username passwords and enables passwords.	Global Configuration
passwords history	Configures the number of password changes that are required before a password in the local database can be reused.	Global Configuration

passwords history hold-time	Configures the duration of time a password is relevant for tracking passwords history.	Global Configuration
passwords lockout	Enables lockout of a user account after a series of authentication failures.	Global Configuration
aaa login-history file	Enables writing to login history file.	Global Configuration
set username active	Reactivates a previously locked out user account.	Privileged EXEC
set line active	Reactivates a previously locked out line.	Privileged EXEC
set enable-password active	Reactivates a previously locked out password.	Privileged EXEC
show passwords configuration	Displays information about the passwords management configuration.	Privileged EXEC
show users login-history	Displays information about the login history of users.	Privileged EXEC

## Tunnel Commands

Command Group	Description	Access Mode
interface tunnel	Enters tunnel interface configuration mode.	Global Configuration
tunnel mode ipv6ip	Configures an IPv6 transition mechanism global support mode.	Interface Tunnel Configuration
tunnel isatap router	Configures a global string that represents a specific automatic tunnel router domain name.	Interface Tunnel Configuration
tunnel source	Sets the local (source) tunnel interface IPv4 address.	Interface Tunnel Configuration
tunnel isatap query-interval	Configures the interval between DNS Queries (before the IP address of the ISATAP router is known) for the automatic tunnel router domain name.	Global Configuration
tunnel isatap solicitation-interval	Configures the interval between ISATAP router solicitations messages (when there is no active ISATAP router).	Global Configuration
tunnel isatap robustness	Configures the number of DNS Query/Router Solicitation refresh messages that the device sends.	Global Configuration
show ipv6 tunnel	Displays information on the ISATAP tunnel.	Privileged EXEC

## User Interface Commands

Command Group	Description	Access Mode
enable	Enters the privileged EXEC mode.	All
disable	Returns to User EXEC mode.	All
login	Changes a login username.	All
configure	Enables the Global Configuration mode	All
exit(configuration)	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.	All
exit(EXEC)	Closes an active terminal session by logging off the device.	All
end	Ends the current configuration session and returns to the previous command mode.	All
help	Displays a brief description of the help system.	All
history	Enables the command history function.	All
terminal datadump	Enables dumping of all the output from the show command without 'prompting'.	Privileged EXEC
history size	Changes the command history buffer size for a particular line.	All
debug-mode	Switches the mode to debug.	All
show history	Lists the commands entered in the current session.	All
show privilege	Displays the current privilege level.	All
do	Executes a Global Configuration mode or any configuration submode.	All

## VLAN Commands

Command Group	Description	Access Mode
vlan database	Enters the VLAN Database Configuration mode.	Global Configuration
vlan	Creates a VLAN.	VLAN Configuration
interface vlan	Enters the Interface Configuration (VLAN) mode.	Global Configuration
interface range vlan	Enters the Interface Configuration mode to configure multiple VLANs.	Global Configuration
name	Configures a name to a VLAN.	Interface Configuration

switchport access vlan	Configures the VLAN membership mode of a port.	Interface Configuration
switchport access vlan	Configures the VLAN ID when the interface is in access mode.	Interface Configuration
switchport trunk allowed vlan	Adds or removes VLANs from a port in general mode.	Interface Configuration
switchport trunk native vlan	Defines the port as a member of the specified VLAN, and the VLAN ID is the "port default VLAN ID (PVID)".	Interface Configuration
switchport general allowed vlan	Adds or removes VLANs from a general port.	Interface Configuration
switchport general pvid	Configures the PVID when the interface is in general mode.	Interface Configuration
switchport general ingress-filtering disable	Disables port ingress filtering.	Interface Configuration
switchport general acceptable-frame-type tagged-only	Discards untagged frames at ingress.	Interface Configuration
switchport forbidden vlan	Forbids adding specific VLANs to a port.	Interface Configuration
map protocol protocols-group	Adds a special protocol to a named group of protocols, which may be used for protocol-based VLAN assignment.	VLAN Configuration
switchport general map protocols-group vlan	Sets a protocol-based classification rule.	Interface Configuration
ip internal-usage-vlan	Reserves a VLAN as the internal usage VLAN of an interface.	Interface Configuration
show vlan	Displays VLAN information.	Privileged User EXEC
show vlan internal usage	Displays a list of VLANs being used internally by the switch.	Privileged User EXEC
show vlan protocols-groups	Displays protocols-groups information.	Privileged User EXEC
show interfaces switchport	Displays switchport configuration.	Privileged User EXEC

## Voice VLAN Commands

<b>Command Group</b>	<b>Description</b>	<b>Access Mode</b>
voice vlan id	Enters the VLAN Configuration mode.	Global Configuration
voice vlan oui-table	Configure the Voice OUI table.	Global Configuration
voice vlan cos	Sets the Voice VLAN Class Of Service.	Global Configuration
voice vlan aging-timeout	Sets the Voice VLAN aging timeout.	Global Configuration
voice vlan enable	Enables automatic Voice VLAN configuration for a port.	Interface Configuration (Ethernet, port-channel)
voice vlan secure	Configures the secure mode for the Voice VLAN.	Interface Configuration (Ethernet, port-channel)
show voice vlan	Displays the Voice VLAN status.	EXEC

## Web Server Commands

<b>Command Group</b>	<b>Description</b>	<b>Access Mode</b>
ip http server	Enables the device to be configured from a browser.	Global Configuration
ip http port	Specifies the TCP port for use by a web browser to configure the device.	Global Configuration
ip https exec-timeout	Sets the interval the system waits for user input before automatically logging off.	Global Configuration
ip https server	Enables the device to be configured from a secured browser.	Global Configuration
ip https port	Configures a TCP port for use by a secure web browser to configure the device.	Global Configuration
ip https exec-timeout	Sets the interval the system waits for user input before automatically logging off.	Global Configuration
crypto certificate generate	Generates a HTTPS certificate.	Global Configuration

crypto certificate import	Imports a certificate signed by Certification Authority for HTTPS.	Global Configuration
ip https certificate	Configures the active certificate for HTTPS.	Global Configuration
ip https port	Configures a TCP port for use by a secure web browser to configure the device.	Global Configuration
ip http exec-timeout	Sets the interval the system waits for user input before automatically logging off.	Global Configuration
ip https server	Enables the device to be configured from a secured browser.	Global Configuration
crypto certificate request	Generates and displays certificate requests for HTTPS.	Privileged EXEC
crypto certificate import	Imports a certificate signed by Certification Authority for HTTPS.	Global Configuration
ip https certificate	Configures the active certificate for HTTPS.	Global Configuration
crypto certificate import pkcs12	Exports the certificate and the RSA keys within a PKCS12 file	Privileged User EXEC
crypto certificate import pkcs12	Imports the certificate and the RSA keys within a PKCS12 file	Privileged User EXEC
show crypto certificate mycertificate	Displays the SSL certificates of the device	Privileged User EXEC
show ip http	Displays the HTTP server configuration.	Privileged User EXEC
show ip https	Displays the HTTPS server configuration.	Privileged User EXEC

## 802.1x Commands

Command	Description	Access Mode
aaa authentication dot1x	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X.	Global Configuration
dot1x system-auth-control	Enables 802.1x globally.	Global Configuration
dot1x port-control	Enables manual control of the authorization state of the port	Interface Configuration
dot1x re-authentication	Enables periodic re-authentication of the client.	Interface Configuration



dot1x timeout re-authperiod	Sets the number of seconds between re-authentication attempts.	Interface Configuration
dot1x re-authenticate	Manually initiates a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.	Privileged User EXEC
dot1x timeout quiet-period	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange.	Interface Configuration
dot1x timeout tx-period	Sets the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP) - request/identity frame, from the client, before resending the request.	Interface Configuration
dot1x max-req	Sets the maximum number of times that the switch sends an EAP - request/identity frame to the client, before restarting the authentication process.	Interface Configuration
dot1x timeout supp-timeout	Sets the time for the retransmission of an Extensible Authentication Protocol (EAP)-request frame to the client.	Interface Configuration
dot1x timeout server-timeout	Sets the time for the retransmission of packets to the authentication server.	Interface Configuration
show dot1x	Allows multiple hosts on an 802.1X-authorized port, that has the <b>dot1x port-control</b> interface configuration command set to <b>auto</b> .	Interface Configuration
show dot1x users	Displays 802.1X statistics for the specified interface.	Privileged User EXEC
show dot1x statistics	Displays 802.1X statistics for the specified interface.	Privileged User EXEC

## 802.1x Advanced Commands

dot1x auth-not-req	Enables unauthorized users access to that VLAN.	VLAN Configuration
dot1x multiple-hosts	Allows multiple hosts (clients) on an 802.1X-authorized port with the dot1x port-control Interface Configuration mode command set to auto.	Interface Configuration (Ethernet)
dot1x single-host-violation	Configures the action to be taken when a station of which the MAC address is not the supplicant MAC address attempts to access the interface.	Interface Configuration (Ethernet)
dot1x guest-vlan	Defines a Guest VLAN. Use the no form of this command to return to default.	Interface Configuration (VLAN)
dot1x guest-vlan enable	Enables unauthorized users on the interface access to the Guest VLAN.	Interface Configuration (Ethernet)
dot1x mac-authentication	Enables authentication based on the station's MAC address.	Interface Configuration
dot1x traps mac-authentication failure	Enables sending traps when a MAC address was failed in authentication of the 802.1X MAC authentication access control.	Global Configuration
dot1x radius-attributes vlan	Enables user-based VLAN assignment.	Interface Configuration
show dot1x advanced	Displays 802.1X advanced features for the switch or for the specified interface.	Privileged EXEC

# Command Modes

## GC (Global Configuration) Mode

Command	Description
aaa authentication enable	Defines authentication method lists for accessing higher privilege levels.
aaa authentication login	Defines login authentication.
aaa authentication dot1x	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X.
arp	Adds a permanent entry in the ARP cache.
arp timeout	Configures how long an entry remains in the ARP cache
asset-tag	Specifies the device asset-tag.
banner exec	Specifies and enables a message to be displayed when an EXEC process is created.
banner login	Enables a message to be displayed before the username and password login prompts.
banner motd	Specifies and enables a message-of-the-day banner.
bridge aging-time	Sets the address table aging time.
bridge multicast filtering	Enables filtering of Multicast addresses.
clock source	Configures an external time source for the system clock.
bridge multicast unregistered	Configures the forwarding state of unregistered multicast addresses.
clock timezone	Sets the time zone for display purposes
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).
crypto certificate generate	Generates a HTTPS certificate.
crypto certificate import	Imports a certificate signed by Certification Authority for HTTPS.
crypto key generate dsa	Generates DSA key pairs.
crypto key generate rsa	Generates RSA key pairs.
crypto key pubkey-chain ssh	Enters SSH Public Key-chain configuration mode.

dot1x system-auth-control	Enables 802.1x globally.
enable password	Sets a local password to control access to normal and privilege levels.
end	Ends the current configuration session and returns to the previous command mode.
gvrp enable (global)	Enables GVRP globally.
hostname	Specifies or modifies the device host name.
interface ethernet	Enters the Interface Configuration mode to configure an Ethernet type interface.
show interfaces port-channel	Enters the Interface Configuration mode of a specific port-channel.
interface ethernet	Enters the Interface Configuration mode to configure multiple ethernet type interfaces.
interface range port-channel	Enters the Interface Configuration mode to configure multiple port-channels.
interface range vlan	Enters the Interface Configuration mode to configure multiple VLANs.
interface tunnel	Enters tunnel interface configuration mode.
interface vlan	Enters the Interface Configuration (VLAN) mode.
ip default-gateway	Defines a default gateway.
ip domain-lookup	Enables the IP Domain Naming System (DNS)-based host name-to-address translation.
ip domain-name	Defines a default domain name, that the software uses to complete unqualified host names.
ip host	Defines static host name-to-address mapping in the host cache.
ip http authentication	Specifies authentication methods for http.
ip http port	Specifies the TCP port for use by a web browser to configure the device.
ip https server	Enables the device to be configured from a browser.
ip https authentication	Specifies authentication methods for https
ip https certificate	Configures the active certificate for HTTPS. Use the <b>no</b> form of this command to return to default.
ip https server	Enables the device to be configured from a secured browser.
ip https port	Configures a TCP port for use by a secure web browser to configure the device.
ip igmp snooping (Global)	Enables Internet Group Management Protocol (IGMP) snooping
ip name-server	Sets the available name servers.
ip ssh port	Specifies the port to be used by the SSH server.
ip ssh pubkey-auth	Enables public key authentication for incoming SSH sessions.

ip ssh server	Enables the device to be configured from a SSH server.
ipv6 default-gateway	Defines an IPv6 default gateway.
ipv6 host	Defines a static host name-to-address mapping in the host name cache.
ipv6 icmp error-interval	Configures the rate limit interval and bucket size parameters for IPv6 ICMP error messages.
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache.
lACP system-priority	Configures the system LACP priority.
line	Identifies a specific line for configuration and enters the Line Configuration command mode.
logging	Logs messages to a syslog server.
logging buffered	Limits syslog messages displayed from an internal buffer based on severity.
logging buffered size	Changes the number of syslog messages stored in the internal buffer.
logging console	Limits messages logged to the console based on severity.
The following example clears messages from the internal syslog message logging buffer.	Limits syslog messages sent to the logging file based on severity.
logging on	Controls error messages logging.
login authentication	Specifies the login authentication method list for a remote telnet or console.
management access-class	Defines which management Access-List is used.
management access-list	Defines a management Access-List, and enters the Access-List for configuration.
port jumbo-frame	Enables jumbo frames for the device.
port storm-control include-multicast	Enables the device to count Multicast packets.
priority-queue out num-of-queues	Enables the egress queues to be expedite queues.
qos	Enables quality of service (QoS) on the device and enters QoS basic or advance mode.
qos map dscp-queue	Modifies the DSCP to CoS map.
qos trust (Global)	Configure the system to "trust" state.
radius-server deadtime	Improves RADIUS response times when servers are unavailable.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

radius-server retransmit	Specifies the number of times the software searches the list of RADIUS server hosts.
radius-server source-ip	Specifies the source IP address used for communication with RADIUS servers.
radius-server source-ipv6	Specifies the source IPv6 address used for the IPv6 communication with RADIUS servers.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.
rmon alarm	Configures alarm conditions.
rmon event	Configures a RMON event.
rmon table-size	Configures the maximum RMON tables sizes.
snmp-server community	Sets up the community access string to permit access to SNMP protocol.
snmp-server contact	Sets up a system contact.
snmp-server enable traps	Enables the switch to send SNMP traps or SNMP notifications.
snmp-server host	Specifies the recipient of Simple Network Management Protocol notification operation.
snmp-server location	Sets up the information on where the device is located.
snmp-server set	Sets SNMP MIB value by the CLI.
snmp-server trap authentication	Enables the switch to send Simple Network Management Protocol traps when authentication failed.
sntp authenticate	Grants authentication for received Network Time Protocol (NTP) traffic from servers.
sntp authentication-key	Defines an authentication key for Simple Network Time Protocol (SNTP).
spanning-tree	Enables spanning tree functionality.
spanning-tree bpdud	Defines BPDU handling when spanning tree is disabled on an interface
spanning-tree forward-time	Configures the spanning tree bridge forward time.
spanning-tree hello-time	Configures the spanning tree bridge Hello Time.
spanning-tree max-age	Configures the spanning tree bridge maximum age.
spanning-tree mode	Configures the spanning tree protocol.
spanning-tree pathcost method	Sets the default pathcost method.
spanning-tree priority	Configures the spanning tree priority.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon.

tacacs-server source-ip	Specifies the source IP address that will be used for the communication with TACACS servers.
tacacs-server timeout	Sets the timeout value.
tacacs-server host	Specifies a TACACS+ host.
tunnel isatap query-interval	Configures the interval between DNS Queries (before the IP address of the ISATAP router is known) for the automatic tunnel router domain name.
tunnel isatap robustness	Configures the number of DNS Query/Router Solicitation refresh messages that the device sends.
tunnel isatap solicitation-interval	Configures the interval between ISATAP router solicitations messages (when there is no active ISATAP router).
username	Establishes a username-based authentication system.
vlan database	Enters the VLAN Database Configuration mode.
wrr-queue cos-map	Maps assigned CoS values to select one of the egress queues.

## IC (Interface Configuration) Mode

Command	Description
back-pressure	Enables Back Pressure on a given interface.
channel-group	Associates a port with a Port-channel.
clear host dhcp	Sets an IP address on the device.
description	Adds a description to an interface.
dot1x auth-not-req	Enables unauthorized users access to that VLAN
dot1x guest-vlan	Defines a Guest VLAN.
dot1x guest-vlan enable	Enables unauthorized users on the interface an access to the Guest VLAN.
dot1x mac-authentication	Enables authentication based on the station's MAC address.
dot1x radius-attributes vlan	Enables user-based VLAN assignment.
dot1x traps mac-authentication failure	Enables sending traps when a MAC address was failed in authentication of the 802.1X MAC authentication access control.
dot1x max-req	Sets the maximum number of times that the switch sends an EAP - request/identity frame to the client, before restarting the authentication process.
dot1x port-control	Enables manual control of the authorization state of the port
dot1x re-authentication	Enables periodic re-authentication of the client.

dot1x single-host-violation	Configures the action to be taken, when a station whose MAC address is not the supplicant MAC address, attempts to access the interface.
dot1x timeout quiet-period	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange.
dot1x timeout re-authperiod	Sets the number of seconds between re-authentication attempts.
dot1x timeout server-timeout	Sets the time for the retransmission of packets to the authentication server
dot1x timeout supp-timeout	Sets the time for the retransmission of an EAP-request frame to the client.
dot1x timeout tx-period	Sets the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP) - request/identity frame, from the client, before resending the request.
duplex	Configures the full/half duplex operation of a given ethernet interface when not using auto-negotiation.
flowcontrol	Configures the Flow Control on a given interface.
garp timer	Adjusts the GARP application join, leave, and leaveall GARP timer values.
gvrp enable (interface)	Enables GVRP on an interface.
gvrp registration-forbid	De-registers all VLANs, and prevents dynamic VLAN registration on the port.
gvrp vlan-creation-forbid	Enables or disables dynamic VLAN creation.
ip address	Sets an IP address
ip address dhcp	Acquires an IP address on an interface from the DHCP server.
ip internal-usage-vlan	Reserves a VLAN as the internal usage VLAN of an interface.
ipv6 address	Configures an IPv6 address for an interface.
ipv6 address autoconfig	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface.
ipv6 address link-local	Configures an IPv6 link-local address for an interface.
ipv6 mld join-group	Configures Multicast Listener Discovery (MLD) reporting for a specified group.
ipv6 mld version	Changes the Multicast Listener Discovery Protocol (MLD) version.
ipv6 nd dad attempts	Configures the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the unicast IPv6 addresses of the interface.
ipv6 enable	Enables IPv6 processing on an interface.
ipv6 unreachable	Enables the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface.
lacp port-priority	Configures the priority value for physical ports.
lacp timeout	Assigns an administrative LACP timeout.



mdix	Enables automatic crossover on a given interface.
name	Configures a name to a VLAN.
negotiation	Enables auto-negotiation operation for the speed and duplex parameters of a given interface.
port monitor	Starts a port monitoring session.
port security	Disables new address learning on an interface.
port security routed secure-address	Adds MAC-layer secure addresses to a routed port.
port storm-control broadcast enable	Enables Broadcast storm control.
port storm-control broadcast rate	Configures the maximum Broadcast rate.
qos cos	Configures the default port CoS value.
qos trust (Interface)	Enables each port trust state while the system is in basic mode.
rmon collection history	Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.
shutdown	Disables interfaces.
snmp client enable (interface)	Enables the Simple Network Time Protocol (SNTP) client on an interface.
spanning-tree cost	Configures the spanning tree path cost for a port.
spanning-tree disable	Disables spanning tree on a specific port.
spanning-tree link-type	Overrides the default link-type setting.
spanning-tree portfast	Enables PortFast mode.
spanning-tree port-priority	Configures port priority.
speed	Configures the speed of a given ethernet interface when not using auto-negotiation.
system flowcontrol	Enables flow control on cascade ports.
tunnel isatap router	Configures a global string that represents a specific automatic tunnel router domain name.
tunnel mode ipv6ip	Configures an IPv6 transition mechanism global support mode.
tunnel source	Sets the local (source) tunnel interface IPv4 address.
qos map dscp-queue	Defines the wrr-queue mechanism on an egress queue.
wrr-queue bandwidth	Assigns Weighted Round Robin (WRR) weights to egress queues.

## LC (Line Configuration) Mode

Command	Description
enable authentication	Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console.
exec-banner	Enables the display of exec banners.
exec-timeout	Configures the interval that the system waits until user input is detected.
history	Enables the command history function.
history size	Changes the command history buffer size for a particular line.
login-banner	Enables the display of login banners.
motd-banner	Enables the display of message-of-the-day banners.
password	Specifies a password on a line.
autobaud	Sets the line for automatic baud rate detection
speed	Sets the line baud rate.

## MA (Management Access-level) Mode

Command	Description
deny (management)	Defines a deny rule.
permit (management)	Defines a permit rule.

## PE (Privileged User EXEC) Mode

Command	Description
boot system	Specifies the system image that the device loads at startup.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
clear bridge	Removes any learned entries from the forwarding database.
clear gvrp statistics	Clears all the GVRP statistics information.
clear host	Deletes entries from the host name-to-address cache
clear host dhcp	Deletes entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
clear logging	Clears messages from the internal logging buffer.

clear logging file	Clears messages from the logging file
clear spanning-tree detected-protocols	Restarts the protocol migration process on all interfaces or on the specified interface.
clock set	Manually sets the system clock.
configure	Enters the global configuration mode.
copy	Copies files from a source to a destination.
crypto certificate request	Generates and displays certificate requests for HTTPS.
dot1x re-authenticate	Manually initiates a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.
ipv6 set mtu	Sets the MTU size of IPv6 packets sent on an interface.
login	Returns to User EXEC mode.
reload	Reloads the operating system.
set interface active	Reactivates an interface that was suspended by the system.
set system	Activates/deactivates specified features.
show arp	Displays entries in the ARP table.
show authentication methods	Displays information about the authentication methods.
show banner	Displays the banners configuration.
show bootvar	Displays the active system image file that the device loads at startup
show bridge address-table	Displays dynamically created entries in the bridge-forwarding database.
show bridge address-table count	Displays the number of addresses present in all VLANs or at specific VLAN.
show bridge multicast address-table	Displays Multicast MAC address table information.
show bridge multicast filtering	Displays the Multicast filtering configuration.
show copper-ports cable-length	Displays the estimated copper cable length attached to a port.
show copper-ports tdr	Displays the last TDR (Time Domain Reflectometry) tests on specified ports.
show crypto key mypubkey	Displays the SSH public keys stored on the device.
show crypto key pubkey-chain ssh	Displays SSH public keys stored on the device.
show crypto certificate mycertificate	Displays the SSL certificates of the device
show dot1x	Displays allowed multiple hosts on an 802.1X-authorized port, that has the dot1x port-control Interface Configuration command set to auto.
show dot1x advanced	Displays 802.1X enhanced features for the switch or for the specified interface.
show dot1x users	Displays 802.1X statistics for a specified interface.

show fiber-ports optical-transceiver	Displays the optical transceiver diagnostics.
show ip ssh	Displays the SSH server configuration.
show ipv6 icmp error-interval	Displays the IPv6 ICMP error interval setting
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
show ipv6 neighbors	Displays IPv6 neighbor discovery cache information.
show ipv6 route	Displays the current state of the IPv6 routing table.
show ipv6 tunnel	Displays information on the ISATAP tunnel.
show lacp port-channel	Displays LACP information for a port-channel.
show logging	Displays the state of logging and the syslog messages stored in the internal buffer.
show logging file	Displays the state of logging and the syslog messages stored in the logging file.
show management access-class	Displays the active management Access-List.
show management access-list	Displays management access-lists.
show ports security	Displays the port-lock status.
show ports storm-control	Displays the storm control configuration.
show radius-servers	Displays the RADIUS server settings.
show running-config	Displays the contents of the currently running configuration file.
show snmp	Displays the SNMP status.
show spanning-tree	Displays spanning tree configuration.
show startup-config	Displays the startup configuration file contents.
show syslog-servers	Displays the syslog servers settings.
show system flowcontrol	Displays the flow control state on cascade ports.
show tacacs	Displays configuration and statistics for a TACACS+ servers.
show users accounts	Displays information about the local user database.
test copper-port tdr	Diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.

## SP (SSH Public Key) Mode

Command	Description
key-string	Manually specifies a SSH public key.
user-key	Specifies which SSH public key is manually configured and enters the SSH public key-string configuration command

## UE (User EXEC) Mode

Command	Description
clear counters	Clears statistics on an interface.
enable	Enters the privileged EXEC mode.
exit(EXEC)	Closes an active terminal session by logging off the device.
login	Changes a login username.
ping	Sends ICMP echo request packets to another node on the network.
show clock	Displays the time and date from the system clock.
show gvrp configuration	Displays GVRP configuration information.
clear gvrp statistics	Displays GVRP statistics.
show history	Lists the commands entered in the current session.
show hosts	Displays the default domain name, a list of name server hosts, the static and the cached list of host names and addresses.
show interfaces configuration	Displays the configuration for all configured interfaces.
show interfaces counters	Displays traffic seen by the physical interface.
show interfaces description	Displays the description for all configured interfaces.
port-channel load-balance	Displays Port-channel information.
show interfaces status	Displays the status for all configured interfaces.
show ip igmp snooping groups	Displays Multicast groups learned by IGMP snooping.
show ip igmp snooping interface	Displays IGMP snooping configuration.
show ip igmp snooping mrouter	Displays information on dynamically learned Multicast router interfaces.
show ip interface	Displays the usability status of interfaces configured for IP.
show lacp ethernet	Displays LACP information for Ethernet ports.
show line	Displays line parameters.
show ports jumbo-frame	Displays the jumbo frames configuration.
show ports monitor	Displays the port monitoring status.
show privilege	Displays the current privilege level.
show qos	Displays the QoS status.
show qos interface	Assigns CoS values to select one of the egress queues.
show qos map	Displays all the maps for QoS.
show rmon alarm	Displays alarm configurations.

show rmon alarm-table	Displays the alarms summary table.
show rmon collection history	Displays the requested history group configuration.
show rmon events	Displays the RMON event table.
show rmon history	Displays RMON Ethernet Statistics history.
show rmon log	Displays the RMON logging table.
show rmon statistics	Displays RMON Ethernet Statistics.
show system	Displays system information.
show system id	Displays the service id information.
show system mode	Displays information on features control
service cpu-utilization	Displays information about the active users.
show version	Displays the system version information.

## VC (VLAN Configuration) Mode

Command	Description
bridge address	Adds a static MAC-layer station source address to the bridge table.
bridge multicast address	Registers MAC-layer Multicast addresses to the bridge table, and adds static ports to the group.
bridge multicast forbidden address	Forbids adding a specific Multicast address to specific ports.
bridge multicast forbidden forward-all	Enables forbidding forwarding of all Multicast frames to a port.
bridge multicast forward-all	Enables forwarding of all Multicast frames on a port.
ip igmp snooping (Interface)	Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN.
ip igmp snooping leave-time-out	Configures the host-time-out.
show ip igmp snooping mrouter	Enables automatic learning of Multicast router ports in the context of a specific VLAN.
ip igmp snooping mrouter-time-out	Configures the mrouter-time-out.
vlan	Creates a VLAN.

# ACL Commands

## ip access-list

The `ip access-list` Global Configuration mode command defines an IPv4 Access List and places the device in IPv4 Access List Configuration mode. Use the `no` form of this command to remove the Access List.

### Syntax

- `ip access-list access-list-name`
- `no ip access-list access-list-name`
  - *access-list-name* — Specifies the name of the IPv4 Access-List.

### Default Configuration

No IPv4 Access List is defined.

### Command Mode

Global Configuration mode.

### User Guidelines

- IPv4 ACLs are defined by a unique name. An IPv4 ACL and MAC ACL cannot share the same name.

### Example

The following example shows how to define an IPv4 Access List called `dell-access-1` and to place the device in IPv4 Access List Configuration mode.

```
Console(config)# ip access-list dell-access-1
Console(config-ip-acl)#
```

## mac access-list

The `mac access-list` Global Configuration mode command enables the MAC-Access List Configuration mode and creates Layer 2 ACLs. Use the `no` form of this command to delete an ACL.

## Syntax

- `mac access-list name`
- `no mac access-list name`
  - *access-list-name* — Name of the MAC Access List.

## Default Configuration

No MAC Access List is defined.

## Command Mode

Global Configuration mode.

## User Guidelines

- MAC ACLs are defined by a unique name. An IPv4 ACL, IPv6 ACL and MAC ACL cannot share the same name.

## Example

The following example shows how to create a MAC ACL.

```
Console(config)# mac access-list mac1-acl1
Console(config-mac-al)#
```

## permit (ip)

The `permit` IP-Access List Configuration mode command permits traffic if the conditions defined in the permit statement match.

## Syntax

- `permit {any | protocol} {any | {source source-wildcard}} {any | {destination destination-wildcard}} [dscp number | ip-precedence number]`
- `permit-icmp {any | {source source-wildcard}} {any | {destination destination-wildcard}} {any | icmp-type} {any | icmp-code} [dscp number | ip-precedence number]`
- `permit-igmp {any | {source source-wildcard}} {any | {destination destination-wildcard}} {any | igmp-type} [dscp number | ip-precedence number]`



- **permit-tcp** {any|{ *source source-wildcard*}} {any|*source-port*} {any|{ **destination destination-wildcard**}} {any|*destination-port*} [**dscp number** | **ip-precedence number**] [**flags list-of-flags**] [**src-port-wildcard source-port-wildcard**] [**dst-port-wildcard source-port-wildcard**]
- **permit-udp** {any|{ *source source-wildcard*}} {any| *source-port*} {any| {*destination destination-wildcard*}} {any|*destination-port*} [**dscp number** | **ip-precedence number**] [**src-port-wildcard source-port-wildcard**] [**dst-port-wildcard source-port-wildcard**]
  - *source* — Specifies the source IP address of the packet.
  - *source-wildcard* — Specifies wildcard bits to be applied to the sources IP address by placing 1s in bit positions to be ignored.
  - *destination* — Specifies the destination IP address of the packet.
  - *destination-wildcard* — Specifies wildcard bits to be applied to the destination IP address by placing 1s in bit positions to be ignored.
  - *protocol* — Specifies the name or the number of an IP protocol. Available protocol names: **icmp**, **igmp**, **ip**, **tcp**, **egp**, **igp**, **udp**, **hmp**, **rdp**, **idpr**, **idrp**, **rsvp**, **gre**, **esp**, **ah**, **eigrp**, **ospf**, **ipip**, **pim**, **l2tp**, **isis**. (Range: 0 - 255)
  - **dscp number** — Specifies the DSCP value.
  - **ip-precedence number** — Specifies the IP precedence value.
  - *icmp-type* — Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: **echo-reply**, **destination-unreachable**, **source-quench**, **redirect**, **alternate-host-address**, **echo-request**, **router-advertisement**, **router-solicitation**, **time-exceeded**, **parameter-problem**, **timestamp**, **timestamp-reply**, **information-request**, **information-reply**, **address-mask-request**, **address-mask-reply**, **traceroute**, **datagram-conversion-error**, **mobile-host-redirect**, **mobile-registration-request**, **mobile-registration-reply**, **domain-name-request**, **domain-name-reply**, **skip**, **photuris**. (Range: 0 - 255)
  - *icmp-code* — Specifies an ICMP message code for filtering ICMP packets. (Range: 0 - 255)
  - *igmp-type* — Specifies IGMP packets filtered by IGMP message type. Enter a number or one of the following values: **host-query**, **host-report**, **dvmrp**, **pim**, **cisco-trace**, **host-report-v2**, **host-leave-v2**, **host-report-v3**. (Range: 0 - 255)
  - *destination-port* — Specifies the UDP/TCP destination port. (Range: 0 - 65535)
  - *destination-port-wildcard* — Specifies wildcard bits to be applied to the destination port by placing 1s in bit positions to be ignored.
  - *source-port* — Specifies the UDP/TCP source port. (Range: 0 - 65535)
  - *source-port-wildcard* — Specifies wildcard bits to be applied to the source port by placing 1s in bit positions to be ignored.
  - **flags list-of-flags** — Specifies the list of TCP flags. If a flag is set, it is prefixed by "+". If a flag is not set, it is prefixed by "-". Available options are **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** and **-fin**. The flags are concatenated to a one string. For example: **+fin-ack**.
  - **byte** — Specifies the user-defined bytes.

## Default Configuration

No IPv4 ACL is defined.

## Command Mode

IP-Access List Configuration mode.

## User Guidelines

- Use the **ip access-list** Global Configuration mode command to enable the IP-Access List Configuration mode.
- Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

## Example

The following example shows how to define a permit statement for an IP ACL.

```
Console(config)# ip access-list ip-acl1
Console(config-ip-acl)# permit rsvp 192.1.1.1 0.0.0.0 any dscp 56
```

## deny (IP)

The **deny** IP-Access List Configuration mode command denies traffic if the conditions defined in the deny statement match.

## Syntax

- **deny** [**disable-port**] {**any** | *protocol*} {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} [**dscp number** | **ip-precedence number**]
- **deny-icmp** [**disable-port**] {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} {**any** | *icmp-type*} {**any** | *icmp-code*} [**dscp number** | **ip-precedence number**]
- **deny-igmp** [**disable-port**] {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} {**any** | *igmp-type*} [**dscp number** | **ip-precedence number**]
- **deny-tcp** [**disable-port**] {**any** | {*source source-wildcard*}} {**any** | *source-port*} {**any** | {*destination destination-wildcard*}} {**any** | *destination-port*} [**dscp number** | **ip-precedence number**] [**flags list-of-flags**] [**src-port-wildcard source-port-wildcard**] [**dst-port-wildcard source-port-wildcard**]
- **deny-udp** [**disable-port**] {**any** | {*source source-wildcard*}} {**any** | *source-port*} {**any** | {*destination destination-wildcard*}} {**any** | *destination-port*} [**dscp number** | **ip-precedence number**] [**src-port-wildcard source-port-wildcard**] [**dst-port-wildcard source-port-wildcard**]

- **disable-port** — Specifies that the Ethernet interface is disabled if the condition is matched.
  - *source* — Specifies the Source IP address of the packet.
  - *source-wildcard* — Specifies wildcard bits to be applied to the source IP address by placing 1s in bit positions to be ignored.
  - *destination* — Specifies the destination IP address of the packet.
  - *destination-wildcard* — Specifies wildcard bits to be applied to the destination IP address by placing 1s in bit positions to be ignored.
  - *protocol* — Specifies the name or the number of an IP protocol. Available protocol names: **icmp**, **igmp**, **ip**, **tcp**, **egp**, **igp**, **udp**, **hmp**, **rdp**, **idpr**, **idrp**, **rsvp**, **gre**, **esp**, **ah**, **eigrp**, **ospf**, **ipip**, **pim**, **l2tp**, **isis**. (Range: 0 - 255).
- **dscp number** — Specifies the DSCP value.
- **ip-precedence number** — Specifies the IP precedence value.
  - *icmp-type* — Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: **echo-reply**, **destination-unreachable**, **source-quench**, **redirect**, **alternate-host-address**, **echo-request**, **router-advertisement**, **router-solicitation**, **time-exceeded**, **parameter-problem**, **timestamp**, **timestamp-reply**, **information-request**, **information-reply**, **address-mask-request**, **address-mask-reply**, **traceroute**, **datagram-conversion-error**, **mobile-host-redirect**, **mobile-registration-request**, **mobile-registration-reply**, **domain-name-request**, **domain-name-reply**, **skip**, **photuris**.
  - *icmp-code* — Specifies an ICMP message code for filtering ICMP packets. (Range: 0 - 255)
  - *igmp-type* — Specifies IGMP packets filtered by IGMP message type. Enter a number or one of the following values: **host-query**, **host-report**, **dvmp**, **pim**, **cisco-trace**, **host-report-v2**, **host-leave-v2**, **host-report-v3**. (Range: 0 - 255)
  - *destination-port* — Specifies the UDP/TCP destination port. (Range: 0 - 65535)
  - *destination-port-wildcard* — Specifies wildcard bits to be applied to the destination port by placing 1s in bit positions to be ignored.
  - *source-port* — Specifies the UDP/TCP source port. (Range: 0 - 65535)
  - *source-port-wildcard* — Specifies wildcard bits to be applied to the source port by placing 1s in bit positions to be ignored.
- **flags list-of-flags** — Specifies the list of TCP flags. If a flag should be set it is prefixed by "+". If a flag is not set, it is prefixed by "-". Available options are **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** and **-fin**. The flags are concatenated to a one string. For example: **+fin-ack**.

### Default Configuration

No IPv4 Access List is defined.

### Command Mode

IP-Access List Configuration mode.

## User Guidelines

- Use the **ip access-list** Global Configuration mode command to enable the IP-Access List Configuration mode.
- Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the defined conditions are denied.

## Example

The following example shows how to define a permit statement for an IP ACL.

```
Console(config)# ip access-list ip-acl1
Console(config-ip-acl)# deny rsvp 192.1.1.1 0.0.0.255 any
```

## permit (MAC)

The **permit** MAC-Access List Configuration mode command defines permit conditions of an MAC ACL.

### Syntax

- **permit** {**any** | {**host** *source source-wildcard*} **any** | {*destination destination-wildcard*}} [**vlan** *vlan-id*] [**cos** *cos cos-wildcard*] [**eth-type** *eth-type*] [**inner-vlan** *vlan-id*]
  - *source* — Specifies the source MAC address of the packet.
  - *source-wildcard* — Specifies wildcard bits to be applied to the source MAC address by placing 1s in bit positions to be ignored.
  - **any** — Specify a MAC address and mask. For example, to set 00:00:00:00:10:XX use the Mac address 00:00:00:00:10:00 and mask 00:00:00:00:00:FF.
  - *destination* — Specifies the MAC address of the host to which the packet is being sent.
  - *destination-wildcard* — Specifies wildcard bits to be applied to the destination MAC address by placing 1s in bit positions to be ignored.
  - *vlan-id* — Specifies the ID of the packet vlan. (Range: 1 - 4094)
  - *cos* — Specifies the Class of Service (CoS) for the packet. (Range: 0 - 7)
  - *cos-wildcard* — Specifies wildcard bits to be applied to the CoS.
  - *eth-type* — Specifies the Ethernet type of the packet in hexadecimal format. (Range: 0 - 05dd-ffff)
  - **inner-vlan** *vlan-id* — Specifies the inner vlan id of a double tagged packet.

## Default Configuration

No MAC ACL is defined.

## Command Mode

MAC-Access List Configuration mode.

## User Guidelines

- Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.
- If the VLAN ID is specified, the policy map cannot be connected to the VLAN interface.

## Example

The following example shows how to create a MAC ACL with permit rules.

```
Console(config)# mac access-list macl-acl1
Console(config-mac-acl)# permit 6:6:6:6:6:6 0:0:0:0:0:0 any vlan 6
```

## deny (MAC)

The **deny** MAC-Access List Configuration mode command denies traffic if the conditions defined in the deny statement match.

## Syntax

- **deny** [**disable-port**] {**any** | {*source source-wildcard*} {**any** | {*destination destination-wildcard*}} [**vlan vlan-id**] [**cos cos cos-wildcard**] [**eth-type eth-type**] [**inner-vlan vlan-id**]
  - **disable-port** — Indicates that the port is disabled if the condition is matched.
  - *source* — Specifies the MAC address of the host from which the packet was sent.
  - *source-wildcard* — Specifies wildcard bits to the source MAC address by placing 1s in bit positions to be ignored.
  - **any** — Specify a MAC address and mask. For example, to set 00:00:00:00:10:XX use the Mac address 00:00:00:00:10:00 and mask 00:00:00:00:00:FF.
  - *destination* — Specifies the MAC address of the host to which the packet is being sent.
  - *destination-wildcard* — Specifies wildcard bits to the destination MAC address by placing 1s in bit positions to be ignored.
  - *vlan-id* — Specifies the vlan id of the packet. (Range: 1 - 4094)

- *cos* — Specifies the packets's Class of Service (CoS). (Range: 0 - 7)
- *cos-wildcard* — Specifies wildcard bits to be applied to the CoS.
- *eth-type* — Specifies the packet's Ethernet type in hexadecimal format. (Range: 0 - 05dd-ffff)
- *inner-vlan vlan id* — Specifies the inner vlan id of a double tagged packet.

### Default Configuration

No MAC Access List is defined.

### Command Mode

MAC-Access List Configuration mode.

### User Guidelines

- The MAC ACL Global Configuration command allows access to the IP-Access List Configuration mode.
- Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

### Example

The following example shows how to create a MAC ACL with deny rules on a device.

```
Console(config)# mac access-list mac11
Console (config-mac-acl)# deny 6:6:6:6:6:6:0:0:0:0:0:0 any
```

## service-acl

The **service-acl** Interface Configuration (Ethernet, port-channel) mode command applies an ACL to the input interface. Use the **no** form of this command to detach an ACL from an input interface.

### Syntax

- **service-acl** {input *acl-name* | *acl-name*}
- **no service-acl** {input}
  - **input** — Applies the specified ACL to the input interface.

### Default Configuration

This command has no default configuration.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

There are no user guidelines for this command.

### Example

The following example binds (services) an ACL to VLAN 2.

```
Console(config)# interface eth g1
Console(config-if)# service-acl input mac11
```

## show access-lists

The `show access-lists` Privileged EXEC mode command displays access control lists (ACLs) defined on the device.

### Syntax

- `show access-lists [name]`
  - *name* — The name of the ACL.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

There are no user guidelines for this command.

### Example

The following example displays access lists defined on a device.

```
Console# show access-lists
IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8 0.0.0.0 any
```

## show interfaces access-lists

The `show interfaces access-lists` Privileged EXEC mode command displays access lists applied on interfaces.

### Syntax

- `show interfaces access-lists [ ethernet interface | port-channel port-channel-number ]`
  - *interface* — Specifies the Valid Ethernet port.
  - *port-channel-number* — Specifies the port-channel index.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

There are no user guidelines for this command.

### Example

The following example displays ACLs applied to the interfaces of a device.

```
Console# show interfaces access-lists
```

Interface	Input ACL	
g1	ACL1	ACL2
g2	ACL3	ACL4



# AAA Commands

## aaa authentication login

The `aaa authentication login` Global Configuration mode command defines login authentication. Use the `no` form of this command to return to the default configuration.

### Syntax

- `aaa authentication login {default | list-name} method1 [method2...]`
- `no aaa authentication login {default | list-name}`
  - **default** — Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
  - *list-name* — Character string used to name the list of authentication methods activated when a user logs in.
  - *method1* [*method2...*] — Specify at least one from the following table:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS servers for authentication.

### Default Configuration

The local user database is checked. This has the same effect as the command `aaa authentication login list-name local`.



**NOTE:** On the console, login succeeds without any authentication check if the authentication method is not defined.

### Command Mode

Global Configuration mode.

## User Guidelines

- The default and optional list names created with the **aaa authentication login** command are used with the **login authentication** command.
- Create a list by entering the **aaa authentication login list-name method** command for a particular protocol, where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.
- The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

## Example

The following example configures authentication login.

```
Console (config)# aaa authentication login default radius local  
enable none
```

## aaa authentication enable

The **aaa authentication enable** Global Configuration mode command defines authentication method lists for accessing higher privilege levels. Use the **no** form of this command to return to the default configuration.

## Syntax

- **aaa authentication enable {default | list-name} method1 [method2...]**
- **no aaa authentication enable default**
  - **default** — Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
  - *list-name* — Character string used to name the list of authentication methods activated, when using access higher privilege levels.
  - *method1* [*method2...*] — Specify at least one from the following table:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication. Uses username "\$enabx\$." where x is the privilege level.
tacacs	Uses the list of all TACACS+ servers for authentication. Uses username "\$enabx\$." where x is the privilege level.

## Default Configuration

If the **default** list is not set, only the enable password is checked. This has the same effect as the command **aaa authentication enable default enable**.

On the console, the enable password is used if it exists. If no password is set, the process still succeeds. This has the same effect as using the command **aaa authentication enable default enable none**.

## Command Mode

Global Configuration mode.

## User Guidelines

- The default and optional list names created with the **aaa authentication enable** command are used with the **enable authentication** command.
- Create a list by entering the **aaa authentication enable list-name method** command where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.
- The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.
- All **aaa authentication enable default** requests sent by the device to a RADIUS or TACACS server include the username "\$enabl5\$".

## Example

The following example sets authentication when accessing higher privilege levels.

```
Console (config)# aaa authentication enable default enable
```

## login authentication

The **login authentication** Line Configuration mode command specifies the login authentication method list for a remote telnet, SSH or console. Use the **no** form of this command to return to the default specified by the authentication login command.

## Syntax

- **login authentication {default | list-name}**
- **no login authentication**
  - **default** — Uses the default list created with the **authentication login** command.
  - *list-name* — Uses the indicated list created with the **authentication login** command.

## Default Configuration

Uses the default set with the command **authentication login**.

### Command Mode

Line Configuration mode.

### User Guidelines

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

### Example

The following example specifies the default authentication method for a console.

```
Console (config)# line console
Console (config-line)# login authentication default
```

### enable authentication

The **enable authentication** Line Configuration mode command specifies the authentication method list when accessing a higher privilege level from a remote telnet, SSH or console. Use the **no** form of this command to return to the default specified by the **enable authentication** command.

### Syntax

- **enable authentication** {default | *list-name*}
- **no enable authentication**
  - **default** — Uses the default list created with the **authentication enable** command.
  - *list-name* — Uses the indicated list created with the **authentication enable** command.

### Default Configuration

Uses the default set with the command **authentication enable**.

### Command Mode

Line Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example specifies the default authentication method when accessing a higher privilege level from a console.

```
Console (config)# line console
Console (config-line)# enable authentication default
```

## ip http authentication

The **ip http authentication** Global Configuration mode command specifies authentication methods for http. Use the **no** form of this command to return to the default.

### Syntax

- **ip http authentication** *method1* [*method2...*]
- **no ip http authentication**
  - *method1* [*method2...*] — Specify at least one from the following table:

Keyword	Source or destination
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS servers for authentication.

### Default Configuration

The local user database is checked. This has the same effect as the command **ip http authentication local**.

### Command Mode

Global Configuration mode.

### User Guidelines

- The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

### Example

The following example configures the http authentication.

```
Console (config)# ip http authentication radius local
Console (config)# ip http authentication tacacs local
```

## ip https authentication

The **ip https authentication** Global Configuration mode command specifies authentication methods for https servers. Use the **no** form of this command to return to the default.

## Syntax

- `ip https authentication method1 [method2...]`
- `no ip https authentication`
  - `method1 [method2...]` — Specify at least one from the following table:

Keyword	Source or destination
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS servers for authentication.

## Default Configuration

The local user database is checked. This has the same effect as the command `ip https authentication local`.

## Command Mode

Global Configuration mode.

## User Guidelines

- The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line.

## Example

The following example configures https authentication.

```
Console (config)# ip https authentication radius local
Console (config)# ip https authentication tacacs local
```

## show authentication methods

The `authentication methods` Privilege EXEC mode command displays information about the authentication methods.

## Syntax

- `show authentication methods`

## Default Configuration

This command has no default configuration.

**Command Mode**

Privileged EXEC mode.

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays the authentication configuration.

```
Console# show authentication methods
```

```
Login Authentication Method Lists
```

```
-----
```

```
Console_Default: None
```

```
Network_Default: Local
```

```
Enable Authentication Method Lists
```

```
-----
```

```
Console_Default: Enable None
```

```
Network_Default: Enable
```

```
Line                Login Method List      Enable Method List
```

```
-----
```

```
Console             Default                 Default
```

```
Telnet              Default                 Default
```

```
SSH                  Default                 Default
```

```
http                 : Tacacs Local
```

```
https                : Tacacs Local
```

```
dot1x                :
```

## password

The `password` Line Configuration mode command specifies a password on a line. Use the `no` form of this command to remove the password.

### Syntax

- `password password [encrypted]`
- `no password`
  - *password* — Password for this level, from 1 to 159 characters in length.
  - `encrypted` — Encrypted password to be entered, copied from another device configuration.

### Default Configuration

No password is required.

### Command Mode

Line Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example specifies a password 'secret' on a line.

```
Console (config-line)# password secret
```

## enable password

The `enable password` Global Configuration mode command sets a local password to control access to normal and privilege levels. Use the `no` form of this command to remove the password requirement.

### Syntax

- `enable password [level level] password [encrypted]`
- `no enable password [level level]`
  - *password* — Password for this level, from 1 to 159 characters in length.
  - *level level* — Level for which the password applies. If not specified the level is 15. (Range: 1 - 15)
  - `encrypted` — Encrypted password entered, copied from another device configuration.

### Default Configuration

This command has no default configuration.



### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example sets a local level 15 password "secret" to control access to user and privilege levels.

```
Console (config)# enable password level 15 secret
```

## username

The **username** Global Configuration mode command establishes a username-based authentication system. Use the **no** form of this command to remove a user name.

### Syntax

- **username** *name* [**password** *password*] [**level** *level*] [**encrypted**]
- **no username** *name*
  - *name* — The name of the user. (Range: 1 - 20 characters)
  - *password* — The authentication password for the user. (Range: 8 - 64 characters)
  - *level* — The user level. (Range: 1 -15)
  - **encrypted** — Encrypted password entered, copied from another device configuration.

### Default Configuration

No user is defined.

### Command Mode

Global Configuration mode.

### User Guidelines

- No password is required.

### Example

The following example configures user "bob" with the password "lee" and user level 15 to the system.

```
Console (config)# username bob password lee level 15
```

## show users accounts

The `show users accounts` Privileged EXEC mode command displays information about the local user database.

### Syntax

- `show users accounts`

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the local users configured with access to the system.

```
Console# show users accounts
```

Username	Privilege	Password	Aging	Password Expiry	Date	Lockout
Bob	15	--		--		--
Robert	15	--		--		--

# Address Table Commands

## bridge address

The `bridge address` VLAN Interface Configuration mode command adds a static MAC-layer station source address to the bridge table. To delete the MAC address, use the `no` form of the `bridge address` command (using the `no` form of the command without specifying a MAC address deletes all static MAC addresses belonging to this VLAN).

### Syntax

- `bridge address mac-address {ethernet interface | port-channel port-channel-number} [permanent | delete-on-reset | delete-on-timeout | secure]`
- `no bridge address [mac-address]`
  - *mac-address* — A valid MAC address in the format of xx:xx:xx:xx:xx:xx.
  - *interface* — A valid Ethernet port.
  - *port-channel-number* — A valid port-channel number.
  - *permanent* — The address can only be deleted by the `no bridge address` command.
  - *delete-on-reset* — The address is deleted after reset.
  - *delete-on-timeout* — The address is deleted after "age out" time has expired.
  - *secure* — The address is deleted after the port changes mode to unlock learning (`no port security` command). This parameter is only available when the port is in learning locked mode.

### Default Configuration

No static addresses are defined. The default mode for an added address is `permanent`.

### Command Mode

Interface Configuration (VLAN) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example adds a permanent static MAC-layer station source address 3aa2.64b3.a245 on port g8 to the bridge table.

```
Console (config)# interface vlan 2  
Console (config-vlan)# bridge address 3a:a2:64:b3:a2:45 ethernet  
g8 permanent
```

## bridge multicast filtering

The **bridge multicast filtering** Global Configuration mode command enables filtering of Multicast addresses. To disable filtering of Multicast addresses, use the **no** form of the **bridge multicast filtering** command.

### Syntax

- **bridge multicast filtering**
- **no bridge multicast filtering**

### Default Configuration

Disabled. All Multicast addresses are flooded to all ports.

### Command Mode

Global Configuration mode.

### User Guidelines

- If devices exist on the VLAN, do not change the unregistered Multicast addresses state to drop on the devices ports.
- If Multicast routers exist on the VLAN and IGMP-snooping is not enabled, the **bridge multicast forward-all** command should be used to enable forwarding all Multicast packets to the Multicast routers.

### Example

In this example, bridge Multicast filtering is enabled.

```
Console (config)# bridge multicast filtering
```

## bridge multicast address

The **bridge multicast address** Interface Configuration mode command registers MAC-layer Multicast addresses to the bridge table, and adds static ports to the group. To unregister the MAC address, use the **no** form of the **bridge multicast address** command.

### Syntax

- **bridge multicast address** {*mac-multicast-address* | *ip-multicast-address*}
- **bridge multicast address** {*mac-multicast-address* | *ip-multicast-address*} [**add** | **remove**] {**ethernet** *interface-list* | *port-channel port-channel-number-list*}
- **no bridge multicast address** {*mac-multicast-address* | *ip-multicast-address*}
  - **add** — Adds ports to the group. If no option is specified, this is the default option.
  - **remove** — Removes ports from the group.
  - *mac-multicast-address* — MAC Multicast address in the format of xx:xx:xx:xx:xx:xx.
  - *ip-multicast-address* — IP Multicast address.
  - *interface-list* — Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
  - *port-channel-number-list* — Separate nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of ports.

### Default Configuration

No Multicast addresses are defined.

### Command Mode

Interface Configuration (VLAN) mode.

### User Guidelines

- If the command is executed without **add** or **remove**, the command only registers the group in the bridge database.
- Static Multicast addresses can only be defined on static VLANs.

### Examples

The following example registers the MAC address.

```
Console (config)# interface vlan 8  
Console (config-if)# bridge multicast address 01:00:5e:02:02:03
```

The following example registers the MAC address and adds ports statically.

```
Console (config)# interface vlan 8
Console (config-if)# bridge multicast address 01:00:5e:02:02:03
add ethernet g1-9
```

## bridge multicast forbidden address

The **bridge multicast forbidden address** Interface Configuration mode command forbids adding a specific Multicast address to specific ports. Use the **no** form of this command to return to default.

### Syntax

- **bridge multicast forbidden address** {*mac-multicast-address* | *ip-multicast-address*} {**add** | **remove**} {**ethernet** *interface-list* | *port-channel port-channel-number-list*}
- **no bridge multicast forbidden address** {*mac-multicast-address* | *ip-multicast-address*}
  - **add** — Adds ports to the group.
  - **remove** — Removes ports from the group.
  - *mac-multicast-address* — MAC Multicast address in the format of xx:xx:xx:xx:xx:xx.
  - *ip-multicast-address* — IP Multicast address is in the format xxx.xxx.xxx.xxx.
  - *interface-list* — Separate non consecutive valid Ethernet ports with a comma and no spaces; hyphen is used to designate a range of ports.
  - *port-channel-number-list* — Separate non consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

### Default Configuration

No forbidden addresses are defined.

### Command Modes

Interface Configuration (VLAN) mode.

### User Guidelines

- Before defining forbidden ports, the Multicast group should be registered.

## Examples

In this example the MAC address 01:00:5e:02:02:03 is forbidden on port g9 within VLAN 8.

```
Console (config)# interface vlan 8
Console (config-if)# bridge multicast address 01:00:5e:02:02:03
Console (config-if)# bridge multicast forbidden address
01:00:5e:02:02:03 add ethernet g9
```

## bridge multicast unregistered

The **bridge multicast unregistered** Interface Configuration mode command configures the forwarding state of unregistered multicast addresses. Use the **no** form of this command to return to default.

### Syntax

- **bridge multicast unregistered** {forwarding | filtering}
- **no bridge multicast unregistered**
  - **forwarding** — Forward unregistered multicast packets.
  - **filtering** — Filter unregistered multicast packets. See usage guidelines for the case where the port is a router port.

### Default Configuration

Forwarding

### Command Modes

Interface configuration (Ethernet, Port-Channel) mode

### Default Configuration

- Unregistered multicast filtering should not be enabled on ports that are connected to routers, because the 224.0.0.x address range should not be filtered. Routers would not necessarily send IGMP reports for the 224.0.0.x range.

## Examples

This example configures the forwarding state of unregistered multicast addresses to allow forwarding.

```
Console (config)# bridge multicast unregistered forwarding
```

## bridge multicast forward-all

The **bridge multicast forward-all** Interface Configuration mode command enables forwarding of all Multicast packets on a port. To restore the default, use the **no** form of the **bridge multicast forward-all** command.

### Syntax

- **bridge multicast forward-all** {**add** | **remove**} {**ethernet** *interface-list* | *port-channel port-channel-number-list*}
- **no bridge multicast forward-all**
  - **add** — Adds ports to the group.
  - **remove** — Removes ports from the group.
  - *interface-list* — Separate non consecutive valid Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
  - *port-channel-number-list* — Separate non consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

### Default Configuration

Disable forward-all on the specified interface.

### Command Mode

Interface Configuration (VLAN) mode.

### User Guidelines

There are no user guidelines for this command.

### Example

In this example all Multicast packets on port g8 are forwarded.

```
Console (config)# interface vlan 2
Console (config-if)# bridge multicast forward-all add ethernet
g8
```

## bridge multicast forbidden forward-all

The **bridge multicast forbidden forward-all** Interface Configuration mode command forbids a port to be a forward-all-Multicast port. To restore the default, use the **no** form of the **bridge multicast forward-all** command.



## Syntax

- `bridge multicast forbidden forward-all {add | remove} {ethernet interface-list | port-channel port-channel-number-list}`
- `no bridge multicast forward-all`
  - `add` — Forbids forwarding all Multicast packets.
  - `remove` — Does not forbid forwarding all Multicast packets.
  - *interface-list* — Separates non consecutive valid Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
  - *port-channel-number-list* — Separates non consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

## Default Configuration

By default, this setting is disabled (for example, forwarding to the port is not forbidden).

## Command Mode

Interface Configuration (VLAN) mode.

## User Guidelines

- IGMP snooping dynamically discovers Multicast router ports. When a Multicast router port is discovered, all the Multicast packets are forwarded to it unconditionally.
- This command prevents a port to be a Multicast router port.

## Example

In this example, forwarding all Multicast packets to `g6` are forbidden.

```
Console (config)# interface vlan 2
Console (config-if)# bridge multicast forbidden forward-all add
ethernet g6
```

## bridge aging-time

The `bridge aging-time` Global Configuration mode command sets the address table aging time. To restore the default, use the `no` form of the `bridge aging-time` command.

## Syntax

- `bridge aging-time seconds`
- `no bridge aging-time`
  - *seconds* — Time is number of seconds. (Range: 10 - 630 seconds)

**Default Configuration**

300 seconds

**Command Mode**

Global Configuration mode.

**User Guidelines**

There are no user guidelines for this command.

**Example**

In this example the bridge aging time is set to 250.

```
Console (config)# bridge aging-time 250
```

## clear bridge

The **clear bridge** Privileged EXEC mode command removes any learned entries from the forwarding database.

**Syntax**

- **clear bridge**
  - This command has no keywords or arguments.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode.

**User Guidelines**

There are no user guidelines for this command.

**Example**

In this example, the bridge tables are cleared.

```
Console# clear bridge
```

## port security

The **port security** Interface Configuration mode command locks the port. By locking the port, new addresses are not learned on the port. To enable new address learning, use the **no** form of the **port security** command.

### Syntax

- **port security** [**forward** | **discard** | **discard-shutdown**] [**trap** *seconds*]
- **no port security**
  - **forward** — Forwards frames with unlearned source addresses, but does not learn the address.
  - **discard** — Discards frames with unlearned source addresses. This is the default if no option is indicated.
  - **discard-shutdown** — Discards frames with unlearned source addresses. The port is also shut down.
  - **trap** *Seconds* — Sends SNMP traps and defines the minimal amount of time in seconds between two consecutive traps. (Range: 1 - 1,000,000)

### Default Configuration

Disabled — No port security.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

In this example, frame forwarding is enabled without learning, and with traps sent every 100 seconds on port g1.

```
Console (config)# interface ethernet g1
Console (config-if)# port security forward trap 100
Console (config-if)# port security discard trap 100
Console (config-if)# port security discard-shutdown trap 100
```

## port security mode

The **port security mode** Interface Configuration (Ethernet, port-channel) mode command configures the port security learning mode. Use the **no** form of this command to restore the default configuration.

### Syntax

- `port security mode {lock | max-addresses}`
- `no port security mode`
  - `lock` — Saves the current dynamic MAC addresses associated with the port and disables learning, relearning and aging.
  - `max-addresses` — Deletes the current dynamic MAC addresses associated with the port and learns up to the maximum number addresses allowed on the port. Relearning and aging are enabled.

### Default Configuration

This setting is disabled.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

There are no user guidelines for this command.

### Example

In this example, port security mode is set to dynamic for Ethernet interface I/7.

```
Console(config)# interface ethernet g7
Console(config-if)# port security mode mac-addresses
```

## port security max

The `port security mode` Interface Configuration (Ethernet, port-channel) mode command configures the maximum addresses that can be learned on the port while the port is in port security max-addresses mode. Use the `no` form of this command to restore the default configuration.

### Syntax

- `port security max {max-addr}`
- `no port security max`
  - `max-addr` — Maximum number of addresses that can be learned on the port. Range is 1-128

### Default Configuration

This default configuration is 1.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

## User Guidelines

- The command is relevant only in port security max-addresses mode.

## Example

In this example, port security mode is set to dynamic for Ethernet interface *g7*.

```
Console(config)# interface ethernet g7
Console(config-if)# port security mode mac-addresses
```

## port security routed secure-address

The `port security routed secure-address` Interface Configuration mode command adds MAC-layer secure addresses to a routed port. Use the `no` form of this command to delete the MAC addresses.

## Syntax

- `port security routed secure-address mac-address`
- `no port security routed secure-address mac-address`
  - *mac-address* — Specify a MAC address in the format of `xx:xx:xx:xx:xx:xx`.

## Default Configuration

No addresses are defined.

## Command Mode

Interface Configuration (Ethernet, port-channel). Cannot be configured for a range of interfaces (range context).

## User Guidelines

- The command enables adding secure MAC addresses to a routed ports in port security mode. The command is available when the port is a routed port and in port security mode. The address is deleted if the port exits the security mode or is not a routed port.

## Example

In this example, the MAC-layer address `66:66:66:66:66:66` is added to port *g1*.

```
Console (config)# interface ethernet g1
Console (config-if)# port security routed secure-address
66:66:66:66:66:66
```

## show bridge address-table

The `show bridge address-table` Privileged EXEC mode command displays all entries in the bridge-forwarding database.

### Syntax

- `show bridge address-table [vlan vlan] [ethernet interface | port-channel port-channel-number]`
  - *vlan* — Specific valid VLAN, such as VLAN 1.
  - *interface* — A valid Ethernet port.
  - *port-channel-number* — A valid port-channel number.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- Internal usage VLANs (VLANs that are automatically allocated on routed ports) would be presented in the VLAN column by a port number and not by a VLAN ID.

### Example

In this example, all classes of entries in the bridge-forwarding database are displayed.

```
Console# show bridge address-table
```

```
Aging time is 300 sec
```

vlan	mac address	port	type
----	-----	----	----
1	00:60:70:4C:73:FF	g8	dynamic
1	00:60:70:8C:73:FF	g7	dynamic
200	00:10:0D:48:37:FF	g4	static
8	00:10:0D:48:37:FF	g2	dynamic

## show bridge address-table static

The `show bridge address-table static` Privileged EXEC mode command displays statically created entries in the bridge-forwarding database.

### Syntax

- `show bridge address-table static [vlan vlan] [ethernet interface | port-channel port-channel-number]`

### Parameters

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port number.
- *port-channel-number* — A valid port-channel number.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

In this example, all static entries in the bridge-forwarding database are displayed.

```
Console# show bridge address-table static
```

```
Aging time is 300 sec
```

vlan	mac address	port	type
----	-----	----	----
1	00:60:70:4C:73:FF	g8	permanent
1	00:60:70:8C:73:FF	g8	delete-on-timeout
200	00:10:0D:48:37:FF	g8	delete-on-reset

## show bridge address-table count

The `show bridge address-table count` Privileged EXEC mode command displays the number of addresses present in all VLANs or in a specific VLAN.

### Syntax

- `show bridge address-table count [vlan vlan] [ethernet interface-number | port-channel port-channel-number]`

### Parameters

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- This command displays the count for 1 VLAN, for all VLANs or for a specific port.
- No commas are allowed.

### Example

In this example, the number of addresses present in the VLANs are displayed.

```
Console# show bridge address-table count
```

```
Free: 8084
```

```
Used: 108
```

```
Secure:8192
```

```
Dynamic addresses:
```

```
97
```

```
Static addresses: 2
```

```
Internal addresses: 9
```



## show bridge multicast address-table

The `show bridge multicast address-table` Privileged EXEC mode command displays Multicast MAC address table information.

### Syntax

- `show bridge multicast address-table [vlan vlan-id] [address mac-multicast-address | ip-multicast-address] [format ip | mac]`
  - *vlan\_id* — A VLAN ID value.
  - *mac-multicast-address* — A MAC Multicast address in the format of `xx:xx:xx:xx:xx:xx`.
  - *ip-multicast-address* — An IP Multicast address.
  - *format* — Multicast address format. Can be `ip` or `mac`. If format is unspecified, the default is `mac`.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

In this example, Multicast MAC address table information is displayed.

```
Console # show bridge multicast address-table
Multicast address table for VLANs in MAC-GROUP bridging mode:
Vlan      MAC Address          Type          Ports
----      -
1         01:00:5e:02:02:03   static       g1, g2
19        01:00:5e:02:02:08   static       g1-8
19        01:00:5e:02:02:08   dynamic      g9-11
```

Forbidden ports for Multicast addresses:

Vlan	MAC Address	Ports
-----	-----	-----
1	01:00:5e:02:02:03	g8
19	01:00:5e:02:02:08	g8


Console # show bridge multicast address-table format ip

Multicast address table for VLANs in MAC-GROUP bridging mode:

Vlan	IP/Mac Address	Type	Ports
-----	-----	-----	-----
1	224-239.130 2.2.3	static	g1,g2
19	224-239.130 2.2.8	static	g1-8
19	224-239.130 2.2.8	dynamic	g9-11

Forbidden ports for Multicast addresses:

Vlan	IP/Mac Address	Ports
-----	-----	-----
1	224-239.130 2.2.3	g8
19	224-239.130 2.2.8	g8

 **NOTE:** A Multicast MAC address maps to multiple IP addresses, as shown above.

## show bridge multicast filtering

The `show bridge multicast filtering` Privileged EXEC mode command displays the Multicast filtering configuration.

### Syntax

- `show bridge multicast filtering vlan-id`
  - *vlan\_id* — A valid VLAN ID value.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

In this example, the Multicast configuration for VLAN 1 is displayed.

```
Console # show bridge multicast filtering 1
Filtering: Enabled
VLAN: 1
```

Port	Static	Status
g1	Forbidden	Filter
g2	Forward	Forward(s)
g3	-	Forward(d)

## show ports security

The `show ports security` Privileged EXEC mode command displays the port-lock status.

### Syntax

- `show ports security [ethernet interface | port-channel port-channel-number]`
  - *interface* — A valid Ethernet port.
  - *port-channel-number* — A valid port-channel number.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

## User Guidelines

- There are no user guidelines for this command.

## Example

In this example, all classes of entries in the port-lock status are displayed.

Console # show ports security

Port	Status	Learning	Action	Maximum	Trap	Frequency
-----	-----		-----	-----	-----	-----
g1	Disabled	Lock	-	1	-	-
g2	Disabled	Lock	-	1	-	-
g3	Disabled	Lock	-	1	-	-
g4	Disabled	Lock	-	1	-	-
g5	Disabled	Lock	-	1	-	-
g6	Disabled	Lock	-	1	-	-
g7	Disabled	Lock	-	1	-	-
g8	Disabled	Lock	-	1	-	-
g9	Disabled	Lock	-	1	-	-
g10	Disabled	Lock	-	1	-	-
g11	Disabled	Lock	-	1	-	-
g12	Disabled	Lock	-	1	-	-
g13	Disabled	Lock	-	1	-	-
g14	Disabled	Lock	-	1	-	-
g15	Disabled	Lock	-	1	-	-
g16	Disabled	Lock	-	1	-	-
g17	Disabled	Lock	-	1	-	-
g18	Disabled	Lock	-	1	-	-
g19	Disabled	Lock	-	1	-	-
g20	Disabled	Lock	-	1	-	-
g21	Disabled	Lock	-	1	-	-
g22	Disabled	Lock	-	1	-	-

Frequency: Minimum time in seconds between consecutive traps

Counter: Number of actions since last trap

## show ports security addresses

The `show ports security addresses` Privileged EXEC mode command displays the current dynamic addresses in locked ports.

### Syntax

- `show ports security addresses [ethernet interface | port-channel port-channel-number]`
  - *interface* — A valid Ethernet port.
  - *port-channel-number* — A valid port-channel number

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

There are no user guidelines for this command.

### Example

This example displays dynamic addresses in all currently locked ports.

```
Console# show ports security addresses
```

Port	Status	Learning	Current	Maximum
----	-----	-----	-----	-----
g1	Enabled	Max-addresses	2	3
g2	Disabled	Max-addresses	-	128
g3	Enabled	Lock	NA	NA



# Login Banner

## banner exec

The **banner exec** Global Configuration mode command specifies and enables a message to be displayed when an EXEC process is created (The user has successfully logged in). Use the **no** form of this command to delete the existing EXEC banner.

### Syntax

- **banner exec** *d*  
*message d*
- **no banner exec**
  - *d* — Delimiting character, for example a pound sign (#). A delimiting character cannot be used in the banner message.
  - *message* — Message text. The message must start in a new line and can be a multi-line message. Tokens in the form \$(token) in the message text can be included. Tokens are replaced with the corresponding configuration variable. Tokens are described in the usage guidelines.

### Default Configuration

Disabled (no EXEC banner is displayed).

### Command Mode

Global Configuration mode.

### User Guidelines

- Follow this command with one or more blank spaces and a delimiting character. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.
- When a user connects to a device, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the device, the EXEC banner is displayed.

- To customize the banner, use tokens in the form \$(token) in the message text. The following table displays the tokens.

Token	Information displayed in the banner
\$(hostname)	Displays the host name for the device.
\$(domain)	Displays the domain name for the device.
\$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
\$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
\$(contact)	Displays the system contact string.
\$(location)	Displays the system location string.
\$(mac-address)	Displays the base MAC address of the device.

- To disable the EXEC banner on a particular line or lines, use the no exec-banner line configuration command.

### Example

The following example sets an EXEC banner that uses tokens. The percent sign (%) is used as a delimiting character. Notice that the \$(token) syntax is replaced by the corresponding configuration variable.

```

Console# (config)# banner exec %
Enter TEXT message. End with the character '%'.

$(bold)Session activated.$(bold) Enter commands at the prompt.
%

When a user logs on to the system, the following output is displayed:

Session activated. Enter commands at the prompt.

```

## banner login

The **banner login** Global Configuration mode command specifies and enables a message to be displayed before the username and password login prompts. Use the **no** form of this command to delete the existing Login banner.



## Syntax

- **banner login**

*d message d*

- **no banner login**

- *d* — Delimiting character, for example a pound sign (#). A delimiting character cannot be used in the banner message.
- *message* — Message text. The message must start in a new line and can be a multi-line message. Tokens in the form \$(token) in the message text can be included. Tokens are replaced with the corresponding configuration variable. Tokens are described in the usage guidelines.

## Default Configuration

Disabled (no Login banner is displayed).

## Command Mode

Global Configuration mode.

## User Guidelines

- Follow this command with one or more blank spaces and a delimiting character. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.
- When a user connects to a device, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the device, the EXEC banner is displayed.
- To customize the banner, use tokens in the form \$(token) in the message text.

The following table displays the tokens.

Token	Information displayed in the banner
\$(hostname)	Displays the host name for the device.
\$(domain)	Displays the domain name for the device.
\$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
\$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
\$(contact)	Displays the system contact string.
\$(location)	Displays the system location string.
\$(mac-address)	Displays the base MAC address of the device.

- To disable the EXEC banner on a particular line or lines, use the `no exec-banner` line configuration command.

## Example

The following example sets a Login banner that uses tokens. The percent sign (%) is used as a delimiting character. Notice that the \$(token) syntax is replaced by the corresponding configuration variable.

```
Console (config)# banner login %  
Enter TEXT message. End with the character '%'.  
You have entered $(hostname).$(domain)  
%
```

When the login banner is executed, the user will see the following banner:  
You have entered host123.ourdomain.com

## banner motd

The **banner motd** Global Configuration mode command specifies and enables a message-of-the-day banner. Use the **no** form of this command to delete the existing MOTD banner.

### Syntax

- **banner motd**  
*d message d*
- **no banner motd**
  - *d* — Delimiting character, for example a pound sign (#). A delimiting character cannot be used in the banner message.
  - *message* — Message text. The message must start in a new line and can be a multi-line message. Tokens in the form \$(token) in the message text can be included. Tokens are replaced with the corresponding configuration variable. Tokens are described in the usage guidelines.

### Default Configuration

Disabled (no MOTD banner is displayed).

### Command Mode

Global Configuration mode.

### User Guidelines

- Follow this command with one or more blank spaces and a delimiting character. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.
- When a user connects to a device, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the device, the EXEC banner is displayed.

- To customize the banner, use tokens in the form \$(token) in the message text.

The following table displays the tokens.

Token	Information displayed in the banner
\$(hostname)	Displays the host name for the device.
\$(domain)	Displays the domain name for the device.
\$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
\$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
\$(contact)	Displays the system contact string.
\$(location)	Displays the system location string.
\$(mac-address)	Displays the base MAC address of the device.

- To disable the EXEC banner on a particular line or lines, use the no exec-banner line configuration command.

### Example

The following example sets a MOTD banner that uses tokens. The percent sign (%) is used as a delimiting character. Notice that the \$(token) syntax is replaced by the corresponding configuration variable..

```

Console (config)# banner motd %
Enter TEXT message. End with the character '%'.
$(bold)Upgrade$(bold) to all devices begins at March 12
%
When the login banner is executed, the user will see the following banner:
Upgrade to all devices begins at March 12

```

## exec-banner

The exec-banner Line Configuration mode command enables the display of exec banners. Use the no form of this command to disable the display of exec banners.

### Syntax

- exec-banner
- no exec-banner

### Default Configuration

Enabled

### Command Mode

Line Configuration mode

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enables the display of exec banners.

```
Console (config)# line console
Console(config-line)# exec-banner
```

## login-banner

The **login-banner** Line Configuration mode command enables the display of login banners. Use the **no** form of this command to disable the display of login banners.

### Syntax

- login-banner
- no login-banner

### Default Configuration

Enabled.

### Command Mode

Line Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enables the display of login banners.

```
Console# Console (config)# line console
Console(config-line)# login-banner
```

## motd-banner

The **motd-banner** Line Configuration mode command enables the display of message-of-the-day banners. Use the **no** form of this command to disable the display of motd banners.

### Syntax

- motd-banner
- no motd-banner

### Default Configuration

Enabled

### Command Mode

Line Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enables the display of message-of-the-day banners.

```
Console# Console (config)# line console  
Console(config-line)# motd-banner
```

## show banner

The **show banner** Privileged EXEC mode command displays the banners configuration.

### Syntax

- show banner motd
- show banner login
- show banner exec

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

## User Guidelines

- There are no user guidelines for this command.

## Example

The following example displays the banners configuration.

```
Device> show motd
Console: Enabled
Telnet: Enabled
SSH: Enabled
MOTD Message
$(bold)Upgrade$(bold) to all devices begins at March 12
```

# Clock

## clock set

The `clock set` Privileged EXEC mode command manually sets the system clock.

### Syntax

- `clock set hh:mm:ss day month year`  
or
- `clock set hh:mm:ss month day year`
  - `hh:mm:ss` — Current time in hours (military format), minutes, and seconds. (0 - 23, mm: 0 - 59, ss: 0 - 59)
  - `day` — Current day (by date) in the month. (1 - 31)
  - `month` — Current month using the first three letters by name. (Jan, ..., Dec)
  - `year` — Current year. (2000 - 2097)

### Default Configuration

The default time set is 0:0:0:0 Jan 1 2000 or xxxxx Month Day Year.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example sets the system time to 13:32:00 on the 7th March 2002.

```
Console# clock set 13:32:00 7 Mar 2002
```

## clock source

The `clock source` Privileged EXEC mode command configures an external time source for the system clock.

### Syntax

- `clock source {sntp}`
- no clock source
  - `sntp` — SNTP servers

### Default Configuration

No external clock source.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example configures an external time source for the system clock.

```
Console# clock source sntp
```

## clock timezone

The `clock timezone` Global Configuration mode command sets the time zone for display purposes. Use the `no` form of this command to set the time to Coordinated Universal Time (UTC).

### Syntax

- `clock timezone hours-offset [minutes minutes-offset] [zone acronym]`
- no clock timezone
  - *hours-offset* — Hours difference from UTC. (Range: -12 – +13)
  - *minutes minutes-offset* — Minutes difference from UTC. (Range: 0 – 59)
  - *zone acronym* — The acronym of the time zone. (Range: Up to 4 characters)

### Default Configuration

UTC.

### Command Mode

Global Configuration mode.

### User Guidelines

- The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.



## Examples

The following example sets the timezone to 6 hours difference from UTC.

```
Console# (config)# clock timezone -6 zone CST
```

## clock summer-time

The **clock summer-time** Global Configuration mode command configures the system to automatically switch to summer time (daylight saving time). Use the **no** form of this command to configure the software to not automatically switch to summer time.

### Syntax

- **clock summer-time** *recurring* {*usa* | *eu* | {*week day month hh:mm week day month hh:mm*}} [*offset offset*] [*zone acronym*]
- **clock summer-time** *date* *date month year hh:mm date month year hh:mm* [*offset offset*] [*zone acronym*]
- **clock summer-time** *date* *month date year hh:mm month date year hh:mm* [*offset offset*] [*zone acronym*]
- **no clock summer-time**
  - **recurring** — Indicates that summer time should start and end on the corresponding specified days every year.
  - **date** — Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
  - **usa** — The summer time rules are the United States rules.
  - **eu** — The summer time rules are the European Union rules.
  - *week* — Week of the month. (Range: 1 - 4, **first**, **last**)
  - *day* — Day of the week. (Range: first three letters by name, like **sun**)
  - *date* — Date of the month. (Range: 1 - 31)
  - *month* — Month. (Range: first three letters by name)
  - *year* — year - no abbreviation. (Range: 2000 - 2097)
  - *hh:mm* — Time in military format, in hours and minutes. (Range: hh: 0 - 23, mm: 0 - 59)
  - **offset** *offset* — Number of minutes to add during summer time. (Range: 1 - 1440)
  - **zone acronym** — The acronym of the time zone to be displayed when summer time is in effect. If unspecified default to the timezone acronym. (Range: Up to 4 characters)

### Default Configuration

Summer time is disabled.

**offset** *offset* — default is 60

**zone** *acronym* — If unspecified default to the timezone acronym.

If the timezone has not been defined, the default will be UTC.

### Command Mode

Global Configuration mode.

### User Guidelines

- In both the **date** and **recurring** forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.
- USA rule for daylight saving time:
  - Start: Second Sunday in March
  - End: First Sunday in November
  - Time: 2 am local time
- EU rule for daylight saving time:
  - Start: Last Sunday in March
  - End: Last Sunday in October
  - Time: 1.00 am (01:00) Greenwich Mean Time (GMT)

### Examples

The following example sets summer time starting on the first Sunday in April at 2am and finishing on the last Sunday in October at 2 am.

```
Console (config)# clock summer-time recurring first sun apr 2:00
last sun oct 2:00
```

## sntp authentication-key

The **sntp authentication-key** Global Configuration mode command defines an authentication key for Simple Network Time Protocol (SNTP). Use the **no** form of this command to remove the authentication key for SNTP.

### Syntax

- `sntp authentication-key number md5 value`
- `no sntp authentication-key number`
  - *number* — Key number. (Range: 1 - 4294967295)
  - *value* — Key value. (Range: Up to 8 characters)

### Default Configuration

No authentication key is defined.

### Command Mode

Global Configuration mode.

### User Guidelines

- Multiple keys can be generated.

### Examples

The following example defines the authentication key for SNTP.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```

## sntp authenticate

The `sntp authenticate` Global Configuration mode command grants authentication for received Network Time Protocol (NTP) traffic from servers. Use the `no` form of this command to disable the feature.

### Syntax

- `sntp authenticate`
- `no sntp authenticate`

This command has no arguments or keywords.

### Default Configuration

No authentication.

### Command Mode

Global Configuration mode.

## User Guidelines

- The command is relevant for both Unicast and Broadcast.

## Examples

The following example defines the authentication key for SNTP and grants authentication.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```

## sntp trusted-key

The **sntp trusted-key** Global Configuration mode command authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize. Use the **no** form of this command to disable authentication of the identity of the system.

## Syntax

- **sntp trusted-key** *key-number*
- **no sntp trusted-key** *key-number*
  - *key-number* — Key number of authentication key to be trusted. (Range: 1 - 4294967295)

## Default Configuration

Not trusted.

## Command Mode

Global Configuration mode.

## User Guidelines

- The command is relevant for both received Unicast and Broadcast.
- If there is at least 1 trusted key, then unauthenticated messages will be ignored.

## Examples

The following example authenticates key 8.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```

## sntp client poll timer

The `sntp client poll timer` Global Configuration mode command sets the polling time for the Simple Network Time Protocol (SNTP) client. Use the **no** form of this command to return to default.

### Syntax

- `sntp client poll timer seconds`
- `no sntp client poll timer`
  - *seconds* — Polling interval in seconds (Range: 60 - 86400)

### Default Configuration

SNTP client polling time is 1024 seconds.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example sets the polling time for the Simple Network Time Protocol (SNTP) client to 120 seconds.

```
Console (config)# sntp client poll timer 120
```

## sntp broadcast client enable

The `sntp broadcast client enable` Global Configuration mode command enables the Simple Network Time Protocol (SNTP) Broadcast clients. Use the **no** form of this command to disable the SNTP Broadcast clients.

### Syntax

- `sntp broadcast client enable`
- `no sntp broadcast client enable`

This command has no arguments or keywords.

### Default Configuration

SNTP Broadcast clients disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- The **sntp broadcast client enable** Interface Configuration mode command enables the device to receive Broadcast transmissions globally and on ALL interfaces.
- Use the **sntp client enable** Interface Configuration mode command to enable the SNTP client on a specific interface.

### Examples

The following example enables the SNTP Broadcast clients.

```
Console (config)# sntp broadcast client enable
```

## sntp anycast client enable

The **sntp anycast client enable** Global Configuration mode command enables Anycast client. Use the **no** form of this command to disable the polling for SNTP Broadcast client.

### Syntax

- **sntp anycast client enable**
- **no sntp anycast client enable**

This command has no arguments or keywords.

### Default Configuration

SNTP Anycast clients disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- Polling time is determined by the **sntp client poll timer** Global Configuration mode command.
- Use the **sntp client enable** Interface Configuration mode command to enable the SNTP client on a specific interface.

### Examples

The following example enables Anycast clients.

```
Console (config-if)# sntp anycast client enable
```

## sntp client enable

The `sntp client enable` Global Configuration mode command enables the Simple Network Time Protocol (SNTP) Broadcast and Anycast client on an interface. Use the `no` form of this command to disable the SNTP client.

### Syntax

- `sntp client enable {ethernet interface-number | vlan vlan-id | port-channel number}`
- `no sntp client enable {ethernet interface-number | vlan vlan-id | port-channel number}`
  - `ethernet interface-number` — Ethernet port number.
  - `vlan vlan-id` — Vlan number.
  - `port-channel number` — Port channel number.

### Default Configuration

The SNTP client is disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- Use the `sntp broadcast client enable` Global Configuration mode command to enable Broadcast clients globally.
- Use the `sntp anycast client enable` Global Configuration mode command to enable Anycast clients globally.

### Examples

The following example enables the SNTP client on the interface.

```
Console (config)# sntp client enable
```

## sntp client enable (interface)

The `sntp client enable` Interface Configuration mode command enables the Simple Network Time Protocol (SNTP) client on an interface. This applies to both receive Broadcast and Unicast updates. Use the `no` form of this command to disable the SNTP client.

### Syntax

- `sntp client enable`
- `no sntp client enable`

This command has no arguments or keywords.

### Default Configuration

Disabled.

### Command Mode

Interface Configuration (Ethernet, Port-Channel, VLAN) mode.

### User Guidelines

- Use the `sntp client enable` Global Configuration mode command to enable Broadcast clients globally.
- Use the `sntp anycast client enable` Global Configuration mode command to enable Anycast clients globally.

### Examples

The following example enables the SNTP client on the interface.

```
Console (config)# sntp client enable
```

## sntp unicast client enable

The `sntp unicast client enable` Global Configuration mode command enables the device to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from servers. Use the `no` form of this command to disable requesting and accepting Network Time Protocol (NTP) traffic from servers.

### Syntax

- `sntp unicast client enable`
- `no sntp unicast client enable`

This command has no arguments or keywords.

### Default Configuration

Disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- Use the `sntp server` command to define SNTP servers.



## Examples

The following example enables the device to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from servers.

```
Console (config)# sntp unicast client enable
```

## sntp unicast client poll

The `sntp unicast client poll` Global Configuration mode command enables polling for the Simple Network Time Protocol (SNTP) predefined Unicast clients. Use the `no` form of this command to disable the polling for SNTP client.

### Syntax

- `sntp unicast client poll`
- `no sntp unicast client poll`

This command has no arguments or keywords.

### Default Configuration

Disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- Polling time is determined by the `sntp client poll timer` Global Configuration mode command.

## Examples

The following example enables polling for the Simple Network Time Protocol (SNTP) predefined Unicast clients.

```
Console (config)# sntp unicast client poll
```

## sntp server

The `sntp server` Global Configuration mode command configures the device to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from a specified server. Use the `no` form of this command to remove a server from the list of SNTP servers.

## Syntax

- **sntp server** {*ip4-address* | *ip6-address* | *hostname*} [**poll**] [**key** *keyid*]
- **no sntp server** {*ip4-address* | *ip6-address* | *hostname*}
  - *ip4-address* — IPv4 server address.
  - *ip6-address* — IPv6 server address. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the usage guidelines for the interface name syntax.
  - *hostname* — Hostname of the server. dddddddddddddddd: 1-158 characters)
  - **poll** — Enable polling.
  - **Key** *keyid* — Authentication key to use when sending packets to this peer. (Range: 1 - 4294967295)

## Default Configuration

No servers are defined.

## Command Mode

Global Configuration mode.

## User Guidelines

- Up to 8 SNTP servers can be defined.
- Use the **sntp unicast client enable** Global Configuration mode command to enable predefined Unicast clients globally.
- To enable polling you should also use the **sntp unicast client poll** Global Configuration mode command for global enabling.
- Polling time is determined by the **sntp client poll timer** Global Configuration mode command.
- The IPv6Z address format: *<ip6-link-local-address>%<interface-name>*
  - *interface-name* — **vlan***<integer>* | **ch***<integer>* | **isatap***<integer>* | *<physical-port-name>* | 0
  - *integer* — *<decimal-number>* | *<integer><decimal-number>*
  - *decimal-number* — 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
  - *physical-port-name* — Designated port number, for example g1.

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is the same as not defining an egress interface.

## Example

The following example configures the device to accept SNTP traffic from the server on 192.1.1.1.

```
Console(config)# sntp server 192.1.1.1
```

## show clock

The `show clock` User EXEC mode command displays the time and date from the system clock.

### Syntax

- `show clock [detail]`
  - `detail` — Shows timezone and summertime configuration.

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- The symbol that precedes the `show clock` display indicates the following:

Symbol	Description
*	Time is not authoritative.
(blank)	Time is authoritative.
.	Time is authoritative, but SNTP is not synchronized.

## Example

The following example displays the time and date from the system clock.

```
Console# show clock

15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Device> show clock detail
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Time zone:
Acronym is PST
Offset is UTC-8

Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.
```

## show sntp configuration

The `show sntp configuration` Privileged EXEC mode command shows the configuration of the Simple Network Time Protocol (SNTP).

### Syntax

- `show sntp configuration`  
This command has no keywords or arguments.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

```
Console# show snmp configuration
Polling interval: 7200 seconds
```

```
MD5 Authentication keys: 8, 9
Authentication is required for synchronization.
Trusted Keys: 8,9
```

```
Unicast Clients Polling: Enabled.
```

Server	Polling	Encryption Key
-----	-----	-----
176.1.1.8	Enabled	9
176.1.8.179	Disabled	Disabled

```
Broadcast Clients: Enabled
Broadcast Clients Poll: Enabled
Broadcast Interfaces: g1, g3
```

## show sntp status

The `show sntp status` Privileged EXEC mode command shows the status of the Simple Network Time Protocol (SNTP).

### Syntax

- `show sntp status`

This command has no keywords or arguments.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

There are no user guidelines for this command.

### Examples

The following example shows the status of the SNTP.

```
Console# show sntp status
Clock is synchronized, stratum 4, reference is 176.1.1.8
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:
Server           Preference      Status      Last response           Offset      Delay
                  [mSec]         [mSec]
-----
176.1.1.8        Primary        Up          AFE252C1.6DBDDFF2      7.33       117.79
176.1.8.179     Secondary     Unknown    AFE21789.643287C9      8.98       189.19

Broadcast:
Interface        IP address      Last response
-----
176.1.1.8        Primary        AFE252C1.6DBDDFF2
176.1.8.179     Secondary     AFE21789.643287C9
```

# Configuration and Image Files

## dir

To display list of files on a flash file system, use the **dir** Privileged EXEC command.

### Syntax

- **dir**

This command has no arguments or keywords.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

```
Console# dir
```

```
Directory of flash:
```

File Name	Permission	FlashSize	DataSize	Modified
bb	rw	500000	97	13-Feb-2005 10:30:21
cc	rw	500000	97	13-Feb-2005 10:30:35
dd	rw	500000	97	13-Feb-2005 10:30:50
ee	rw	500000	97	13-Feb-2005 10:31:04
image-1	rw	5767168	--	07-Feb-2005 10:15:56
image-2	rw	5767168	--	07-Feb-2005 10:15:56
aaafile.prv	--	262144	--	07-Feb-2005 10:16:02

```

syslog1.sys      r-          262144    --        07-Feb-2005  10:16:02
syslog2.sys      r-          262144    --        07-Feb-2005  10:16:02
directry.prv     --          262144    --        07-Feb-2005  10:15:56
startup-config  rw          400000    95        13-Feb-2005  18:46:34
Total size of flash: 33292288 bytes
Free size of flash: 20708893 bytes

```

## more

To display a file, use the **more** Privileged EXEC command.

### Syntax

- **more** *url*
  - *url* — The location URL or reserved keyword of the source file to be copied.

The following table shows keywords and URL prefixes:

Keyword	Source or Destination
flash	Source or destination URL for Flash memory. It's the default in case a URL is specified without a prefix.
running-config	Represents the current running configuration file.
startup-config	Represents the startup configuration file.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- Files are displayed in ASCII format, except for the images that are displayed in hexadecimal format.

 **CAUTION: \*.prv files can't be displayed.**



## Examples

```
Console# more
!  
version 12.1  
!  
.  
.  
.  
interface FastEthernetg1  
ip address 176.242.100.100 255.  
ip pim dense-mode  
duplex auto  
speed auto  
!  
.  
.  
.  
end
```

## rename

To rename a file, use the **rename** Privileged EXEC command

### Syntax

- **rename** *url* *new-url*
  - *url* — The location URL.
  - *new-url* — New URL.

The following table shows keywords and URL prefixes:

Keyword	Source Destination
flash	Source or destination URL for Flash memory. It's the default in case a URL is specified without a prefix.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

**NOTICE:** \*.sys and \*.prv files can't be renamed.

### Example

```
Console# rename configuration.bak m-config.bak
```

## delete startup-config

The `delete startup-config` Privileged EXEC mode command deletes the startup-config file.

Syntax

```
delete startup-config
```

This command has no arguments or keywords.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example deletes the startup-config file.

```
Console# delete startup-config
```

## copy

The `copy` Privileged EXEC command copies any file from a source to a destination.

### Syntax

- `copy source-url destination-url [snmp]`
  - *source-url* — The location URL or reserved keyword of the source file to be copied. (Range: 1 - 160 characters)
  - *destination-url* — The destination file URL or reserved keyword of the destination file. (Range: 1 - 160 characters)
  - **snmp** — Used only when copying from/to **startup-config**. Specifies that the destination/source file is in SNMP format.

The following table displays keywords and URL prefixes.

Keyword	Source or destination
flash	Source or destination URL for Flash memory. It's the default in case a URL is specified without a prefix
running-config	Represents the current running configuration file.
startup-config	Represents the startup configuration file.
image	If source file, represent the active image file. If destination file, represent the non-active image file.
boot	Boot file.
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is <b>tftp://host/[directory]/filename</b> . The host can be IPv4 address, IPv6 address or hostname.
xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
null:	Null destination for copies or files. A remote file can be copied to null to determine its size.
backup-config	Represents the backup configuration file.
logging	Copy from a syslog file.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

## User Guidelines

- The location of a file system dictates the format of the source or destination URL.
- The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the usage guidelines for the interface name syntax.

The IPv6Z address format: `<ipv6-link-local-address>%<interface-name>`

- *interface-name* — `vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name> | 0`
- *integer* — `<decimal-number> | <integer><decimal-number>`
- *decimal-number* — `0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9`
- *physical-port-name* — Designated port number, for example `g1`.

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is the same as not defining an egress interface.

## Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, the following cannot be copied:

- If the source file and destination file are the same file.
- `xmodem` cannot be a destination. Can only be copied to `image`, `boot` and `null`.
- `tftp` cannot be the source and destination on the same copy.
- `*.prv` files can't be copied.

## Copy Character Descriptions:

Character	Description
!	For network transfers, an exclamation point indicates that the copy process is taking place. Each exclamation point indicates the successful transfer of ten packets (512 bytes each).
.	For network transfers, a period indicates that the copy process timed out. Many periods in a row typically mean that the copy process may fail.

### Copying image file from a Server to Flash Memory

Use the `copy source-url image` command to copy an image file from a server to Flash memory.

### Copying boot file from a Server to Flash Memory

Use the `copy source-url boot` command to copy a boot file from a server to Flash memory.

### Copying a Configuration File from a Server to the Running Configuration

Use the `copy source-url running-config` command to load a "configuration file" from a network server to the device "running configuration". The configuration is added to the "running configuration" as if the commands were typed in the command-line interface (CLI). The resulting configuration file is a combination of the previous "running configuration" and the loaded "configuration file", with the loaded "configuration file" having precedence.

### Copying a Configuration File from a Server to the Startup Configuration

Use the `copy source-url startup-config` command to copy a "configuration file" from a network server to the device "startup configuration". These commands replace the startup configuration file with the copied configuration file.

### Storing the Running or Startup Configuration on a Server

Use the `copy running-config destination-url` command to copy the current configuration file to a network server using TFTP. Use the `copy startup-config destination-url` command to copy the "startup configuration" file to a network server.

The configuration file copy can serve as a backup copy.

### Saving the Running Configuration to the Startup Configuration

Use the `copy running-config startup-config` command to copy the "running configuration" to the "startup configuration".

### Backup the Running Configuration or Startup Configuration to a Backup Configuration file

Use the `copy running-config flash: //FILE_NAME` to backup the running configuration to the backup configuration file. Use the `copy startup-config flash: //FILE_NAME` command to backup the startup configuration to the backup configuration file.

## Examples

The following example copies a system image named file1 from the TFTP server with an IP address of 172.16.101.101 to non active image file.

```
Console# copy tftp://172.16.101.101/file1 image
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

## delete

The `delete` Privileged EXEC mode command deletes a file from a Flash memory device.

### Syntax

- `delete url`
  - `url` — The location URL or reserved keyword of the source file to be copied.

The following table shows keywords and URL prefixes:

Keyword	Source or Destination
flash	Source or destination URL for Flash memory. It's the default in case a URL is specified without a prefix
startup-config	Represents the startup configuration file.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- Note that `*.sys`, `*.prv`, `image-1` and `image-2` files can't be deleted.

### Examples

The following example deletes a file from Flash memory.

```
Console# delete flash:test
Delete flash:test? [confirm]
```

## boot system

The `boot system` Privileged EXEC mode command specifies the system image that the device loads at startup.

### Syntax

- `boot system {image-1 | image-2}`
  - `image-1` — Specifies image 1 as the system startup image.
  - `image-2` — Specifies image 2 as the system startup image.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- Use the `show bootvar` command to find out which image is the active image.

### Examples

The following example loads system image 1 for the next device startup.

```
Console# boot system image-1
```

## show running-config

The `show running-config` Privileged EXEC mode command displays the contents of the currently running configuration file.

### Syntax

- `show running-config`
  - *sort type* — Specifies the sorting type of the file. Can be one of the following values: `interface`, `feature`.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- `show running-config` does not show all the port configurations under the port. Although the device is already configured with some default parameters, "show running config" on an empty device is empty.

## Examples

The following example displays the contents of the running-config file.

```
Console# show running-config
no spanning-tree
vlan database
vlan 2
exit
interface range ethernet g(1-2)
switchport access vlan 2
exit
interface vlan 2
bridge address 00:00:00:00:00:01 ethernet g1
exit
interface ethernet g1
gvrp enable
exit
gvrp enable
interface ethernet g24
ip address dhcp
exit
ip name-server 10.6.1.36
console#
```

## show startup-config

The `show startup-config` Privileged EXEC mode command displays the startup configuration file contents.

### Syntax

```
show startup-config
```

- `sort type` — Specifies the sorting type of the file. Can be one of the following values: **interface**, **feature**.



### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example displays the contents of the startup-config file.

```
Console# show startup-config
no spanning-tree
vlan database
vlan 2
exit
interface range ethernet g(1-2)
switchport access vlan 2
exit
interface vlan 2
bridge address 00:00:00:00:00:01 ethernet g1
exit
interface ethernet g1
gvrp enable
exit
gvrp enable
interface ethernet g24
ip address dhcp
exit
ip name-server 10.6.1.36
console#
```

## show bootvar

The `show bootvar` Privileged EXEC mode command displays the active system image file that the device loads at startup.

### Syntax

- `show bootvar`

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example displays the active system image file that the device loads at startup.

```
Console# show bootvar
Images currently available on the FLASH
image-1          active (selected for next boot)
image-2          not active
```

# Ethernet Configuration Commands

## interface ethernet

The **interface ethernet** Global Configuration mode command enters the Interface Configuration mode to configure an Ethernet type interface.

### Syntax

- **interface ethernet** *interface*
- *interface* — Valid Ethernet port.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enables port g8 for configuration.

```
Console(config)# interface ethernet g8  
Console(config-if)#
```

## interface range ethernet

The **interface range ethernet** Global Configuration mode command enters the Interface Configuration mode to configure multiple Ethernet type interfaces.

### Syntax

- `interface range ethernet {port-range | all}`
  - *port-range* — List of valid ports to add. Separate non consecutive ports with a comma and no spaces; a hyphen is used to designate a range of ports.
  - *all* — All Ethernet ports.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- Commands under the interface range context are executed independently on each active interface in the range. If the command returns an error on one of the active interfaces, it does not stop executing commands on other active interfaces.

### Example

The following example shows how ports `g18` to `g20` and ports `g22` to `g24` are grouped to receive the same command.

```
Console(config)# interface range ethernet g(22-24)
Console(config-if)#
```

## shutdown

The `shutdown` Interface Configuration mode command disables interfaces. Use the `no` form of this command to restart a disabled interface.

### Syntax

- `shutdown`
- `no shutdown`

### Default Configuration

The interface is enabled.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

## User Guidelines

- There are no user guidelines for this command.

## Examples

The following example disables port g5.

```
Console(config)# interface ethernet g5
Console(config-if)# shutdown
```

The following example re-enables port g5.

```
Console(config)# interface ethernet g5
Console(config-if)# no shutdown
```

## description

The **description** Interface Configuration mode command adds a description to an interface. Use the **no** form of this command to remove the description.

### Syntax

- **description** *string*
- **no description**
  - *string* — Comment or a description of the port up to 64 characters.

### Default Configuration

By default, the interface does not have a description.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example adds a description to the Ethernet g5.

```
Console(config)# interface ethernet g5
Console(config-if)# description RD SW#3
```

## speed

The **speed** Interface Configuration mode command configures the speed of a given Ethernet interface when not using auto-negotiation. Use the **no** form of this command to restore the default.

### Syntax

- `speed {10 | 100 | 1000}`.
- `no speed`
  - `10` — Force 10 Mbps operation.
  - `100` — Force 100 Mbps operation.
  - `1000` — Force 1000 Mbps operation.

### Default Configuration

Maximum port capability.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- The command `'no speed'` in port-channel context returns each port in the port-channel to its maximum capability.

### Example

The following example configures the speed operation of Ethernet g5 to force 100-Mbps operation.

```
Console(config)# interface ethernet g5  
Console(config-if)# speed 100
```

## duplex

The **duplex** Interface Configuration mode command configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation. Use the **no** form of this command to restore the default.

### Syntax

- `duplex {half | full}`
- `no duplex`
  - `half` — Force half-duplex operation
  - `full` — Force full-duplex operation

### Default Configuration

The interface is set to full duplex.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- Before attempting to force a particular duplex mode on the port operating at 10/100/1000 Mbps, disable the auto-negotiation on that port.
- Half duplex mode can be set only for ports operating at 10 Mbps or 100 Mbps.

### Example

The following example configures the duplex operation of Ethernet g5 to force full duplex operation.

```
Console(config)# interface ethernet g5
Console(config-if)# duplex full
```

## negotiation

Use **negotiation** command to enable auto negotiation operation for the speed and duplex parameters of a given interface. Use the **no** form of this command to disable it.

### Syntax

- **negotiation** [*capability1* [*capability2...capability5*]]
- **no negotiation**
  - *capability* — Specify the capabilities to advertise. Can be one or more of the following: 10h, 10f, 100h, 100f, 1000f. If unspecified defaults to list of all the capabilities of the port.

### Default Configuration

Auto negotiation default is enabled.

### Command Mode

Interface Configuration (Ethernet, Port-channel).

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enables auto negotiation of Ethernet port 5.

```
(config)# interface ethernet g5
(config-if)# negotiation
(config-if)#
```

## flowcontrol

The **flowcontrol** Interface Configuration mode command configures the Flow Control on a given interface. Use the **no** form of this command to restore the default.

### Syntax

- **flowcontrol** {auto | on | off}
- **no flowcontrol**
  - **auto** — Enables auto-negotiation of Flow Control.
  - **on** — Enables Flow Control.
  - **off** — Disables Flow Control.

### Default Configuration

Flow Control is off.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- Flow Control will operate only if duplex mode is set to FULL. Back Pressure will operate only if duplex mode is set to HALF.
- When Flow Control is ON, the head-of-line-blocking mechanism of this port is disabled.
- If a link is set to NOT use auto-negotiation, the other side of the link must also be configured to not use auto-negotiation.
- To select **auto**, ensure negotiation for Flow Control is enabled.

### Example

In the following example, Flow Control is enabled on g5.

```
Console(config)# interface ethernet g5
Console(config-if)# flowcontrol on
```



## system flowcontrol

The `system flowcontrol` Interface Configuration mode command enables flow control on cascade ports. To disable flow control, use the `no` form of this command.

### Syntax

```
system flowcontrol
no system flowcontrol
```

### Default Configuration

System flowcontrol is disabled.

### Command Mode

Interface Configuration mode.

### User Guidelines

This command is only operational on the 48 port device.

### Example

The following example enables flow control on port 1/4.

```
Console(config)# interface ethernet 1/4
Console(config-if)# system flowcontrol
```

## mdix

The `mdix` Interface Configuration mode command enables automatic crossover on a given interface. Use the `no` form of this command to disable automatic crossover.

### Syntax

- `mdix {on | auto}`
- `no mdix`
  - `on` — Manual mdix
  - `auto` — Auto mdi/mdix

### Default Configuration

Automatic crossover is enabled.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- **Mdix Auto:** All possibilities to connect a PC with cross OR normal cables are supported and are automatically detected.
- **Mdix ON:** It is possible to connect to a PC only with a normal cable and to connect to another switch ONLY with a cross cable.
- If MDIX is set to "no mdix", the device works opposite from the "MDIX On" behavior. With this setting you can only use either an ethernet standard cross-over cable to connect to a PC, or an ethernet standard cable to connect to another switch.

### Example

In the following example, automatic crossover is enabled on g5.

```
Console(config)# interface ethernet g5  
Console(config-if)# mdix auto
```

## back-pressure

The **back-pressure** Interface Configuration mode command enables Back Pressure on a given interface. Use the **no** form of this command to disable Back Pressure.

### Syntax

- back-pressure
- no back-pressure

### Default Configuration

Back Pressure is disabled.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- Back Pressure will operate only if duplex mode is set to half.

### Example

In the following example Back Pressure is enabled on g5.

```
Console(config)# interface ethernet g5  
Console(config-if)# back-pressure
```

## port jumbo-frame

The `port jumbo-frame` Global Configuration mode command enables jumbo frames for the device. The size of the port jumbo frame is 10K. Use the `no` form of this command to disable jumbo frames.

### Syntax

- `port jumbo-frame`
- `no port jumbo-frame`

### Default Configuration

Jumbo Frames are not enabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- The command would be effective only after reset.

### Example

In the following example, Jumbo Frames are enabled on the device.

```
Console(config)# port jumbo-frame
```

## clear counters

The `clear counters` User EXEC mode command clears statistics on an interface.

### Syntax

- `clear counters [ethernet interface | port-channel port-channel-number]`
  - *interface* — Valid Ethernet port.
  - *port-channel-number* — Valid port-channel trunk index.

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

In the following example, the counters for interface g1 are cleared.

```
Console# clear counters ethernet g1
```

## set interface active

The **set interface active** Privileged EXEC mode command reactivates an interface that was suspended by the system.

### Syntax

- **set interface active** {*ethernet interface* | **port-channel** *port-channel-number*}
- *interface* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel trunk index.

### Default Configuration

This command has no default configuration.

### Command Mode

Privilege EXEC mode.

### User Guidelines

- This command is used to activate interfaces that were configured to be active, but were shutdown for some reason.

### Example

The following example activates interface g5, which is disabled.

```
Console# set interface active ethernet g5
```

## show interfaces configuration

The **show interfaces configuration** Privilege EXEC mode command displays the configuration for all configured interfaces.

### Syntax

- **show interfaces configuration** [*ethernet interface* | **port-channel** *port-channel-number* |
- *interface* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel trunk index.

### Default Configuration

This command has no default configuration.

### Command Modes

Privilege EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the configuration for all configured interfaces:

```
Console# show interfaces configuration
```

Port	Type	Duplex	Speed	Neg	Flow Control	Admin State	MdixMode
g1	1G	Full	1000	Auto	On	Up	Auto
g2	1G	Full	100	Off	Off	Up	Off
g3	1G	Full	1000	Off	Off	Up	On

Ch	Type	Speed	Neg	Flow Control	Admin State
ch1	--	--	Enabled	Off	up
ch2	--	--	Enabled		up
ch3	--	--	Enabled		up

The displayed port configuration information includes the following:

- **Port** — The port number.
- **Port Type** — The port designated IEEE shorthand identifier. For example 1000Base-T refers to 1000 Mbps baseband signaling.
- **Duplex** — Displays the port Duplex status.
- **Speed** — Refers to the port speed.
- **Neg** — Describes the Auto-negotiation status.
- **Flow Control** — Displays the Flow Control status.
- **Back Pressure** — Displays the Back Pressure status.
- **MDIX Mode** — Displays the Auto-crossover status.
- **Admin State** — Displays whether the port is enabled or disabled.

## show interfaces status

The `show interfaces status` User EXEC mode command displays the status for all configured interfaces.

### Syntax

```
show interfaces status [ethernet interface | port-channel port-channel-number]
```

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel trunk index.

### Default Configuration

This command has no default configuration.

### Command Mode

Privilege EXEC mode

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the status for all configured interfaces.

```
Console# show interfaces status
```

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	MDIX Mode
g1	1G Copper	half	10	Enabled	off	up	Disable	on
g2	1G Copper	half	10	Enabled	off	up	Disable	on
g3	1G-Copper	half	10	Enabled	off	up	Disable	on
g4	1G-Copper	half	10	Enabled	off	up	Disable	on
g5	1G-Copper	half	10	Enabled	off	up	Disable	on
g6	1G-Copper	half	10	Enabled	off	up	Disable	on
g7	1G-Copper	half	10	Enabled	off	up	Disable	on
g8	1G-Copper	half	10	Enabled	off	up	Disable	on
g9	1G-Copper	half	10	Enabled	off	up	Disable	on
g10	1G-Copper	half	10	Enabled	off	up	Disable	on
g11	1G-Copper	half	10	Enabled	off	up	Disable	on
g12	1G-Copper	half	10	Enabled	off	up	Disable	on
g13	1G-Copper	half	10	Enabled	off	up	Disable	on
g14	1G-Copper	half	10	Enabled	off	up	Disable	on
g15	1G-Copper	half	10	Enabled	off	up	Disable	on
g16	1G-Copper	half	10	Enabled	off	up	Disable	on
g17	1G-Copper	half	10	Enabled	off	up	Disable	on
g18	1G-Copper	half	10	Enabled	off	up	Disable	on
g19	1G-Copper	half	10	Enabled	off	up	Disable	on
g20	1G-Copper	half	10	Enabled	off	up	Disable	on
g21	1G-Combo-C	half	10	Enabled	off	up	Disable	on
g22	1G-Combo-C	half	10	Enabled	off	up	Disable	on
g23	1G-Combo-C	half	10	Enabled	off	up	Disable	on
g24	1G-Combo-C	half	10	Enabled	off	up	Disable	on

Ch	Type	Duplex	Speed	Neg	Flow Control	Link State
----	-----	-----	---	-----	-----	
ch1	--	--	--	--	--	Not Present
ch2	--	--	--	--	--	Not Present
ch3	--	--	--	--	--	Not Present
ch4	--	--	--	--	--	Not Present
ch5	--	--	--	--	--	Not Present
ch6	--	--	--	--	--	Not Present
ch7	--	--	--	--	--	Not Present
ch8	--	--	--	--	--	Not Present
console#						

The displayed port status information includes the following:

- **Port** — The port number.
- **Description** — If the port has a description, the description is displayed.
- **Port Type** — The port designated IEEE shorthand identifier. For example, 1000Base-T refers to 1000 Mbps baseband signaling.
- **Duplex** — Displays the port Duplex status.
- **Speed** — Refers to the port speed.
- **Neg** — Describes the Auto-negotiation status.
- **Flow Control** — Displays the Flow Control status.
- **Back Pressure** — Displays the Back Pressure status.
- **Link State** — Displays the Link Aggregation status.



## show interfaces advertise

The `show interfaces advertise` Privileged EXEC mode command displays auto-negotiation data.

### Syntax

```
show interfaces advertise [ ethernet interface | port-channel port-channel-number ]
```

- *interface* — A valid Ethernet port.
- *port-channel-number* — Port channel index. A valid port channel.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode

### User Guidelines

There are no user guidelines for this command.

### Example

The following example displays auto-negotiation information.

```
Console# show interfaces advertise
```

Port	Type	Neg	Operational	Link	Advertisement
g1	1G Copper	Enabled	1000f,	100f,	100h, 10f, 10h
g2	1G Copper	Enabled	1000f,	100f,	100h, 10f, 10h
g3	1G-Copper	Enabled	1000f,	100f,	100h, 10f, 10h
g4	1G-Copper	Enabled	1000f,	100f,	100h, 10f, 10h
g5	1G-Copper	Enabled	1000f,	100f,	100h, 10f, 10h
g6	1G-Copper	Enabled	1000f,	100f,	100h, 10f, 10h
g7	1G-Copper	Enabled	1000f,	100f,	100h, 10f, 10h
g8	1G-Copper	Enabled	1000f,	100f,	100h, 10f, 10h
g9	1G-Copper	Enabled	1000f,	100f,	100h, 10f, 10h
g10	1G-Copper	Enabled	1000f,	100f,	100h, 10f, 10h
g11	1G-Copper	Enabled	1000f,	100f,	100h, 10f, 10h

```

g12  1G-Copper  Enabled 1000f, 100f, 100h, 10f, 10h
g13  1G-Copper  Enabled 1000f, 100f, 100h, 10f, 10h
g14  1G-Copper  Enabled 1000f, 100f, 100h, 10f, 10h
g15  1G-Copper  Enabled 1000f, 100f, 100h, 10f, 10h
g16  1G-Copper  Enabled 1000f, 100f, 100h, 10f, 10h
g17  1G-Copper  Enabled 1000f, 100f, 100h, 10f, 10h
g18  1G-Copper  Enabled 1000f, 100f, 100h, 10f, 10h
g19  1G-Copper  Enabled 1000f, 100f, 100h, 10f, 10h
g20  1G-Copper  Enabled 1000f, 100f, 100h, 10f, 10h
g21  1G-Combo-C Enabled 1000f, 100f, 100h, 10f, 10h
g22  1G-Combo-C Enabled 1000f, 100f, 100h, 10f, 10h
g23  1G-Combo-C Enabled 1000f, 100f, 100h, 10f, 10h
g24  1G-Combo-C Enabled 1000f, 100f, 100h, 10f, 10h

```

```

-----
Ch   Type          Neg      Operational Link Advertisement
-----

```

```

ch1  --            Enabled  ----
ch2  --            Enabled  ----
ch3  --            Enabled  ----
ch4  --            Enabled  ----
ch5  --            Enabled  ----
ch6  --            Enabled  ----
ch7  --            Enabled  ----
ch8  --            Enabled  ----

```

```

console#
console#
console#
console#

```

```

Console# show interfaces advertise ethernet g1
Port: g1

```

```

Type: 1G-Copper
Link state: Up
Auto Negotiation: enabled
                                1000f      1000h  100f  100h   10f   10h
Admin Local Link Advertisement    yes      no    yes  yes   yes   yes
Oper Local Link Advertisement     yes      no    yes  yes   yes   yes
Remote Link Advertisement         N/A      N/A   N/A  N/A   N/A   N/A
Priority Resolution                --      -    -    -    -    yes
Link State: Up
Auto Negotiation: disabled.

```

## show interfaces description

The **show interfaces description** User EXEC mode command displays the description for all configured interfaces.

### Syntax

```
show interfaces description [ethernet interface | port-channel port-channel-number]
```

- *interface* — Valid Ethernet port.
- *port-channel-number* — A valid port-channel trunk index.

### Default Configuration

This command has no default configuration.

### Command Modes

Privilege EXEC mode

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the description for the interface g1.

```
Console# show interfaces description ethernet g1

Port          Description
-----      -
g1            Management_port
g2            R&D_port
g3            Finance_port

Ch            Description
-----      -
Ch 1          Output
```

## show interfaces counters

The `show interfaces counters` User EXEC mode command displays traffic seen by the physical interface.

### Syntax

```
show interfaces counters [ethernet interface | port-channel port-channel-number]
```

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel index.

### Default Configuration

This command has no default configuration.

### Command Modes

Privilege EXEC mode

### User Guidelines

- There are no user guidelines for this command.

## Examples

The following example displays traffic seen by the physical interface.

```
Console# show interfaces counters
```

Port	InUcastPkts	InMcastPkts	InBcastPkts	InOctets
g1	1289	987	8	183892
g2	0	0	0	0
g3	1788	373	19	123899

Port	OutUcastPkts	OutMcastPkts	OutBcastPkts	OutOctets
g4	9	8	0	9188
g5	0	0	0	0
g6	27	8	0	8789

Ch	InUcastPkts	InMcastPkts	InBcastPkts	InOctets
1	928	0	78	27889

Ch	OutUcastPkts	OutMcastPkts	OutBcastPkts	OutOctets
1	882	0	122	23739

The following example displays counters for port g1.

```
Console# show interfaces counters ethernet g1
```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
g1	183892	1289	987	8

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
g1	9188	9	8	0

FCS Errors: 8

Single Collision Frames: 0

Multiple Collision Frames: 0

SQE Test Errors: 0

Deferred Transmissions: 0

Late Collisions: 0

Excessive Collisions: 0

Internal MAC Tx Errors: 0

Carrier Sense Errors: 0

Oversize Packets: 0

Internal MAC Rx Errors: 0

Received Pause Frames: 0

Transmitted Pause Frames: 0

The following table describes the fields shown in the display:

<b>Field</b>	<b>Description</b>
InOctets	Counted received octets.
InUcastPkts	Counted received Unicast packets.
InMcastPkts	Counted received Multicast packets.
InBcastPkts	Counted received Broadcast packets.
OutOctets	Counted transmitted octets.
OutUcastPkts	Counted transmitted Unicast packets.
OutMcastPkts	Counted transmitted Multicast packets.
OutBcastPkts	Counted transmitted Broadcast packets.
Alignment Errors	A count of frames received that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	Counted frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	Counted frames that are involved in a single collision, and are subsequently transmitted successfully.
Multiple Collision Frames	A count of frames that are involved in more than one collision and are subsequently transmitted successfully
SQE Test Errors	A count of times that the SQE TEST ERROR is received. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6.
Deferred Transmissions	A count of frames for which the first transmission attempt is delayed because the medium is busy.
Late Collisions	Counted times that a collision is detected later than one slotTime into the transmission of a packet.
Excessive Collisions	Counted frames for which transmission fails due to excessive collisions.
Internal MAC Tx Errors	Counted frames for which transmission fails due to an internal MAC sublayer transmit error.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Oversize Packets	Counted frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	Counted frames for which reception fails due to an internal MAC sublayer receive error.

Symbol Errors	For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII. For an interface operating at 10 Gb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Receive Error' on the XGMII.
Received Pause Frames	Counted MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	Counted MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

## show ports jumbo-frame

The `show ports jumbo-frame` User EXEC mode command displays the jumbo frames configuration.

### Syntax

```
show ports jumbo-frame
```

### Default Configuration

This command has no default configuration.

### Command Modes

User EXEC mode

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the jumbo frames configuration.

```
Console# show ports jumbo-frame
Jumbo frames are disabled
Jumbo frames will be enabled after reset
```



## port storm-control include-multicast

The **port storm-control include-multicast** Interface Configuration (Ethernet) mode command enables counting Multicast packets in the **port storm-control broadcast rate** command. Use the **no** form of this command to disable counting Multicast packets.

### Syntax

- **port storm-control include-multicast** [unknown-unicast]
- **no port storm-control include-multicast**  
Count unknown Unicast packets.

### Default Configuration

Disabled.

### Command Modes

Interface Configuration (Ethernet) mode

### User Guidelines

- To control Multicasts storms use the commands **port storm-control broadcast enable** and **port storm-control broadcast rate**.

### Example

The following example enables the counting of Multicast packets.

```
Console# configure  
Console(config)# port storm-control include-multicast
```

## port storm-control broadcast enable

The **port storm-control broadcast enable** Interface Configuration mode command enables Broadcast storm control. Use the **no** form of this command to disable Broadcast storm control.

### Syntax

```
port storm-control broadcast enable  
no port storm-control broadcast enable
```

### Default Configuration

Broadcast storm control is disabled.

### Command Modes

Interface Configuration (Ethernet) mode

### User Guidelines

- Use the port storm-control Broadcast rate Interface Configuration command to set the maximum rate.
- Use the port storm-control include-multicast Interface Configuration command to count also Multicast packets and optionally unknown Unicast packets in the storm control calculation.
- The command can be enabled on specific port only if rate-limit Interface Configuration command is not enabled on that port.

### Example

The following example enables Broadcast storm control on port g5.

```
Console(config)# interface ethernet g5
Console(config-if)# port storm-control broadcast enable
```

## port storm-control broadcast rate

The **port storm-control broadcast rate** Interface Configuration mode command configures the maximum Broadcast rate. Use the **no** form of this command to return to the default value.

### Syntax

**port storm-control broadcast rate** *rate*

**no port storm-control broadcast rate**

- *rate* — Maximum kilobytes per second of Broadcast, Unicast and Multicast traffic on a port. (Rate: 3.5M-1G)

### Default Configuration

The default storm control Broadcast rate is 3.5M.

### Command Mode

Interface Configuration (Ethernet) mode

### User Guidelines

- Use the **port storm-control broadcast enable** Interface Configuration mode command to enable Broadcast storm control.
- The calculated rate includes the 20 bytes of Ethernet framing overhead.

### Example

The following example configures the maximum Broadcast rate 10 kilobytes per second.

```
console(config)# interface ethernet g2
console(config-if)# port storm-control broadcast rate 10
```

## show ports storm-control

The `show ports storm-control` Privileged EXEC mode command displays the storm control configuration.

### Syntax

```
show ports storm-control [interface]
```

- *interface* — A valid Ethernet port.

### Default Configuration

This command has no default configuration.

### Command Modes

Privileged EXEC mode

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the storm control configuration.

```
Console# show ports storm-control
Port          State          Rate          Included
-----
g1            Disabled      3500          Broadcast
g2            Disabled      3500          Broadcast
g3            Disabled      3500          Broadcast
g4            Disabled      3500          Broadcast
g5            Disabled      3500          Broadcast
g6            Disabled      3500          Broadcast
g7            Disabled      3500          Broadcast
g8            Disabled      3500          Broadcast
```

g9	Disabled	3500	Broadcast
g10	Disabled	3500	Broadcast
g11	Disabled	3500	Broadcast
g12	Disabled	3500	Broadcast
g13	Disabled	3500	Broadcast
g14	Disabled	3500	Broadcast
g15	Disabled	3500	Broadcast
g16	Disabled	3500	Broadcast
g17	Disabled	3500	Broadcast
g18	Disabled	3500	Broadcast
g19	Disabled	3500	Broadcast
g20	Disabled	3500	Broadcast
g21	Disabled	3500	Broadcast
g22	Disabled	3500	Broadcast
g23	Disabled	3500	Broadcast
g24	Disabled	3500	Broadcast

## show system flowcontrol

The show system flowcontrol EXEC mode command displays the flow control state on cascade ports.

### Syntax

```
show system flowcontrol
```

### Default Configuration

This command has no default configuration.

### Command Modes

Privileged EXEC mode

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the flow control state on cascade ports..

```
console(config)# show system flowcontrol  
  
Flow control for internal cascade ports: Enabled
```



# DHCP Snooping

## ip dhcp snooping

The `ip dhcp snooping` Global Configuration mode command globally enables DHCP snooping. Use the `no` form of this command to return to the default setting.

### Syntax

- `ip dhcp snooping`
- `no ip dhcp snooping`

### Default Configuration

DHCP snooping disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- For any DHCP snooping configuration to take effect, you must globally enable DHCP snooping. DHCP snooping is not active until you enable snooping on a VLAN by using the `ip dhcp snooping vlan` Global Configuration command.

### Example

The following example globally enables DHCP snooping.

```
console (config)#ip dhcp snooping
```

## ip dhcp snooping vlan

The `ip dhcp snooping vlan` Global Configuration mode command enables DHCP snooping on a VLAN. Use the `no` form of this command to disable DHCP snooping on a VLAN.

### Syntax

`ip dhcp snooping vlan vlan-id`

`no ip dhcp snooping vlan vlan-id`

- `vlan-id` — Specify VLAN ID

### Default Configuration

DHCP snooping on VLAN disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- Prior to enabling DHCP snooping on a VLAN, globally enable DHCP snooping.

### Example

The following example enables DHCP snooping on a VLAN.

```
console (config)#ip dhcp snooping vlan vlan-id
```

## ip dhcp snooping trust

The `ip dhcp snooping trust` Interface Configuration mode command configures a port as trusted for DHCP snooping purposes. Use the `no` form of this command to return to the default setting.

### Syntax

- `ip dhcp snooping trust`
- `no ip dhcp snooping trust`

### Default Configuration

The interface is untrusted.

### Command Mode

Interface Configuration (Ethernet, Port-channel) mode.

### User Guidelines

- Configure as trusted ports those that are connected to a DHCP server or to other switches or routers.  
Configure as untrusted ports those that are connected to DHCP clients.

## ip dhcp snooping information option allowed-untrusted

The `ip dhcp snooping information option allowed-untrusted` Global Configuration mode command on a switch configures the switch to accept DHCP packets with option-82 information from an untrusted port. Use the `no` form of this command to configure the switch to drop these packets from an untrusted port.



### Syntax

- `ip dhcp snooping information option allowed-untrusted`
- `no ip dhcp snooping information option allowed-untrusted`

### Default Configuration

Discard DHCP packets with option-82 information from an untrusted port.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures a switch to accept DHCP packets with option-82 information from an untrusted port.

```
console (config)#ip dhcp snooping information option allowed-untrusted
```

## ip dhcp snooping verify

The `ip dhcp snooping verify` Global Configuration mode command configures the switch to verify on an untrusted port that the DHCP packet source *MAC address* matches the client hardware address. Use the `no` form of this command to configure the switch to not verify the MAC addresses.

### Syntax

- `ip dhcp snooping verify`
- `no ip dhcp snooping verify`

### Default Configuration

The switch verifies the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the switch to verify on an untrusted port that the source MAC address in a DHCP packet matches the client hardware address.

```
console (config)#ip dhcp snooping verify
```

## ip dhcp snooping database

The `ip dhcp snooping database` Global Configuration mode command configures the DHCP snooping binding file. Use the `no` form of this command to delete the binding file.

### Syntax

- `ip dhcp snooping database`
- `no ip dhcp snooping database`

### Default Configuration

The URL is not defined.

### Command Mode

Global Configuration mode.

### User Guidelines

- To ensure that the lease time in the database is accurate, Simple Network Time Protocol (SNTP) is enabled and configured.
- The switch writes binding changes to the binding file only when the switch system clock is synchronized with SNTP.

### Example

The following example configures the DHCP snooping binding file.

```
console (config)# ip dhcp snooping database
```

## ip dhcp snooping database update-freq

The `ip dhcp snooping database update-freq` Global Configuration mode command configures the update frequency of the DHCP snooping binding file. Use the `no` form of this command to return to default.

### Syntax

- `ip dhcp snooping database update-freq seconds`
- `no ip dhcp snooping database update-freq`
  - *seconds* — Specify, in seconds, the update frequency.

### Default Configuration

1200.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the update frequency of the DHCP snooping binding file.

```
console (config)# ip dhcp snooping database update-freq seconds
```

## ip dhcp snooping binding

The `ip dhcp snooping binding` Privileged EXEC mode command configures the DHCP snooping binding database and adds binding entries to the database. Use the `no` form of this command to delete entries from the binding database.

### Syntax

- `ip dhcp snooping binding mac-address vlan-id ip-address {ethernet interface | port-channel port-channel-number} expiry seconds`
- `no ip dhcp snooping binding mac-address vlan-id`
  - *mac-address* — Specify a MAC address.
  - *vlan-id* — Specify a VLAN number
  - *ip-address* — Specify an IP address
  - *interface* — Specify Ethernet port.
  - *port-channel-number* — Specify Port-channel number.
  - *expiry seconds* — Specify the interval, in seconds, after which the binding entry is no longer valid.

### Default Configuration

No static binding exists.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- After entering this command, an entry is added to the DHCP snooping database. If DHCP snooping binding file exists, the entry is also added to that file.
- The entries are displayed in the show commands as a 'DHCP Snooping entry'.

### Example

The following example configures the DHCP snooping binding database and adds binding entries to the database.

```
Console# ip dhcp snooping binding mac-address vlan-id ip-address {ethernet interface | port-channel port-channel-number} expiry seconds
```

## clear ip dhcp snooping database

Use the clear ip dhcp snooping database privileged EXEC command to clear the DHCP binding database.

### Syntax

- clear ip dhcp snooping database

### Default Configuration

HTTP server is disabled by default.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example clears the DHCP binding database.

```
Console#clear ip dhcp snooping database
```

## show ip dhcp snooping

Use the show ip dhcp snooping EXEC command to display the DHCP snooping configuration.

### Syntax

- show ip dhcp snooping [ethernet interface | port-channel port-channel-number]
  - *interface* — Specify Ethernet port.
  - *port-channel-number* — Specify Port-channel number.

### Default Configuration

This command has no default configuration.

### Command Mode

EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the DHCP snooping configuration.

```
Console # show ip dhcp snooping
DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 2, 7-18
DHCP snooping database: enabled
Verification of hwaddr field is enabled
Interface                               Trusted
g1                                       Yes
g2                                       Yes
```

## show ip dhcp snooping binding

The `show ip dhcp snooping binding` User EXEC mode command displays the DHCP snooping binding database and configuration information for all interfaces on a switch.

### Syntax

- `show ip dhcp snooping binding [mac-address mac-address] [ip-address ip-address] [vlan vlan] [ethernet interface | port-channel port-channel-number]`
  - *mac-address* — Specify a MAC address.
  - *ip-address* — Specify an IP address.
  - *vlan-id* — Specify a VLAN number.
  - *interface* — Specify Ethernet port.
  - *port-channel-number* — Specify Port-channel number.

### Default Configuration

This command has no default configuration.

**Command Mode**

EXEC mode.

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays the DHCP snooping binding database and configuration information for all interfaces on a switch.

```
Console# show ip dhcp snooping binding
Update frequency: 1200
Total number of binding: 2
Mac Address      IP Address  Lease(sec)  Type           VLAN  Interface
0060.704C.73FF   10.1.8.1    7983        snooping       3     g21
0060.704C.7BC1   10.1.8.2    92332       snooping       (s)3  g22
```

## GVRP Commands

### **gvrp enable (global)**

GVRP, or GARP VLAN Registration Protocol, is an industry-standard protocol designed to propagate VLAN information from device to device. With GVRP, a single switch is manually configured with all desired VLANs for the network, and all other switches on the network learn these VLANs dynamically.

The **gvrp enable** Global Configuration mode command enables GVRP globally. Use the **no** form of this command to disable GVRP globally on the switch.

#### **Syntax**

- `gvrp enable`
- `no gvrp enable`

#### **Default Configuration**

GVRP is globally disabled.

#### **Command Mode**

Global Configuration mode.

#### **User Guidelines**

- There are no user guidelines for this command.

#### **Example**

The following example globally enables GVRP on the device.

```
Console (config)# gvrp enable
```

### **gvrp enable (interface)**

The **gvrp enable** Interface Configuration mode command enables GVRP on an interface. Use the **no** form of this command to disable GVRP on an interface.

## Syntax

- `gvrp enable`
- `no gvrp enable`

## Default Configuration

GVRP is disabled on all interfaces by default.

## Command Mode

Interface Configuration (Ethernet, port-channel) mode.

## User Guidelines

- An access port would not dynamically join a VLAN because it is always a member in only one VLAN.
- Membership in an untagged VLAN would be propagated in a same way as a tagged VLAN. i.e. in such a case it's the administrator's responsibility to set the PVID to be the untagged VLAN VID.

## Example

The following example enables GVRP on ethernet g8.

```
Console (config)# interface ethernet g8
Console (config-if)# gvrp enable
```

## garp timer

The `garp timer` Interface Configuration mode command adjusts the GARP application join, leave, and leaveall GARP timer values. Use the `no` form of this command to reset the timer to default values.

## Syntax

- `garp timer {join | leave | leaveall} timer_value`
- `no garp timer`
  - `join` — Indicates the time in milliseconds that PDUs are transmitted. (Range: 10-2147483640)
  - `leave` — Indicates the amount of time in milliseconds that the device waits before leaving its GARP state. The Leave Time is activated by a Leave All Time message sent/received, and cancelled by the Join message. (Range: 10-2147483640)
  - `leaveall` — Used to confirm the port within the VLAN. The time in milliseconds between messages sent. (Range: 10-2147483640)
  - `timer_value` — Timer values in milliseconds.



### Default Configuration

The default timer values are as follows:

- Join timer — 200 milliseconds
- Leave timer — 600 milliseconds
- Leavall timer — 10000 milliseconds

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- The timer\_value value must be a multiple of 10.
- You must maintain the following relationship for the various timer values:
  - Leave time must be greater than or equal to three times the join time.
  - Leave-all time must be greater than the leave time.
- Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP application will not operate successfully.

### Example

The following example sets the leave timer for port g8 to 900 milliseconds.

```
Console (config)# interface ethernet g8
Console (config-if)# garp timer leave 900
```

## gvrp vlan-creation-forbid

The `gvrp vlan-creation-forbid` Interface Configuration mode command enables or disables dynamic VLAN creation. Use the `no` form of this command to disable dynamic VLAN creation.

### Syntax

- `gvrp vlan-creation-forbid`
- `no gvrp vlan-creation-forbid`

### Default Configuration

By default, dynamic VLAN creation is enabled.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- This command forbids dynamic VLAN creation from the interface. The creation or modification of dynamic VLAN registration entries as a result of the GVRP exchanges on an interface are restricted only to those VLANs for which static VLAN registration exists.

### Example

The following example disables dynamic VLAN creation on port g8.

```
Console (config)# interface ethernet g8
Console (config-if)# gvrp vlan-creation-forbid
```

## gvrp registration-forbid

The **gvrp registration-forbid** Interface Configuration mode command de-registers all dynamic VLANs, and prevents dynamic VLAN registration on the port. Use the **no** form of this command to allow dynamic registering for VLANs on a port.

### Syntax

- **gvrp registration-forbid**
- **no gvrp registration-forbid**

### Default Configuration

Dynamic registering and deregistering for each VLAN on the port is allowed.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows how default dynamic registering and deregistering is forbidden for each VLAN on port g8.

```
Console (config)# interface ethernet g8
Console (config-if)# gvrp registration-forbid
```

## clear gvrp statistics

The `clear gvrp statistics` Privileged EXEC mode command clears all the GVRP statistics information.

### Syntax

- `clear gvrp statistics [ethernet interface | port-channel port-channel-number]`
  - *interface* — A valid Ethernet interface.
  - *port-channel-number* — A valid port-channel trunk index.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example clears all the GVRP statistics information on port g8.

```
Console# clear gvrp statistics ethernet g8
```

## show gvrp configuration

The `show gvrp configuration` User EXEC mode command displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.

### Syntax

- `show gvrp configuration [ethernet interface | port-channel port-channel-number]`
  - *interface* — A valid Ethernet interface.
  - *port-channel-number* — A valid port-channel trunk index.

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows how to display GVRP configuration information:

```
Console# show gvrp configuration

GVRP Feature is currently enabled on the switch.
Maximum VLANs: 255

Port(s)  GVRP-      Registration  Dynamic   Timers      Leave   Leave All
         Status                VLAN      (milliseconds)
         Creation              Join
-----  -
g1       Enabled   Normal       Enabled   200         600    10000
g4       Enabled   Normal       Enabled   200         600    10000
```

## show gvrp statistics

The `show gvrp statistics` User EXEC mode command displays GVRP statistics.

### Syntax

- `show gvrp statistics [ethernet interface | port-channel port-channel-number]`
  - *interface* — A valid Ethernet interface.
  - *port-channel-number* — A valid trunk index.

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows GVRP statistics information:

```
Console# show gvrp statistics

GVRP statistics:
-----

rJE  : Join Empty Received      rJIn : Join In Received
rEmp : Empty Received          rLIn : Leave In Received
rLE  : Leave Empty Received    rLA  : Leave All Received
sJE  : Join Empty Sent         sJIn : Join In Sent
sEmp : Empty Sent              sLIn : Leave In Sent
sLE  : Leave Empty Sent        sLA  : Leave All Sent

Por  rJE  rJIn rEmp rLIn rLE  rLA  sJE  sJI  sEm  sLI  sLE  sLA
t    --- ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---
    -  -  -  -  -  -  -  -  -  -  -  -  -
g1   0   0   0   0   0   0   0   0   0   0   0   0
g2   0   0   0   0   0   0   0   0   0   0   0   0
g3   0   0   0   0   0   0   0   0   0   0   0   0
g4   0   0   0   0   0   0   0   0   0   0   0   0
g5   0   0   0   0   0   0   0   0   0   0   0   0
g6   0   0   0   0   0   0   0   0   0   0   0   0
g7   0   0   0   0   0   0   0   0   0   0   0   0
g8   0   0   0   0   0   0   0   0   0   0   0   0
```



# IGMP Snooping Commands

## ip igmp snooping (Global)

The `ip igmp snooping` Global Configuration mode command enables Internet Group Management Protocol (IGMP) snooping. Use the `no` form of this command to disable IGMP snooping.

### Syntax

- `ip igmp snooping`
- `no ip igmp snooping`

### Default Configuration

IGMP snooping is disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enables IGMP snooping.

```
Console (config)# ip igmp snooping
```

## ip igmp snooping (Interface)

The `ip igmp snooping` Interface Configuration mode command enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN. Use the `no` form of this command to disable IGMP snooping on a VLAN interface.

### Syntax

- `ip igmp snooping`
- `no ip igmp snooping`

### Default Configuration

IGMP snooping is disabled.

### Command Mode

Interface Configuration (VLAN) mode.

### User Guidelines

- IGMP snooping can only be enabled on static VLANs.

### Example

The following example enables IGMP snooping on VLAN 2.

```
Console (config)# interface vlan 2
Console (config-if)# ip igmp snooping
```

## ip igmp snooping mrouter

The `ip igmp snooping mrouter` Interface Configuration mode command enables automatic learning of Multicast router ports of a specific VLAN. Use the `no` form of this command to remove automatic learning of Multicast router ports.

### Syntax

- `ip igmp snooping mrouter learn-pim-dvmrp`
- `no ip igmp snooping mrouter learn-pim-dvmrp`

### Default Configuration

Automatic learning of mrouter ports is enabled.

### Command Mode

Interface Configuration (VLAN) mode.

### User Guidelines

- Multicast router ports can be configured statically by the `bridge multicast forward-all` command.

### Example

The following example enables automatic learning of Multicast router ports on VLANs.

```
Console (config) # interface vlan 2
Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp
```



## ip igmp snooping host-time-out

The **ip igmp snooping host-time-out** Interface Configuration mode command configures the host-time-out. If an IGMP report for a Multicast group was not received for a host-time-out period from a specific port, this port is deleted from the member list of that Multicast group. Use the **no** form of this command to reset to default host-time-out.

### Syntax

- **ip igmp snooping host-time-out** *time-out*
- **no ip igmp snooping host-time-out**
  - *time-out* — Host timeout in seconds. (Range: 60 - 2147483647)

### Default Configuration

The default host-time-out is 260 seconds.

### Command Mode

Interface Configuration (VLAN) mode.

### User Guidelines

- The timeout should be at least greater than  $2 * \text{query\_interval} + \text{max\_response\_time}$  of the IGMP router.

### Example

The following example configures the host timeout to 300 seconds.

```
Console (config)# interface vlan 2
Console (config-if)# ip igmp snooping host-time-out 300
```

## ip igmp snooping mrouter-time-out

The **ip igmp snooping mrouter-time-out** Interface Configuration mode command configures the mrouter-time-out. The **mrouter-time-out** command is used for setting the aging-out time after Multicast router ports are automatically learned. Use the **no** form of this command to configure the default mrouter-time-out.

### Syntax

- **ip igmp snooping mrouter-time-out** *time-out*
- **no ip igmp snooping mrouter-time-out**
  - *time-out* — mrouter timeout in seconds (Range: 1 - 2147483647)

### Default Configuration

The default value is 300 seconds.

### Command Mode

Interface Configuration (VLAN) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the mrouter timeout to 200 seconds.

```
Console (config)# interface vlan 2
Console (config-if)# ip igmp snooping mrouter-time-out 200
```

## ip igmp snooping leave-time-out

The `ip igmp snooping leave-time-out` VLAN Interface Configuration mode command configures the leave-time-out. If an IGMP report for a Multicast group is not received within the leave-time-out period after an IGMP leave was received from a specific port, the current port is deleted from the member list of that Multicast group. Use the `no` form of this command to configure the default leave-time-out.

### Syntax

- `ip igmp snooping leave-time-out {time-out | immediate-leave}`
- `no ip igmp snooping leave-time-out`
  - *time-out* — leave-time-out in seconds. (Range: 0 - 2147483647)
  - `immediate-leave` — Specifies that the port should be immediately removed from the members list after receiving IGMP Leave.

### Default Configuration

The default leave-time-out configuration is 10 seconds.

### Command Mode

Interface Configuration (VLAN) mode.

### User Guidelines

- The leave timeout should be set greater than the maximum time that a host is allowed to respond to an IGMP Query.
- Use `immediate leave` only where there is only one host connected to a port.

## Example

The following example configures the host leave-time-out to 60 seconds.

```
Console (config)# interface vlan 2
Console (config-if)# ip igmp snooping leave-time-out 60
```

## ip igmp snooping querier enable

The **ip igmp snooping querier enable** Interface Configuration mode command enables Internet Group Management Protocol (IGMP) querier on a specific VLAN. Use the **no** form of this command to disable IGMP querier on a VLAN interface.

### Syntax

- ip igmp snooping querier enable
- no ip igmp snooping querier enable

### Default Configuration

IGMP querier is disabled.

### Command Mode

Interface Configuration (VLAN) mode.

### User Guidelines

- IGMP snooping querier can be enabled on a VLAN only if IGMP snooping is enabled for that VLAN. No more than one switch can be configured as an IGMP Querier for a VLAN. When IGMP Snooping Querier is enabled, it starts after host-time-out/2 with no IGMP traffic detected from a Multicast router. The IGMP Snooping Querier disables itself if it detects IGMP traffic from a Multicast router. It restarts itself after host-time-out/2. Following are the IGMP Snooping Querier parameters as function of the IGMP Snooping parameters:
  - QueryMaxResponseTime: host-time-out/15.
  - QueryInterval: host-time-out/ 3.

## Example

The following example enables IGMP querier on a specific VLAN.

```
Console (config)# ip igmp snooping querier enable
```

## ip igmp snooping querier address

The `ip igmp snooping querier address` Interface Configuration mode command defines the source IP address that the IGMP Snooping querier uses. Use the **no** form of this command to return to default.

### Syntax

- `ip igmp snooping querier address ip-address`
- `no ip igmp snooping querier address`
  - *ip-address* — Source IP address.

### Default Configuration

If an IP address is configured for the VLAN, it is used as the source address of the IGMP snooping querier.

### Command Mode

Interface Configuration mode (VLAN).

### User Guidelines

- If an IP address is not configured by this command, and no IP address is configured for the IGMP querier VLAN interface, the querier is disabled.

### Example

The following example defines the source IP address to be used by the IGMP Snooping querier.

```
Console (config)#ip igmp snooping querier address ip-address
```

## show ip igmp snooping mrouter

The `show ip igmp snooping mrouter` User EXEC mode command displays information on dynamically learned Multicast router interfaces.

### Syntax

- `show ip igmp snooping mrouter [interface vlan-id]`
  - *vlan\_id* — VLAN ID value.

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows IGMP snooping mrouter information.

```
Console # show ip igmp snooping mrouter

VLAN          Ports
-----
2             g1
```

## show ip igmp snooping interface

The `show ip igmp snooping interface` User EXEC mode command shows IGMP snooping configuration.

### Syntax

- `show ip igmp snooping interface vlan-id`
  - *vlan\_id* — VLAN ID value.

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

## Example

The example displays IGMP snooping information.

```
Console # show ip igmp snooping interface 1000
IGMP Snooping is globally enabled

IGMP Snooping admin: Enabled
Hosts and routers IGMP version: 2
IGMP snooping oper mode: Enabled
IGMP snooping querier admin: Enabled
IGMP snooping querier oper: Enabled
IGMP snooping querier address admin:
IGMP snooping querier address oper: 172.16.1.1

IGMP host timeout is 300 sec
IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec
IGMP mrouter timeout is 300 sec
Automatic learning of multicast router ports is enabled
```

## show ip igmp snooping groups

The `show ip igmp snooping groups` User EXEC mode command displays the Multicast groups learned by IGMP snooping.

### Syntax

- `show ip igmp snooping groups [vlan vlan-id] [ip-multicast-address ip-multicast-address]`
  - *vlan\_id* — VLAN ID value
  - *ip-multicast-address* — IP Multicast address

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- To see the full Multicast address table (including static addresses) use the **show bridge address-table** command.

### Example

The example shows IGMP snooping information.

```
Console # show ip igmp snooping groups
```

Vlan	IP Address	Querier	Ports
1	224-239.130 2.2.3	Yes	g1, g2
19	224-239.130 2.2.8	Yes	g9-11





# IP Addressing Commands

## clear host dhcp

The `clear host dhcp` Privileged EXEC mode command deletes entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).

### Syntax

- `clear host dhcp {name | *}`
  - `name` — Particular host entry to remove. (Range: 1 - 158 characters.)
  - `*` — Removes all entries.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- This command would delete the host name-to-address mapping temporarily until the next renew of the IP address.

### Examples

The following example deletes all entries from the host name-to-address mapping.

```
Console# clear host dhcp *
```

## ip address

The `ip address` Interface Configuration mode command sets an IP address. Use the `no` form of this command to remove an IP address.

## Syntax

- `ip address ip-address {mask | prefix-length}`
- `no ip address [ip-address]`
  - *ip-address* — IP address
  - *mask* — Specifies the network mask of the IP address. (Range: Valid Subnet mask)
  - *prefix-length* — The number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 8 -30)

## Default Configuration

No IP address is defined for interfaces.

## Command Mode

Interface Configuration (Ethernet, VLAN, port-channel).

## User Guidelines

- An IP address cannot be configured for a range of interfaces (range context).

## Example

The following example configures VLAN 1 with the IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console (config)# interface vlan 1
Console (config-if)# ip address 131.108.1.27 255.255.255.0
```

## ip address dhcp

The `ip address dhcp` Interface Configuration mode command acquires an IP address on an interface from the Dynamic Host Configuration Protocol (DHCP) server. Use the `no` form of this command to deconfigure any acquired address.

The `no ip address dhcp` command deconfigures any IP address that was acquired, thus sending a DHCPRELEASE message.

## Syntax

- `ip address dhcp [hostname host-name]`
- `no ip address dhcp`
  - *hostname* — Specifies the host name. (Range: 1 - 20 characters)
  - *host-name* — DHCP host name. This name need not be the same as the host name entered in Global Configuration mode.

## Default Configuration

This command has no default configuration.

## Command Mode

Interface Configuration (Ethernet, VLAN, port-channel).

## User Guidelines

- The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol.
- Some DHCP Servers require that the DHCPDISCOVER message have a specific host name. The most typical usage of the **ip address dhcp hostname *host-name*** command is when *host-name* is the host name provided by the system administrator.
- If a device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.
- If the **ip address dhcp** command is used with or without the optional keyword, the DHCP option 12 field (host name option) is included in the DISCOVER message. By default, the specified DHCP host name is the device globally configured host name.
- However, you can use the **ip address dhcp hostname *host-name*** command to place a different name in the DHCP option 12 field than the globally configured host name of the device.
- The **no ip address dhcp** command deconfigures any IP address that was acquired, thus sending a DHCPRELEASE message.

## Example

The following example acquires an IP address on an Ethernet interface from DHCP.

```
Console (config)# interface ethernet g8
Console (config-if)# ip address dhcp
```

## ip default-gateway

The **ip default-gateway** Global Configuration mode command defines a default gateway (router). Use the **no** form of this command to remove the default gateway.

## Syntax

- **ip default-gateway ip-address**
- **no ip default-gateway**
  - *ip-address* — Valid IP address that specifies the IP address of the default gateway.

## Default Configuration

No default gateway is defined.

**Command Mode**

Global Configuration mode.

**User Guidelines**

- There are no User Guidelines for this command.

**Example**

The following example defines an ip default gateway.

```
Console(config)# ip default-gateway 192.168.1.1
```

## show ip interface

The `show ip interface` User EXEC mode command displays the usability status of interfaces configured for IP.

**Syntax**

- `show ip interface [ethernet interface-number | vlan vlan-id | port-channel number]`
  - `ethernet interface-number` — Valid port number.
  - `vlan vlan-id` —VLAN number.
  - `port-channel number` — Port-channel number.

**Default Configuration**

This command has no default configuration.

**Command Mode**

User EXEC mode.

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example the displays the usability status of interfaces configured for IP.

```
Console# show ip interface
```

Gateway IP Address	Type	Activity Status
-----	-----	-----
10.7.1.1	Static	Active

IP address	Interface	Type
-----	-----	-----
10.7.1.192/24	VLAN 1	Static
10.7.2.192/24	VLAN 2	DHCP

## arp

The **arp** Global Configuration mode command adds a permanent entry in the Address Resolution Protocol (ARP) cache. Use the **no** form of this command to remove an entry from the ARP cache.

### Syntax

- **arp** *ip\_addr hw\_addr* {**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*}
- **no arp** *ip\_addr* {**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*}
- *ip\_addr* — IP address or IP alias to map to the specified MAC address.
- *hw\_addr* — MAC address to map to the specified IP address or IP alias.
- **ethernet** *interface-number* — Ethernet port number.
- **vlan** *vlan-id* — VLAN number.
- **port-channel** *number* — Port-channel number.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses. Because most hosts support dynamic resolution, static ARP cache entries do not need to be specified.

### Example

The following example adds the IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
Console (config)# arp 198.133.219.232 00:00:0c:40:0f:bc ethernet
g8
```

## arp timeout

The **arp timeout** Global Configuration mode command configures how long an entry remains in the ARP cache. Use the **no** form of this command to restore the default value.

### Syntax

- `arp timeout seconds`
- `no arp timeout`
  - *seconds* — Time (in seconds) that an entry remains in the ARP cache. (Range: 1 - 40000000)

### Default Configuration

The default timeout is 60000 seconds.

### Command Mode

Global Configuration mode.

### User Guidelines

- It is recommended not to set the timeout value to less than 3600.

### Example

The following example configures ARP timeout to 12000 seconds.

```
Console (config)# arp timeout 12000
```

## clear arp-cache

The **clear arp-cache** Privileged EXEC mode command deletes all dynamic entries from the ARP cache.

### Syntax

- `clear arp-cache`

### Default Configuration

This command has no default configuration.

**Command Mode**

Privileged EXEC mode.

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example deletes all dynamic entries from the ARP cache.

```
Console# clear arp-cache
```

## show arp

The `show arp` Privileged EXEC mode command displays entries in the ARP table.

**Syntax**

- `show arp [ip-address ip-address] [mac-address mac-address] [ethernet interface | port-channel port-channel-number]`

**Parameters**

- *ip-address* — Displays the ARP entry of a specific IP address.
- *mac-address* — Displays the ARP entry of a specific MAC address.
- *interface* — Displays the ARP entry of a specific Ethernet port interface.
- *port-channel-number* — Displays the ARP entry of a specific Port-channel number interface.

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode.

**User Guidelines**

- There are no user guidelines for this command.

## Example

The following example displays entries in the ARP table.

```
Console# show arp
ARP timeout: 60000 Seconds

Interface      IP address      HW address      status
-----
g1             10.7.1.102     00:10:B5:04:DB:4B Dynamic
g2             10.7.1.135     00:50:22:00:2A:A4 Static
```

## ip domain-lookup

The `ip domain-lookup` Global Configuration mode command enables the IP Domain Naming System (DNS)-based host name-to-address translation. Use the `no` form of this command to disable the DNS.

### Syntax

- `ip domain-lookup`
- `no ip domain-lookup`

This command has no arguments or keywords.

### Default Configuration

The DNS -based host name-to-address translation is enabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example enables the IP Domain Naming System (DNS)-based host name-to-address translation.

```
Console (config)# ip domain-lookup
```



## ip domain-name

The **ip domain-name** Global Configuration mode command defines a default domain name, that the software uses to complete unqualified host names (names without a dotted-decimal domain name). Use the **no** form of this command to disable use of the Domain Name System (DNS).

### Syntax

- **ip domain-name** *name*
- **no ip domain-name**
  - *name* — Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Range: 1 - 158 characters)

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example defines a default domain name of `www.dell.com`.

```
Console (config)# ip domain-name www.dell.com
```

## ip name-server

The **ip name-server** Global Configuration mode command sets the available name servers. Use the **no** form of this command to remove a name server.

### Syntax

- **ip name-server** *server-address* [*server-address2* ... *server-address8*]
- **no ip name-server** [*server-address1* ... *server-address8*]
  - *server-address* — IP addresses of the name server. Up to 8 servers can be defined in one command or by using multiple commands.

### Default Configuration

No name server addresses are specified.

### Command Mode

Global Configuration mode.

### User Guidelines

- The preference of the servers is determined by the order they were entered.
- Up to 8 servers can be defined.

### Examples

The following example sets the available name server.

```
Console (config)# ip name-server 176.16.1.18
```

## ip host

The **ip host** Global Configuration mode command defines a static host name-to-address mapping in the host cache. Use the **no** form of this command to remove the name-to-address mapping.

### Syntax

**ip host** *name address*

**no ip host** *name*

- *name* — Name of the host. (Range: 1 - 158 characters)
- *address* — Associated IP address.

### Default Configuration

No host is defined.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example defines a static host name-to-address mapping in the host cache.

```
Console (config)# ip host accounting.dell.com 176.10.23.1
```

## clear host

The `clear host` Privileged EXEC mode command deletes entries from the host name-to-address cache.

### Syntax

- `clear host {name | *}`
  - *name* — Particular host entry to remove. (Range: 1 - 158 characters)
  - \* — Removes all entries.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example deletes entries from the host name-to-address cache.

```
Console (config)# clear host *
```

## show hosts

The `show hosts` User EXEC mode command displays the default domain name, a list of name server hosts, the static and the cached list of host names and addresses.

### Syntax

- `show hosts [name]`
  - *name* — Name of the host. (Range: 1 - 158 characters)

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

## Examples

The following example displays host information.

```
console> show hosts
Default domain is GM.COM
Name/address lookup is enabled
Name servers: 176.16.1.18 176.16.1.19
Static host name-to-address mapping:

Host                               Addresses
----                               -
www.dell.com                       176.16.8.8 176.16.8.9
Cache:

          TTL(Hours)
Host      Total      Elapsed  Type      Addresses
----      -
www.dell.com 72          3        IP        171.64.14.203
```

# IPv6 Addressing

## ipv6 enable

The `ipv6 enable` Interface Configuration mode command enables IPv6 processing on an interface. Use the `no` form of this command to disable IPv6 processing on an interface.

### Syntax

- `ipv6 enable [no-autoconfig]`
- `no ipv6 enable`
  - `no-autoconfig` — Enables IPv6 processing on an interface without a stateless address autoconfiguration procedure.

### Default Configuration

IPv6 is disabled. When the interface is enabled unless using the `no-autoconfig` parameter, stateless address autoconfiguration procedure is enabled.

### Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. This command cannot be configured for a range of interfaces (range context).

### User Guidelines

- The `ipv6 enable` command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The `no ipv6 enable` command removes the entire IPv6 interface configuration.
- To enable stateless address autoconfiguration on an enabled IPv6 interface, use the `ipv6 address autoconfig` command.

### Example

The following example enables IPv6 processing on VLAN 1.

```
Console (config)# interface vlan 1  
Console (config-if)# ipv6 enable
```

## ipv6 address autoconfig

The `ipv6 address autoconfig` Interface Configuration mode command enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface. Addresses are configured depending on the prefixes received in Router Advertisement messages. , Use the `no` form of this command to disable address autoconfiguration on the interface.

### Syntax

- `ipv6 address autoconfig`
- `no ipv6 address autoconfig`

### Default Configuration

Address autoconfiguration is enabled on the interface, no addresses are assigned by default.

### Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode.

### User Guidelines

- When address autoconfig is enabled, router solicitation ND procedure is initiated to discover a router and assign IP addresses to the interface, based on the advertised on-link prefixes.
- When disabling address autoconfig, automatically generated addresses assigned to the interface are removed.
- The default state of the address autoconfig is 'enabled'. To enable an IPv6 interface without address autoconfig, use the `enable ipv6 no-autoconfig` command.

### Example

The following example enables automatic configuration of IPv6 addresses using stateless autoconfiguration on VLAN 1.

```
Console (config)# interface vlan 1
Console (config-if)# ipv6 address autoconfig
```

## ipv6 icmp error-interval

The `ipv6 icmp error-interval` Global Configuration mode command configures the rate limit interval and bucket size parameters for IPv6 Internet Control Message Protocol (ICMP) error messages. Use the `no` form of this command to return the interval to its default setting.

### Syntax

- `ipv6 icmp error-interval milliseconds [bucketsize]`
- `no ipv6 icmp error-interval`

- *milliseconds* — The time interval between tokens being placed in the bucket, each token represents a single ICMP error message. (Range: 0 - 2147483647)
- *bucketsize* — The maximum number of tokens stored in the bucket. (Range: 1 - 200)

### Default Configuration

The default interval is 100ms and the default bucketsize is 10 tokens.

### Command Mode

Global Configuration mode.

### User Guidelines

- To set the average icmp error rate limit, calculate the interval by the following formula:  
Average Packets Per Second = (1/ interval) \* bucket size

### Example

The following example configures the rate limit interval to 200ms and bucket size to 20 tokens for IPv6 Internet Control Message Protocol (ICMP) error messages.

```
Console (config)# ipv6 icmp error-interval 200 10
```

## show ipv6 icmp error-interval

The `show ipv6 error-interval` command Privileged EXEC mode command displays the IPv6 ICMP error interval setting.

### Syntax

- `show ipv6 icmp error-interval`

### Default Configuration

This command has no default setting.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

## Example

The following example displays the IPv6 ICMP error interval setting..

```
Console> show ipv6 icmp error-interval
Rate limit interval: 100 ms
Bucket size: 10 tokens
```

## ipv6 address

The `ipv6 address` Interface Configuration mode command configures an IPv6 address for an interface. use the `no` form of this command to remove the address from the interface.

### Syntax

- `ipv6 address ipv6-address/prefix-length [eui-64] [anycast]`
- `no ipv6 address [ipv6-address/prefix-length] [eui-64]`
  - *ipv6-address* — The IPv6 network assigned to the interface. The address is specified in hexadecimal using 16-bit values between colons.
  - *prefix-length* — The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal. (Range: 3-128 only 64 when the `eui-64` parameter is used)
  - `eui-64` — Specifies to build an interface ID in the low order 64 bits of the IPv6 address based on the interface MAC address.
  - `anycast` — Indicates that this address is an anycast address.

### Default Configuration

No IP address is defined for the interface.

### Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. Cannot be configured for a range of interfaces (range context).

### User Guidelines

- If the value specified for the `/prefix-length` argument is greater than 64 bits, the prefix bits have precedence over the interface ID.
- Using the `no ipv6 address` command without arguments removes all manually configured IPv6 addresses from an interface, including link local manually configured addresses.



## Example

The following example configures an IPv6 address FE80::260:3EFF:FE11:6770 for interface g1.

```
Console# Console (config)# interface g1
Console (config-if)# ipv6 address FE80::260:3EFF:FE11:6770
```

## ipv6 address link-local

The **ipv6 address link-local** Interface Configuration mode command configures an IPv6 link-local address for an interface. Use the **no** form of this command to return to the default link local address on the interface.

### Syntax

- **ipv6 address** *ipv6-address* **link-local**
- **no ipv6 address link-local**
  - *ipv6-address* — The IPv6 network address assigned to the interface. The address is specified in hexadecimal using 16-bit values between colons.

### Default Configuration

IPv6 is enabled on the interface. Link local address of the interface is FE80::EUI64 (interface MAC address).

### Command Mode

Interface configuration (Ethernet, VLAN, Port-channel). Cannot be configured for a range of interfaces (range context).

### User Guidelines

- Using the **no ipv6 link-local address** command removes the manually configured link local IPv6 address from an interface. Multiple IPv6 addresses can be configured per interface, but only one link-local address. When the **no ipv6 link-local address** command is used, the interface is reconfigured with the standard link local address (the same IPv6 link-local address that is set automatically when the **enable ipv6** command is used). The system automatically generates a link-local address for an interface when IPv6 processing is enabled on the interface. To manually specify a link-local address to be used by an interface, use the **ipv6 link-local address** command. The system supports only 64 bits prefix length for link-local addresses.

### Example

The following example assigns FE80::260:3EFF:FE11:6770 as the link-local address.

```
Console# Console (config)# interface g1
Console (config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-
local
```

## ipv6 unreachablees

The **ipv6 unreachablees** Interface Configuration mode command enables the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface. Use the **no** form of this command to prevent the generation of unreachable messages.

### Syntax

- **ipv6 unreachablees**
- **no ipv6 unreachablees**

### Default Configuration

ICMP unreachable messages are sent by default.

### Command Mode

Interface configuration mode (Ethernet, VLAN, Port-channel).

### User Guidelines

- If a packet addressed to one of the interface's IP address with TCP/UDP port not assigned is received, and ICMP unreachable messages is enabled, the device sends an ICMP unreachable message. To disable sending ICMP unreachable messages on the interface, use the **no ipv6 unreachablees** command

### Example

The following example enables the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on interface g1.

```
Console# Console (config)# interface g1
Console (config-if)# ipv6 unreachablees
```

## ipv6 default-gateway

The **ipv6 default-gateway** Global Configuration mode command defines an IPv6 default gateway. Use the **no** form of this command to remove the default gateway.

## Syntax

- `ipv6 default-gateway ipv6-address`
- `no ipv6 default-gateway`
  - *ipv6-address* — IPv6 address of the next hop that can be used to reach that network. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the usage guidelines for the interface name syntax.

## Default Configuration

No default gateway is defined.

## Command Mode

Global Configuration mode.

## User Guidelines

- The IPv6Z address format: `<ipv6-link-local-address>%<interface-name>`
- *interface-name* — `vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name> | 0`
- *integer* — `<decimal-number> | <integer><decimal-number>`
- *decimal-number* — `0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9`
- *physical-port-name* — Designated port number, for example `g1`.
- Configuring a new default GW without deleting the previous configured information overwrites the previous configuration.
- A configured default GW has a higher precedence over automatically advertised (via router advertisement message).
- If the egress interface is not specified, the default interface will be selected. Specifying `interface zone=0` is equal to not defining an egress interface.

## Example

The following example defines an IPv6 default gateway.

```
Console(config)# ipv6 default-gateway fe80::11
```

## ipv6 mld join-group

The `ipv6 mld join-group` interface configuration command configures Multicast Listener Discovery (MLD) reporting for a specified group. To cancel reporting and leave the group, use the **no** form of this command.

### Syntax

- `ipv6 mld join-group group-address`
- `no ipv6 mld join-group group-address`
  - `group-address` — The multicast group IPv6 address.

### Default Configuration

This command has no default setting.

### Command Mode

Interface configuration (Ethernet, VLAN, Port-channel).

### User Guidelines

- The `ipv6 mld join-group` command configures MLD reporting for a specified group. The packets that are addressed to a specified group address will be passed up to the client process in the device.

### Example

The following example configures MLD reporting for specific groups.

```
Console(config-if)# ipv6 mld join-group ff02::10
```

## ipv6 mld version

The `ipv6 mld version` interface configuration command changes the Multicast Listener Discovery Protocol (MLD) version. To change to the default version, use the `no` form of this command.

### Syntax

- `ipv6 mld version {1 | 2}`
- `no ipv6 mld version`
  - 1 — Specifies MLD version 1.
  - 2 — Specifies MLD version 2.

### Default Configuration

MLD version 2.

### Command Mode

Interface configuration (Ethernet, VLAN, Port-channel).

### User Guidelines

- There are no user guidelines for this command.

## Example

The following example defines an IPv6 default gateway.

```
Console(config-if)# ipv6 mld version 1
```

## show ipv6 interface

The **show ipv6 interface** Privileged EXEC mode command displays the usability status of interfaces configured for IPv6.

### Syntax

- **show ipv6 interface** [*ethernet interface-number* | *vlan vlan-id* | *port-channel number*]
  - *ethernet interface-number* — Ethernet port number
  - *vlan vlan-id* — VLAN number
  - *port-channel number* — Port channel number

### Default Configuration

Displays all IPv6 interfaces.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- To display IPv6 neighbor discovery cache information, use the **show ipv6 neighbors** command in the privileged EXEC mode.

### Examples

The following examples displays the usability status of interfaces configured for IPv6.

```
Console# show ipv6 interface
Interface                IP addresses                Type
-----                -
g2                        7001::5668/64 [ANY]        manual
g2                        6001::1234/64              manual
g2                        fe80::22/64                 manual
g2                        ff02::1                     linklayer
g2                        ff02::78                    manual
```

```

g2                ff02::1:ff00:22                manual
g2                ff02::1:ff00:1234              manual
g2                ff02::1:ff00:5668              manual
VLAN 1            2002:1:1:1:200:b0ff:fe00::      other
VLAN 1            3001::1/64                      manual
VLAN 1            4004::55/64 [ANY]              manual
VLAN 1            fe80::200:b0ff:fe00:0          linklayer
VLAN 1            ff02::1                        linklayer
VLAN 1            ff02::77                       manual
VLAN 1            ff02::1:ff00:0                 manual
VLAN 1            ff02::1:ff00:1                 manual
VLAN 1            ff02::1:ff00:55                manual

```

Default Gateway IP address	Type	Interface	State
fe80::77	Static	VLAN 1	unreachable
fe80::200:cff:fe4a:dfa8	Dynamic	VLAN 1	stale

```

Console# show ipv6 interface vlan 15

```

```

IPv6 is disabled

```

```

Console# show ipv6 interface vlan 1

```

```

Number of ND DAD attempts: 1

```

```

MTU size: 1500

```

```

Stateless Address Autoconfiguration state: enabled

```

```

ICMP unreachable message state: enabled

```

```

MLD version: 2

```

IP addresses	Type	DAD State
-----	-----	-----
2002:1:1:1:200:b0ff:fe00::	other	Active
3001::1/64	manual	Active
4004::55/64 [ANY]	manual	Active
fe80::200:b0ff:fe00:0	linklayer	Active
ff02::1	linklayer	Active
ff02::77	manual	-----
ff02::1:ff00:0	manual	-----
ff02::1:ff00:1	manual	-----
ff02::1:ff00:55	manual	-----

## show ipv6 route

The `show ipv6 route` Privileged EXEC mode command displays the current state of the IPv6 routing table.

### Syntax

- `show ipv6 route`

### Default Configuration

This command has no default setting.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

## Example

The following example displays the current state of the IPv6 routing table.

```
Console> show ipv6 route
Codes: L - Local, S - Static, I - ICMP, ND - Router Advertisement
The number in the brackets is the metric.

S  ::/0 via fe80::77 [0] VLAN 1 Lifetime Infinite
ND ::/0 via fe80::200:cff:fe4a:dfa8 [0] VLAN 1 Lifetime 1784 sec
L  2001::/64 is directly connected, g2 Lifetime Infinite
L  2002:1:1:1::/64 is directly connected, VLAN 1 Lifetime 2147467
sec
L  3001::/64 is directly connected, VLAN 1 Lifetime Infinite
L  4004::/64 is directly connected, VLAN 1 Lifetime Infinite
L  6001::/64 is directly connected, g2 Lifetime Infinite
```

## ipv6 nd dad attempts

The `ipv6 nd dad attempts` Interface Configuration mode command configures the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the unicast IPv6 addresses of the interface. Use the `no` form of this command to return the number of messages to the default value.

### Syntax

- `ipv6 nd dad attempts attempts-number`
- `no ipv6 nd dad attempts`
  - *attempts-number* — The number of neighbor solicitation messages. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions. (Range: 0 - 600)

### Default Configuration

Duplicate address detection on unicast IPv6 addresses with the sending of one (1) neighbor solicitation message is enabled.

### Command Mode

Interface configuration (Ethernet, VLAN, Port-channel). Cannot be configured for a range of interfaces (range context).



## User Guidelines

- Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.
- An interface returning to administratively “up” restarts duplicate address detection for all of the unicast IPv6 addresses on the interface. While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to TENTATIVE. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.
- When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message is displayed.
- All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.
- If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).
- Until DAD process is completed, an IPv6 address is in tentative state and can not be used for data transfer. It is recommended to limit the configured value.

## Example

The following example configures the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the unicast IPv6 addresses of the interface to 10.

```
Console# Console (config)# interface g1
Console (config-if)# ipv6 nd dad attempts 10
```

## ipv6 host

The **ipv6 host** Global Configuration mode command defines a static host name-to-address mapping in the host name cache. Use the **no** form of this command to remove the host name-to-address mapping.

## Syntax

- `ipv6 host name ipv6-address1 [ipv6-address2...ipv6-address4]`
- `no ipv6 host name`
  - *name* — Name of the host. (Range: 1 - 158 characters)
  - *ipv6-address1* — Associated IPv6 address. The address is specified in hexadecimal using 16-bit values between colons. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the usage guidelines for the interface name syntax.
  - *ipv6-address2-4* (optional) — Addition IPv6 addresses that may be associated with the host's name

## Default Configuration

No host is defined.

## Command Mode

Global Configuration mode.

## User Guidelines

- The IPv6Z address format: `<ipv6-link-local-address>%<interface-name>`
  - *interface-name* — `vlan<integer>` | `ch<integer>` | `isatap<integer>` | `<physical-port-name>` | 0
  - *integer* — `<decimal-number>` | `<integer><decimal-number>`
  - *decimal-number* — 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
  - *physical-port-name* — Designated port number, for example g1.

## Example

The following example defines a static host name-to-address mapping in the host name cache.

```
Console (config)# ipv6 host ABC fe80::11 fe80::22
```

## ipv6 neighbor

The `ipv6 neighbor` Global Configuration mode command configures a static entry in the IPv6 neighbor discovery cache. Use the `no` form of this command to remove a static IPv6 entry from the IPv6 neighbor discovery cache.

## Syntax

- `ipv6 neighbor ipv6_addr hw_addr {ethernet interface-number | vlan vlan-id | port-channel number }`
- `no ipv6 neighbor ipv6_addr {ethernet interface-number | vlan vlan-id | port-channel number}`
  - `ipv6_addr` — IPv6 address to map to the specified MAC address.
  - `hw_addr` — MAC address to map to the specified IPv6 address.
  - `ethernet interface-number` — Valid port number.
  - `vlan vlan-id` — VLAN number.
  - `port-channel number` — Port channel number.

## Default Configuration

This command has no default setting.

## Command Mode

Global Configuration mode.

## User Guidelines

- The `ipv6 neighbor` command is similar to the `arp (global)` command.
- If an entry for the specified IPv6 address already exists in the neighbor discovery cache, learned through the IPv6 neighbor discovery process, the entry is automatically converted to a static entry.
- Use the `show ipv6 neighbors` command to view static entries in the IPv6 neighbor discovery cache.

## Example

The following example configures a static entry in the IPv6 neighbor discovery cache.

```
Console (config)# ipv6 neighbor ff02::78 00:02:85:0E:1C:00  
ethernet g1 vlan 1 port-channel 1
```

## ipv6 set mtu

The `ipv6 mtu` Privileged EXEC mode command sets the Maximum Transmission Unit (MTU) size of IPv6 packets sent on an interface. Use the default parameter to restore the default MTU size.

## Syntax

- `ipv6 set mtu {ethernet interface | vlan vlan-id | port-channel port-channel-number} { bytes | default}`
  - `ethernet interface` — Valid interface number.
  - `vlan vlan-id` — VLAN number.
  - `port-channel port-channel-number` — Valid Port Channel index.
  - `bytes` — MTU in bytes with a minimum is 1280 bytes.
  - `default`— Sets the default MTU size to 1500 bytes.

## Default Configuration

1500 bytes.

## Command Mode

Privileged EXEC mode.

## User Guidelines

This command is intended for debugging and testing purposes and should be used only by technical support personnel.

## Example

The following example sets the Maximum Transmission Unit (MTU) size of IPv6 packets sent on an interface to 1700.

```
Console> ipv6 set mtu ethernet g1 1700
```

## show ipv6 neighbors

The `show ipv6 neighbors` Privileged EXEC mode command displays IPv6 neighbor discovery cache information.

## Syntax

- `show ipv6 neighbors {static | dynamic} [ipv6-address ipv6-address] [mac-address mac-address]`
  - `static` — Display static neighbor discovery cache entries.
  - `dynamic` — Display dynamic neighbor discovery cache entries.
  - `ipv6-address` — Display the neighbor discovery cache information entry of a specific IPv6 address.
  - `mac-address` — Display the neighbor discovery cache information entry of a specific MAC address.

## Command Mode

Privileged EXEC mode.

## User Guidelines

- The associated interface of a MAC address can be aged out from the FDB table, so the Interface field can be empty.
- When an ARP entry is associated with an IP interface that is defined on a port or port-channel, the VLAN field is empty.
- The possible neighbor cash states are:

**INCMP** (Incomplete) — Address resolution is being performed on the entry. Specifically, a Neighbor Solicitation has been sent to the solicited-node multicast address of the target, but the corresponding Neighbor Advertisement has not yet been received.

**REACH** (Reachable) — Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While REACHABLE, no special action takes place as packets are sent.

**STALE** — More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While stale, no action takes place until a packet is sent.

**DELAY** — More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly, and a packet was sent within the last DELAY\_FIRST\_PROBE\_TIME seconds. If no reachability confirmation is received within DELAY\_FIRST\_PROBE\_TIME seconds of entering the DELAY state, a Neighbor Solicitation is sent and the state is changed to PROBE.

**PROBE** — A reachability confirmation is actively sought by retransmitting Neighbor Solicitations every RetransTimer milliseconds until a reachability confirmation is received.

## Example

The following example displays IPv6 neighbor discovery cache information.

```
Console# show ipv6 neighbors dynamic

Interface IPv6 address          HW address          State
-----  -
VLAN 1    2031:0:130F::010:B504:D  00:10:B5:04:DB:4B  REACH
          BB4
VLAN 1    2031:0:130F::050:2200:2  00:50:22:00:2A:A4  REACH
          AA4
```

## clear ipv6 neighbors

The `clear ipv6 neighbors` Privileged EXEC mode command deletes all entries in the IPv6 neighbor discovery cache, except static entries.

### Syntax

- `clear ipv6 neighbors`

### Default Configuration

This command has no default setting.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example deletes all entries in the IPv6 neighbor discovery cache, except static entries.

```
Console> clear ipv6 neighbors
```

# iSCSI Commands

## iscsi enable

The `iscsi enable` Global Configuration mode command globally enables iSCSI awareness. Use the `no` form of this command to disable iSCSI awareness.

### Syntax

- `iscsi enable`
- `no iscsi enable`

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- Until iSCSI VLAN is configured by using `iscsi vlan` command the switch will not assign any specific VLAN to iSCSI flows.
- When User uses the `no iscsi enable` command, iSCSI resources (TCAM) should be released.

### Example

The following example enable iSCSI awareness.

```
Console (config)# iscsi enable
```

## iscsi target port

The `iscsi target port` Global Configuration mode command configures iTCP port(s), iSCSI targets' addresses and names. Use the `no` form of this command to delete iSCSI port/s, target.

## Syntax

- **iscsi target port** *tcp-port-1* [*tcp-port-2... tcp-port-8*] [**address** *ip-address*] [**name** *targetname*]
- **no iscsi target port** *tcp-port-1* [*tcp-port-2... tcp-port-8*] [**address** *ip-address*]
  - *tcp-port* — TCP port number or list of TCP port numbers on which iSCSI target/s listen to requests. Up to 16 TCP ports can be defined in the system in one command or by using multiple commands.
  - *ip-address* — IP address of the iSCSI target. When the **no** form is used, and the tcp port to be deleted is one bound to a specific IP address, the address field must be present.
  - *targetname* — iSCSI name of the iSCSI target. The name can be statically configured; however, it can be obtained from iSCSI or from sendTargets response. The initiator **MUST** present both its iSCSI Initiator Name and the iSCSI Target Name to which it wishes to connect in the first login request of a new session or connection.

## Default Configuration

iSCSI well-known ports 3260 and 860 are configured as default but can be removed as any other configured target.

## Command Mode

Global Configuration mode.

## User Guidelines

- When working with private iSCSI ports (not IANA assigned iSCSI ports 3260/860), it is recommended to specify the target IP address as well, so the switch will only snoop frames with which the TCP destination port is one of the configured TCP ports, AND their destination IP is the target's IP address. This way the CPU is not be falsely loaded by non-iSCSI flows (if by chance other applications also choose to use these {un-reserved} ports).
- When a port is already defined and not bound to an IP, and the user binds it to an IP, the User should first remove it by using the **no** form of the command and then add it again, this time together with the relevant IP.
- Target names are only for display when using show iscsi command. These names are not used to match (or for doing any sanity check) with the iSCSI session information acquired by snooping.
- Maximum of 16 TCP ports can be configured either bound to IP or not. This number can be changed by using iscsi max target ports command; however it will take affect only after reset.

## Example

The following example configures TCP Port49154 to target IP address 172.16.1.20.

```
Console (config)# iscsi target port 49154 address 172.16.1.20
```



## iscsi cos

The `iscsi cos` Global Configuration mode command sets the quality of service profile that will be applied to iSCSI flows. Use the `no` form of this command to return to default.

### Syntax

- `iscsi cos {vpt vpt | dscp dscp} [remark]`
- `no iscsi cos`
  - *vpt/dscp* — The Virtual Priority Tag (VPT) or DSCP to which the iSCSI frames are assigned.
  - **remark** — Mark the iSCSI frames with the configured VPT/DSCP when egressing the switch.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- iSCSI flows are assigned by default with a VPT/DSCP mapped to the highest queue not used for stack management or Voice VLAN (if mapping not changed by the user). The user should also take care of configuring the relevant (VPT to queue/DSCP to queue) table in order to complete the setting.
- Setting the VPT/DSCP sets the QoS profile, which determines the egress queue to which the frame is mapped. The switch default setting for egress queues scheduling is strict priority. The downside of strict priority is that, in certain circumstances (under heavy high priority traffic), other lower priority traffic may get starved. In WRR the queue to which the flow is assigned to can be set to get the required percentage. The user must complete the QoS setting by configuring the relevant ports to work in WRR mode with the adequate weights.

### Example

The following example sets the quality of service profile that will be applied to iSCSI flows.

```
Console (config)# iscsi cos vpt 5 remark
```

## iscsi aging time

The `iscsi aging-time` Global Configuration mode command sets aging time for iSCSI sessions. Use the `no` form of this command to cancel aging.

## Syntax

- `iscsi aging-time time`
- `no iscsi aging-time`
  - *time* — The number in minutes a session is not active prior to its removal. (Range: 1- 43,200)

## Default Configuration

5 minutes.

## Command Mode

Global Configuration mode.

## User Guidelines

- All connections are measured in groups of 32. The aging time is the minimum time a connection's activity is measured deterministically. The actual aging may depend on the number of currently monitored connections, causing the activity to take longer. The result is 256 connections, which are all not active, with an aging time of 5 minutes can be measured in  $256/32 * 5\text{min} = 40\text{ min}$ . The above example is a 'worst case' scenario.
- Behavior when changing aging time:
  - When aging time is increased — Time for aging out current sessions is recalculated and increased only by the difference.
  - When aging time is decreased — Time for aging out current sessions will be decreased by the difference. If after re-calculation, it is deemed that the session 'silence' time is already greater than the new aging time, the session will be immediately declared as aged-out.

## Example

The following example sets aging time for iSCSI sessions to 100 minutes.

```
Console (config)# iscsi aging-time 100
```

## iscsi max connections

The `iscsi max connections` Global Configuration mode command sets the maximum number of iSCSI connections that can be supported. Use the `no` form of this command to return to the default value.

## Syntax

`iscsi max tcp connections max-connections`

`no iscsi max tcp connections`

- *max-connections* — The maximum number of iSCSI connections that can be supported. (Range: 64 – 512)

**Default Configuration**

256 connections.

**Command Mode**

Global Configuration mode.

**User Guidelines**

- The new setting takes effect after reset.
- The amount of iSCSI connections affects other system features: iSCSI aware, DHCP snooping and ACL rules use the same system resource. When increasing the number of iSCSI connections the other application rules (DHCP snooping or ACL) can be removed after reset.
- If more than the Max Connections (default 256) connections exist in Network, the connections still receive their QoS profile but only the Max Connections number will be displayed.

**Example**

The following example sets the maximum number of iSCSI connections to 100.

```
Console (config)# iscsi max tcp connections 100
```

**show iscsi**

The show iscsi Privileged EXEC mode command displays the iSCSI settings.

**Syntax**

- show iscsi

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode.

**User Guidelines**

There are no user guidelines for this command.

## Example

The following example displays the iSCSI settings.

```
Console # show iscsi
iscsi enabled
iscsi vpt is 5, remark
Session aging time: 60 min
Maximum number of connections is 256
-----
iscsi targets and TCP ports:
-----

TCP Port      Target IP Address      Name
860
3260
5000
30001         172.16.1.1             iqn.1993-11.com.disk-
                        vendor:diskarrays.sn.
                        45678.tape:sys1.xyz
30033         172.16.1.10
30033         172.16.1.25
```

## show iscsi sessions

The `show iscsi sessions` Privileged EXEC mode command displays the iSCSI sessions.

### Syntax

- `show iscsi sessions [detailed]`
  - *detailed* — Displayed list is detailed when this option is used.

### Default Configuration

If not specified, sessions are displayed in short mode (not detailed).

### Command Mode

Privileged EXEC mode.

## User Guidelines

- The aging mechanism checks session activity in a group of N TCP iSCSI connections. In the worst case, when all 256 sessions are monitored and are not terminated gracefully, the existing mechanism causes inaccuracy: the last group of monitored iSCSI sessions ages out after  $(256/N) * \text{aging-time}$ .
- In general, the higher number of ungracefully terminated iSCSI TCP connections, the higher the aging inaccuracy is.

## Example

The following example displays the iSCSI sessions.

```
Console # show iscsi sessions
Target: iqn.1993-11.com.disk-vendor:diskarrays.sn.45678
-----
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
ISID: 11
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
ISID: 222
-----
Target: iqn.103-1.com.storage-vendor:sn.43338.
storage.tape:sys1.xyz
Session 3:
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
Session 4:
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
-----
```

```
Console# show iscsi sessions detailed
Target: iqn.1993-11.com.disk-vendor:diskarrays.sn.45678
-----
Session 1:
```

Initiator: iqn.1992-04.com.os-  
vendor.plan9:cdrom.12.storage:sys1.xyz

---

Time started: 23-Jul-2002 10:04:50

Time for aging out: 10 min

ISID: 11

Initiator	Initiator	Target	Target
IP address	TCP port	IP address	IP port
172.16.1.3	49154	172.16.1.20	30001
172.16.1.4	49155	172.16.1.21	30001
172.16.1.5	49156	172.16.1.22	30001

Session 2:

---

Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10

Time started: 23-Jul-2002 21:04:50

Time for aging out: 2 min

ISID: 22

Initiator	Initiator	Target	Target
IP address	TCP port	IP address	IP port
172.16.1.30	49200	172.16.1.20	30001
172.16.1.30	49201	172.16.1.21	30001

# LACP Commands

## lacp system-priority

The `lacp system-priority` Global Configuration mode command configures the system priority. Use the `no` form of this command to reset to default.

### Syntax

- `lacp system-priority value`
- `no lacp system-priority`
  - *value* — Value of the priority. (Range: 1 - 65535)

### Default Configuration

The default system priority value is 1.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the system priority to 120.

```
Console (config)# lacp system-priority 120
```

## lacp port-priority

The `lacp port-priority` Interface Configuration mode command configures the priority value for physical ports. Use the `no` form of this command to reset to default priority value.

### Syntax

- `lacp port-priority value`
- `no lacp port-priority`
  - *value* — Port priority value. (Range: 1 - 65535)

### Default Configuration

The default port priority value is 1.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the priority value for port g8 to 247.

```
Console (config)# interface ethernet g8
Console (config-if)# lacp port-priority 247
```

## lacp timeout

The **lacp timeout** Interface Configuration mode command assigns an administrative LACP timeout. Use the **no** form of this command to reset the default administrative LACP timeout.

### Syntax

- **lacp timeout** {long | short}
- **no lacp timeout**
  - **long** — Specifies a long timeout value.
  - **short** — Specifies a short timeout value.

### Default Configuration

The default port timeout value is **long**.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example assigns an administrative LACP timeout for port g8 to a long timeout value.

```
Console (config)# interface ethernet g8
Console (config-if)# lacp timeout long
```



## show lacp ethernet

The `show lacp ethernet` Privilege EXEC mode command displays LACP information for Ethernet ports.

### Syntax

- `show lacp ethernet interface [parameters | statistics | protocol-state]`
  - *Interface* — Ethernet interface.

### Default Configuration

This command has no default configuration.

### Command Mode

Privilege EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows how to display LACP statistics information.

```
Console# show lacp ethernet g1 statistics  
Port g1 LACP Statistics:  
LACP PDUs sent:2  
  
LACP PDUs received:2
```

## show lacp port-channel

The `show lacp port-channel` Privileged EXEC mode command displays LACP information for a port-channel.

### Syntax

- `show lacp port-channel [port_channel_number]`
  - *port\_channel\_number* — The port-channel number.

### Default Configuration

This command has no default configuration.

**Command Mode**

Privileged EXEC mode.

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example shows how to display LACP port-channel information.

```
Console# show lacp port-channel 1
Port-Channel 1:Port Type 1000 Ethernet
  Actor
    System Priority:1
    MAC Address: 00:02:85:0E:1C:00
    Admin Key:      29
    Oper Key:       29
  Partner
    System Priority:0
    MAC Address: 00:00:00:00:00:00
    Oper Key:     14
```

# Line Commands

## line

The **line** Global Configuration mode command identifies a specific line for configuration and enters the Line

### Syntax

- `line {console | telnet | ssh}`
  - `console` — Console terminal line.
  - `telnet` — Virtual terminal for remote console access (Telnet).
  - `ssh` — Virtual terminal for secured remote console access (SSH).

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example configures the device as a virtual terminal for remote console access.

```
Console(config)# line telnet  
Console(config-line)#
```

## speed

The **speed** Line Configuration mode command sets the line baud rate.

### Syntax

- `speed bps`
  - `bps` — Baud rate in bits per second (bps). The options are 2400, 4800, 9600, 19200 and 38400.

### Default Configuration

This default speed is 9600.

### Command Mode

Line Configuration (console) mode.

### User Guidelines

- The configured speed would be applied when Autobaud is disabled.
- If Autobaud is disabled, the new speed is implemented immediately.

### Examples

The following example sets the baud rate to 9600.

```
Console (config)# line console
Console(config-line)# speed 9600
```

## autobaud

The **autobaud** Line Configuration mode command sets the line for automatic baud rate detection (autobaud). Use the **no** form of this command to disable automatic baud rate detection.

### Syntax

- `autobaud`
- `no autobaud`

### Default Configuration

Autobaud disabled.

### Command Mode

Line Configuration (console) mode.

### User Guidelines

- To start communications using automatic baud detection, press the *Enter* key twice.

## Examples

The following example sets the line for automatic baud rate detection.

```
Console (config)# line console
Console(config-line)# autobaud
```

## exec-timeout

The **exec-timeout** Line Configuration mode command sets the interval that the system waits until user input is detected. Use the **no** form of this command to restore the default setting.

### Syntax

- **exec-timeout** *minutes* [*seconds*]
- **no exec-timeout**
  - *minutes* — Integer that specifies the number of minutes. (Range: 0 - 65535)
  - *seconds* — Additional time intervals in seconds. (Range: 0 - 59)

### Default Configuration

The default configuration is 10 minutes.

### Command Mode

Line Configuration mode.

### User Guidelines

- To specify no timeout, enter the **exec-timeout** ("0 0") command.

## Examples

The following example configures the interval that the system waits until user input is detected to 20 minutes.

```
Console (config)# line console
Console(config-line)# exec-timeout 20
```

## show line

The `show line` User EXEC mode command displays line parameters.

### Syntax

- `show line [console | telnet | ssh]`
  - *console* — Console terminal line.
  - *telnet* — Virtual terminal for remote console access (Telnet).
  - *ssh* — Virtual terminal for secured remote console access (SSH).

### Default Configuration

Default value is `console`.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example displays the Line Configuration.

```
Console (config)# line console
Console(config-line)# exec-timeout 20
```

## terminal history

The `terminal history` EXEC mode command enables the command history function for the current terminal session. Use the `no` form of this command to disable the command history function.

### Syntax

- `terminal history`
- `no terminal history`

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

The command enables the command history for the current session. The default would be determined by the history Line Configuration command.

### Examples

The following example disables the command history function for the current terminal session.

```
console# show line console
Interactive timeout: 10 minutes
History: 10
```

## terminal history size

The **terminal history size** EXEC mode command changes the command history buffer size for the current terminal session. Use the no form of this command to reset the command history buffer size to the default.

### Syntax

- terminal history size number-of-commands
- no terminal history size

### Default Configuration

The default is determined by the history size Line Configuration command.

### Command Mode

User EXEC mode.

### User Guidelines

- The maximum for the sum of all buffers is 256.

### Examples

The following example configures the command history buffer size to 20 commands for the current terminal session.

```
Console> terminal history size 20
```





# LLDP Commands

## **lldp enable (global)**

The **lldp enable** Global Configuration mode command enables Link Layer Discovery Protocol (LLDP). Use the **no** form of this command to disable LLDP.

### **Syntax**

- **lldp enable**
- **no lldp enable**

### **Default Configuration**

LLDP is enabled.

### **Command Mode**

Global Configuration mode.

### **User Guidelines**

- There are no guidelines for this command.

### **Example**

The following example enables Link Layer Discovery Protocol (LLDP) .

```
console (config)# lldp enable
```

## **lldp enable (interface)**

The **lldp enable** Interface Configuration mode command enables Link Layer Discovery Protocol (LLDP) on an interface. Use the **no** form of this command to disable LLDP on an interface.

## Syntax

- `lldp enable [rx | tx | both]`
- `no lldp enable`
  - *rx* — Receive only LLDP packets.
  - *tx* — Transmit only LLDP packets.
  - *both* — Receive and transmit LLDP packets (default)

## Default Configuration

Enabled in both modes.

## Command Modes

Interface Configuration (Ethernet) mode.

## User Guidelines

- LLDP manages LAG ports individually. LLDP sends separate advertisements on each port in a LAG. LLDP data received through LAG ports is stored individually per port.
- LLDP operation on a port is not dependent on STP state of a port. I.e. LLDP frames are sent and received on blocked ports. If a port is controlled by 802.1X, LLDP operates only if the port is authorized.

## Examples

The following example enables Link Layer Discovery Protocol (LLDP) on an interface (*g5*).

```
Console(config)# interface ethernet g5
Console(config-if)# lldp enable
```

## lldp timer

The `lldp timer command` Global Configuration mode command specifies how often the system sends Link Layer Discovery Protocol (LLDP) updates. Use the **no** form of this command to revert to the default setting.

## Syntax

- `lldp timer seconds`
- `no lldp timer`
  - *seconds* — Specifies in seconds how often the software sends LLDP update. (Range: 5 - 32768 seconds)

### Default Configuration

Default — 30 seconds.

### Command Modes

Global Configuration mode.

### User Guidelines

There are no user guidelines for this command.

### Examples

The following example specifies the system to send Link Layer Discovery Protocol (LLDP) updates every 50 seconds.

```
Console (config) # lldp timer 50
```

## lldp hold-multiplier

The `lldp hold-multiplier` Global Configuration mode command specifies the amount of time the receiving device should hold a Link Layer Discovery Protocol (LLDP) packet before discarding it. Use the `no` form of this command to revert to the default setting.

### Syntax

- `lldp hold-multiplier number`
- `no lldp hold-multiplier`
  - *number* — Specifies the hold time to be sent in the LLDP update packets as a multiple of the timer value. (Range: 2 - 10)

### Default Configuration

The default configuration is 4.

### Command Modes

Global Configuration mode.

### User Guidelines

- The actual time-to-live value used in LLDP frames can be expressed by the following formula:  $TTL = \min(65535, LLDP\text{-}Timer * LLDP\text{-}HoldMultiplier)$ . For example, if the value of LLDP timer is '30', and the value of the LLDP hold multiplier is '4', then the value '120' is encoded in the TTL field in the LLDP header.

## Examples

The following example specifies the amount of time the receiving device should hold a Link Layer Discovery Protocol (LLDP) packet to 10 before discarding it.

```
Console (config) # lldp hold-multiplier 10
```

## Ildp reinit-delay

The `lldp reinit-delay` Global Configuration mode command specifies the minimum time an LLDP port waits before reinitializing LLDP transmissions. Use the **no** form of this command to revert to the default setting.

### Syntax

- `lldp reinit-delay` *seconds*
- `no lldp reinit-delay`
  - *seconds* — Specifies the minimum time in seconds an LLDP port will wait before reinitializing LLDP transmissions. (Range 1 - 10 seconds)

### Default Configuraiton

2 seconds.

### Command Modes

Global Configuration mode.

### User Guidelines

There are no user guidelines for this command.

## Examples

The following example pecifies the minimum time an LLDP port will wait before reinitializing LLDP transmissions to 5 seconds.

```
Console (config) # lldp reinit-delay 5
```

## Ildp tx-delay

The `lldp tx-delay` Global Configuration mode command specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. Use the **no** form of this command to revert to the default setting.

### Syntax

- `lldp tx-delay seconds`
- `no lldp tx-delay`

### Parameters

- *seconds* — Specifies the delay in seconds between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. (Range 1 - 8192 seconds)

### Default Configuration

The default value is 2 seconds.

### Command Modes

Global Configuration mode.

### Usage Guidelines

- It is recommended that the TxDelay would be less than 0.25 of the LLDP timer interval.

### Examples

The following example specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB to 10 seconds.

```
Console (config) # lldp tx-delay 10
```

## lldp optional-tlv

The `lldp optional-tlv` Interface Configuration mode command specifies which optional TLVs from the basic set should be transmitted. Use the `no` form of this command to revert to the default setting.

### Syntax

- `lldp optional-tlv tlv1 [tlv2 ... tlv5]`
- `no lldp optional-tlv`
  - *tlv* — Specifies TLV that should be included. Available optional TLVs are: `port-desc`, `sys-name`, `sys-desc`, `sys-cap`, `802.3-mac-phy`.

### Default Configuration

No optional TLV is transmitted.

### Command Modes

Interface Configuration (Ethernet) mode.

## User Guidelines

There are no user guidelines for this command.

## Example

The following example specifies which optional TLV (2)s from the basic set should be transmitted.

```
Console(config)# interface ethernet g5
Console(config-if)# lldp optional-tlv sys-name
```

## Ildp management-address

The `lldp management-address` Interface Configuration mode command specifies the management address that would be advertised from an interface. Use the **no** form of this command to stop advertising management address information.

## Syntax

- `lldp management-address ip-address`
- `no management-address`
  - *ip-address* — Specifies the management address to advertise.

## Default Configuration

No IP address is advertised.

## Command Modes

Interface Configuration (Ethernet) mode.

## User Guidelines

- Each port can advertise one IP address.
- Only static IP addresses can be advertised.

## Example

The following example specifies management address that would be advertised from an interface as 192.168.0.1.

```
Console(config)# interface ethernet g5
Console(config-if)# lldp management-address 192.168.0.1
```

## Ildp med enable

The `lldp med enable` Interface Configuration mode command enables Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) on an interface. Use the `no` form of this command to disable LLDP MED on an interface.

### Syntax

- `lldp med enable [tlv1 ... tlv3]`
- `no lldp med enable`
  - *tlv* — Specifies TLV that should be included. Available TLVs are: network-policy and location. The capabilities TLV is always included if LLDP-MED is enabled.

### Default Configuration

LLDP is disabled.

### Command Modes

Interface Configuration (Ethernet) mode.

### User Guidelines

There are no user guidelines for this command.

### Example

The following example enables Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) on an interface as network-policy.

```
Console(config)# interface ethernet g5
Console(config-if)# lldp med enable network-policy
```

## Ildp med network-policy (global)

The `lldp med network-policy` Global Configuration mode command defines LLDP MED network policy. Use the `no` form of this command to remove LLDP MED network policy.

## Syntax

- `lldp med network-policy number application [vlan id] [vlan-type {tagged | untagged}] [up priority] [dscp value]`
- `no lldp med network-policy number`
  - *number* — Network policy sequential number.
  - *application* — The name or the number of the primary function of the application defined for this network policy. Available application names are: voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling.
  - *vlan id* — VLAN identifier for the application.
  - *vlan-type* — Specifies if the application is using a ‘tagged’ or an ‘untagged’ VLAN.
  - *up priority* — User Priority (Layer 2 priority) to be used for the specified application.
  - *dscp value* — DSCP value to be used for the specified application.

## Default Configuration

No Network policy is defined.

## Command Modes

Global Configuration mode.

## User Guidelines

- Use the `lldp med network-policy` Interface Configuration command to attach a network policy to a port.
- Up to 32 network policies can be defined.

## lldp med network-policy (interface)

The `lldp med network-policy` Interface Configuration (Ethernet) mode command attaches a LLDP MED network policy to a port.

## Syntax

- `lldp med network-policy {add | remove} number`
  - *number* — Network policy sequential number.
  - *add* — Specifies **attach** to a port.
  - *remove* — Specifies **remove** from a porty.

## Default Configuration

No network policy is attached.



### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

There are no guidelines for this command.

## lldp med location

The **lldp med location** Interface Configuration mode command configures location information for the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) for an interface. Use the **no** form of this command to delete location information for an interface.

### Syntax

- **lldp med location coordinate** *data*
- **no lldp med location coordinate**
- **lldp med location civic-address** *data*
- **no lldp med location civic-address**
- **lldp med location ecs-elin** *data*
- **no lldp med location ecs-elin**
  - **coordinate** — The location is specified as coordinates.
  - **civic-address** — The location is specified as civic address.
  - **ecs-elin** — The location is specified as ECS ELIN.
  - **data** — The data format is as defined in ANSI/TIA 1057. Specifies the location as dotted hexadecimal data: Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon.

### Default Configuration

The location is not configured.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

There are no guidelines for this command.

### Example

The following example configures location information for the LLDP MED for an interface.

```
Console(config)# lldp med location coordinate data
```

## clear lldp rx

The `clear lldp rx` Privileged EXEC mode command restarts the LLDP RX state machine and clears the neighbors table.

### Syntax

- `clear lldp rx [ethernet interface]`
  - *interface* — Ethernet port

### Command Modes

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example restarts the LLDP RX state machine and clears the neighbors table.

```
console (config)# clear lldp rx
```

## show lldp configuration

The `show lldp configuration` privileged EXEC mode command displays the Link Layer Discovery Protocol (LLDP) configuration.

### Syntax

- `show lldp configuration [ethernet interface]`
  - *Interface* — Ethernet port

### Command Modes

Privileged EXEC mode.

### User Guidelines

There are no user guidelines for this command.

### Example

The following example displays the Link Layer Discovery Protocol (LLDP) configuration.

```
Console# show lldp configuration

LLDP state: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds

Port      State                Optional TLVs        Addres
-----  -----
g1        Rx and Tx
g2        Rx and Tx
g3        Rx and Tx
```

## show lldp local

The `show lldp local` Privileged EXEC mode command displays the Link Layer Discovery Protocol (LLDP) information advertised from a specific port.

### Syntax

- `show lldp local ethernet interface`
  - *interface* — Ethernet interface

### Command Modes

Privileged EXEC mode.

### User Guidelines

There are no user guidelines for this command.

## Example

The following example displays the Link Layer Discovery Protocol (LLDP) information that is advertised from port g1.

```
Switch# show lldp local ethernet g1
Device ID: 0060.704C.73FF
Port ID: 1
Capabilities: Bridge
System Name: ts-7800-1
System description:
Port description:
Management address: 172.16.1.8
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex,
1000BASE-T full duplex
Operational MAU type: 1000BaseTFD
LLDP-MED capabilities: Network Policy, Location Identification
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice
Flags: Tagged VLAN
VLAN ID: 2
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
Device Type: Power Sourcing Entity
Power source: Primary Power Source
Power priority: High
Power value: 9.6 Watts
LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01
```

## show lldp neighbors

The `show lldp neighbors` Privileged EXEC mode command displays information about neighboring devices discovered using Link Layer Discovery Protocol (LLDP).

### Syntax

- `show lldp neighbors [ethernet interface]`
  - *interface* — Ethernet interface

### Command Modes

Privileged EXEC mode.

### User Guidelines

There are no user guidelines for this command.

### Example

The following example displays information about neighboring devices discovered using Link Layer Discovery Protocol (LLDP).

```
Console# show lldp neighbors
```

Port	Device ID	Port ID	System Name	Capabilities
----	-----	-----	-----	-----
g1	0060.704C.73FE	1	ts-7800-2	B
g1	0060.704C.73FD	1	ts-7800-2	B
g2	0060.704C.73FC	9	ts-7900-1	B, R
g3	0060.704C.73FB	1	ts-7900-2	W

```
LLDP-MED Inventory
Hardware revision: 2.1
Firmware revision: 2.3
Software revision: 2.7.1
Serial number: LM759846587
Manufacturer name: VP
Model name: TR12
Asset ID: 9
```

## show lldp med configuration

The `show lldp med configuration` Privileged EXEC mode command displays the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) configuration.

### Syntax

- `show lldp med configuration [ethernet interface]`
  - *interface* — Ethernet port.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

There are no guidelines for this command.

### Example

The following example displays the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) configuration.

```
Switch# show lldp med configuration
Network policy 1
-----
Application type: Voice
VLAN ID: 2 tagged
Layer 2 priority: 0
DSCP: 0

Port          Capabilities  Network Policy  Location  PoE
-----
g1            Yes           Yes: 1          Yes       Yes
g2            Yes           Yes: 1          Yes       Yes
g3            Yes           No              No        Yes

Switch# show lldp med configuration ethernet g1

Port          Capabilities  Network Policy  Location  PoE
-----
g1            Yes           Yes: 1          Yes       Yes
```





# Management ACL

## management access-list

The **management access-list** Global Configuration mode command defines an Access-List for management, and enters the Access-List for configuration. Once in the Access-List Configuration mode, the denied or permitted access conditions are configured with the **deny** and **permit** commands. Use the **no** form of this command to remove an Access List.

### Syntax

- **management access-list** *name*
- **no management access-list** *name*
  - *name* — The Access List name using up to 32 characters.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- This command enters the Access List Configuration mode, where the denied or permitted access conditions with the **deny** and **permit** commands must be defined.
- If no match criteria are defined the default is "deny".
- If reentering to an Access-List context, the new rules are entered at the end of the Access-List.
- Use the **management access-class** command to select the active Access-List.
- The active management list cannot be updated or removed.
- Management ACL requires a valid management interface (valid IFindex). A valid management interface is an interface with an IP address. A valid (IFindex) management interface can be a single port, VLAN or port-channel. Management ACL only restricts access to the device for management configuration or viewing.

## Examples

The following example shows how to create an Access-List called 'mlist', configure two management interfaces ethernet g1 and ethernet g9, and make the Access-List the active list.

```
Console (config)# management access-list mlist
Console (config-macl)# permit ethernet g1
Console (config-macl)# permit ethernet g9
Console (config-macl)# exit
Console (config)# management access-class mlist
```

The following example shows how to create an Access-List called 'mlist', configure all interfaces to be management interfaces except interfaces ethernet g1 and ethernet g9, and make the Access-List the active list.

```
Console (config)# management access-list mlist
Console (config-macl)# deny ethernet g1
Console (config-macl)# deny ethernet g9
Console (config-macl)# permit
Console (config-macl)# exit
Console (config)# management access-class mlist
```

## permit (management)

The `permit` Management Access-List Configuration mode command defines a permit rule.

### Syntax

- `permit [ethernet interface-number | vlan vlan-id | port-channel number] [service service]`
- `permit ip-source {ipv4-address | ipv6-address/prefix-length} [mask mask | prefix-length] [ethernet interface-number | vlan vlan-id | port-channel number] [service service]`
  - `ethernet interface-number` — A valid Ethernet port number.
  - `vlan vlan-id` — A valid VLAN number.
  - `port-channel number` — A valid port channel number.
  - `ipv4-address` — Source IPv4 address.
  - `ipv6-address/prefix-length` — Source IPv6 address and prefix length. The prefix length is optional.
  - `mask mask` — Specifies the network mask of the source IPv4 address. The parameter is relevant only to IPv4 addresses. (Range: Valid subnet mask)
  - `mask prefix-length` — Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). The parameter is relevant only to IPv4 addresses. (Range: 0 - 32)
  - `service service` — Indicates service type. Can be one of the following: `telnet`, `ssh`, `http`, `https` or `snmp`.

### Default Configuration

If no `permit` statement is present, the default is set to `deny`.

### Command Mode

Management Access-list Configuration mode.

### User Guidelines

- Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface. The system supports up to 256 management access rules.

### Example

The following example shows how all ports are permitted in the Access-List called 'mlist'.

```
Console (config)# management access-list mlist
Console (config-macl)# permit
```

## deny (management)

The `deny` Management Access-List Configuration mode command defines a deny rule.

### Syntax

- `deny` [`ethernet interface-number` | `vlan vlan-id` | `port-channel number`] [`service service`]
- `deny ip-source` {`ipv4-address` | `ipv6-address/prefix-length`} [`mask mask` | `prefix-length`] [`ethernet interface-number` | `vlan vlan-id` | `port-channel number`] [`service service`]
  - `ethernet interface-number` — A valid Ethernet port number.
  - `vlan vlan-id` — A valid VLAN number.
  - `port-channel number` — A valid port-channel number.
  - `ipv4-address` — Source IPv4 address.
  - `ipv6-address/prefix-length` — Source IPv6 address and prefix length. The prefix length is optional.
  - `mask mask` — Specifies the network mask of the source IPv4 address. The parameter is relevant only to IPv4 addresses. (Range: Valid subnet mask)
  - `mask prefix-length` — Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). The parameter is relevant only to IPv4 addresses. (Range: 0 - 32)
  - `service service` — Indicates service type. Can be one of the following: `telnet`, `ssh`, `http`, `https` or `snmp`.

### Default Configuration

This command has no default configuration.

### Command Mode

Management Access-list Configuration mode.

### User Guidelines

- Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface. The system supports up to 256 management access rules.

### Example

The following example shows how all ports are denied in the Access-List called 'mlist'.

```
Console (config)# management access-list mlist
Console (config-macl)# deny
```

## management access-class

The `management access-class` Global Configuration mode command defines which management Access-List is used. Use the `no` form of this command to disable restriction.

### Syntax

- `management access-class {console-only | name}`
- `no management access-class`
  - *name* — Name of the Access List. If unspecified, defaults to an empty Access-List. (Range: 1 - 32 characters)
  - `console-only` — The device can be managed only from the console.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures an Access-List called 'mlist' as the management Access-List.

```
Console (config)# management access-class mlist
```

## show management access-list

The `show management access-list` Privileged EXEC mode command displays management access-lists.

### Syntax

- `show management access-list [name]`
  - *name* — Name of the Access List. If unspecified, defaults to an empty Access-List. (Range: 1 - 32 characters)

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the active management Access-List.

```
Console# show management access-list
mlist
-----
permit ethernet g1
permit ethernet g9
! (Note: all other access implicitly denied)
```

## show management access-class

The show management access-class Privileged EXEC mode command displays the active management Access-List.

### Syntax

- show management access-class

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the management Access-List information.

```
Console# show management access-class
Management access-class is enabled, using access list mlist
```

# PHY Diagnostics Commands

## test copper-port tdr

The `test copper-port tdr` Privileged EXEC mode command diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.

### Syntax

- `test copper-port tdr interface`
  - *interface* — A valid Ethernet port.

### Default Configuration


This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- The port under test should be conducted when the fiber link is down.

 **NOTE:** The maximum distance VCT can function is 120 meters.

### Examples

The following example results in a report on the cable attached to port g3.

```
Console# test copper-port tdr g3
Cable is open at 100 meters
```

## show copper-ports tdr

The `show copper-ports tdr` Privileged EXEC mode command display the last TDR (Time Domain Reflectometry) tests on specified ports.

### Syntax

- `show copper-ports tdr [interface]`
  - *interface* — A valid Ethernet port.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the last TDR (Time Domain Reflectometry) tests on all ports.

```
Console# show copper-ports tdr
```

Port	Result	Length [meters]	Date
g1	OK		
g2	Short	50	13:32:00 23 July 2003
g3	Test has not been performed		
g4	Short	128	13:32:00 23 July 2003
g5	Fiber	-	-

## show copper-ports cable-length

The `show copper-ports cable-length` Privileged EXEC mode command displays the estimated copper cable length attached to a port.

### Syntax

- `show copper-ports cable-length [interface]`
  - *interface* — A valid Ethernet port.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.



### User Guidelines

- The port must be active and working in 1000M.

### Example

The following example displays the estimated copper cable length attached to all ports.

```
Console# show copper-ports cable-length

Port          Length [meters]
----          -
g1            < 50
g2            Giga link not active
g3            110-140
```

## show fiber-ports optical-transceiver

The `show fiber-ports optical-transceiver` Privileged EXEC mode command displays the optical transceiver diagnostics.

### Syntax

- `show fiber-ports optical-transceiver` [*interface*] [*detailed*]
  - *interface* — A valid Ethernet port.
  - *detailed* — Detailed diagnostics.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- To test optical transceivers, ensure a fiber link is up. The test is only supported on Dell supported SFP modules.

## Examples

The following example displays the optical transceiver diagnostics.

```
console# show fiber-ports optical-transceiver
```

Port	Temp	Voltage	Current Power	Output Power	Input Power	LOS
g3	Copper					
g21	W	OK	E	OK	OK	OK
g22	OK	OK	OK	OK	OK	OK

Temp - Internally measured transceiver temperature.  
Voltage - Internally measured supply voltage.  
Current - Measured TX bias current.  
Output Power - Measured TX output power.  
Input Power - Measured RX received power.  
LOS - Loss of signal

The following example displays detailed optical transceiver diagnostics.

```
console# show fiber-ports optical-transceiver detailed
```

Port	Temp [C]	Voltage [Volt]	Current [mA]	Output Power [mWatt]	Input Power [mWatt]	LOS
---	-----	-----	-----	-----	-----	---
g23	70	7.27	0.79	3.30	2.50	No
g21	70	7.24	0.78	2.20	2.49	No

Temp - Internally measured transceiver temperature.

Voltage - Internally measured supply voltage.

Current - Measured TX bias current.

Output Power - Measured TX output power.

Input Power - Measured RX received power.

LOS - Loss of signal



# Port Channel Commands

## interface port-channel

The **interface port-channel** Global Configuration mode command enters the Interface Configuration mode of a specific port-channel.

### Syntax

- **interface port-channel** *port-channel-number*
  - *port-channel-number* — A valid port-channel trunk index.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- Eight aggregated links can be defined with up to 8 member ports per port channel. Turning off auto-negotiation of an aggregate link may, under some circumstances, make it non-operational. If the other side has auto-negotiation turned on, it may re-synchronize all members of the aggregated link to half-duplex operation, and may, as per the standards, set them all to inactive.

### Example

The following example enters the context of port-channel number 1.

```
Console (config)# interface port-channel 1
```

## interface range port-channel

The **interface range port-channel** Global Configuration mode command enters the Interface Configuration mode to configure multiple port-channels.

## Syntax

- **interface range port-channel** {*port-channel-range* | *all*}
- *port-channel-range* — List of port-channels to configure. Separate non-consecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels.
- **all** — All the channel-ports.

## Default Configuration

This command has no default configuration.

## Command Mode

Global Configuration mode.

## User Guidelines

- Commands under the interface range context are executed independently on each interface in the range: If the command returns an error on one of the interfaces, it will not stop the execution of the command on other interfaces.

## Example

The following example shows how port-channels 1, 2 and 8 are grouped to receive the same command.

```
Console (config)# interface range port-channel 1-2  
Console (config-if)#
```

# channel-group

The **channel-group** Interface Configuration mode command associates a port with a port-channel. Use the **no** form of this command to remove a port from a port channel.

## Syntax

- **channel-group** *port-channel-number* **mode** {**on** | **auto**}
- **no channel-group**
  - *port-channel\_number* — Specifies the number of the valid port-channel for the current port to join.
  - **on** — Forces the port to join a channel.
  - **auto** — Allows the port to join a channel as a result of an LACP operation.

## Default Configuration

The port is not assigned to any port-channel.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows how port g5 is configured to port-channel number 1 without LACP.

```
Console (config)# interface ethernet g5
Console (config-if)# channel-group 1 mode on
```

## port-channel load-balance

The **port-channel load-balance** Global Configuration mode command configures the load balancing policy of the port channeling. Use the **no** form of this command to reset to default.

### Syntax

- **port-channel load-balance** {layer-2 | layer-3 | layer-2-3}
- **no port-channel load-balance**
  - **layer-2** — Port channel load balancing is based on layer 2 parameters.
  - **layer-3** — Port channel load balancing is based on layer 3 parameters.
  - **layer-2-3** — Port channel load balancing is based on layer 2 and layer 3 parameters.

### Default Configuration

Layer 2.

### Command Modes

Global Configuration mode.

### User Guidelines

- In L2+L3 load balancing policy, fragmented packets might be reordered.

### Example

The following example configures the load balancing policy of the port channeling on layer 2.

```
Console (config) # port-channel load-balance layer-2
```

## show interfaces port-channel

The `show interfaces port-channel` Privileged EXEC mode command shows Port channel information.

### Syntax

- `show interfaces port-channel [port-channel-number]`
  - *port\_channel\_number* — Number of the Port channel to display. (Range: Valid port channel)

### Default Configuration

This command has no default configuration.

### Command Modes

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows how all port channel information is displayed.

```
Console# show interfaces port-channel

Load balancing: Layer2 and Layer 3.

Channel          Ports
-----          -
1                Active: 1, 2
2                Active: 2, 7
3                Active: 3, 8
```



# Port Monitor Commands

## port monitor

The **port monitor** Interface Configuration mode command starts a port monitoring session. Use the **no** form of this command to stop a port monitoring session.

### Syntax

- **port monitor** *src-interface* [**rx** | **tx**]
- **no port monitor** *src-interface*
  - *src-interface* — Valid Ethernet port or port-channel number.
  - **rx** — Monitors received packets only. If no option specified, monitors both rx and tx.
  - **tx** — Monitors transmitted packets only. If no option specified, monitors both rx and tx.

### Default Configuration

The default is both **rx** and **tx**.

### Command Mode

Interface Configuration mode.

### User Guidelines

- This command enables traffic on one port to be copied to another port, or between the source port (*src-interface*) and a destination port (the port being configured). Only a single target port can be defined per system.
- The port being monitored cannot be set faster than the monitoring port.

- The following restrictions apply to ports configured to be destination ports:
  - The port cannot be already configured as a source port.
  - The port cannot be a member in a port-channel.
  - An IP interface is not configured on the port.
  - GVRP is not enabled on the port.
  - The port is not a member in any VLAN, except for the default VLAN (will automatically be removed from the default VLAN).
- The following restrictions apply to ports configured to be source ports:
  - Port monitoring Source Ports must be simple ports, and not port-channels.
  - The port cannot be already configured as a destination port.
  - All the frames are transmitted as either always tagged or always untagged.

General Restrictions:

- Ports cannot be configured as a group using the **interface range ethernet** command.



**NOTE:** The Port Mirroring target must be a member of the Ingress VLAN of all Mirroring source ports. Therefore, Multicast and Broadcast frames in these VLANs are seen more than once. (Actually N, where N equals four).

When both transmit (Tx) and receive (Rx) directions of more than one port are monitored, the capacity may exceed the bandwidth of the target port. In this case, the division of the monitored packets may not be equal. The user is advised to use caution in assigning port monitoring.

### Example

The following example shows how traffic on port g8 (source port) is copied to port g1 (destination port).

```
Console(config)# interface ethernet g1
Console(config-if)# port monitor g8
```

## show ports monitor

The show ports monitor User EXEC mode command displays the port monitoring status.

### Syntax

- show ports monitor

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows how the port copy status is displayed.

```
Console# show ports monitor
```

Source Port	Destination Port	Type	Status
g1	g8	RX, TX	Active
g2	g8	RX, TX	Active
g18	g8	Rx	Active



# QoS Commands

## qos

The `qos` Global Configuration mode command enables quality of service (QoS) on the device and enters QoS basic mode. Use the `no` form of this command to disable the QoS features on the device.

### Syntax

- `qos`
- `no qos`

### Default Configuration

There is no default configuration for this command.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows how QoS is enabled on the device, in basic mode.

```
Console(config)# qos
```

## show qos

The `show qos` User EXEC mode command displays the quality of service (QoS) mode for the entire device.

### Syntax

- `show qos`  
This command has no arguments or keywords.

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays a QoS mode.

```
Console#show qos
Qos: disabled
Trust: dscp
```

## wrr-queue cos-map

The `wrr-queue cos-map` Global Configuration mode command maps assigned CoS values to select one of the egress queues. Use the `no` form of this command to return to the default values.

### Syntax

- `wrr-queue cos-map queue-id cos1...cos8`
- `no wrr-queue cos-map [queue-id]`
  - *queue-id* — The queue number to which the following CoS values are mapped.
  - *cos1...cos8* — Map to specific queues up to eight CoS values from 0 to 7.

### Default Configuration

The map default values for 8 queues:

- Cos0 is mapped to queue 3
- Cos1 is mapped to queue 1
- Cos2 is mapped to queue 2
- Cos3 is mapped to queue 4
- Cos4 is mapped to queue 5
- Cos5 is mapped to queue 6
- Cos6 is mapped to queue 7
- Cos7 is mapped to queue 8

### Command Mode

Global Configuration mode.

## User Guidelines

- You can use this command to distribute traffic into different queues, where each queue is configured with different weighted round robin (WRR) parameters.
- To enable the expedite queues, use the **priority-queue out** Interface Configuration mode command **wrr-queue cos-map**.

## Example

The following example maps CoS 3 to queue 4.

```
Console(config)# wrr-queue cos-map 4 3
```

## wrr-queue bandwidth

The **wrr-queue bandwidth** Interface Configuration mode command assigns Weighted Round Robin (WRR) weights to egress queues. The weights ratio determines the frequency in which the packet scheduler dequeues packets from each queue. Use the **no** form of this command to return to the default values.

## Syntax

- **wrr-queue bandwidth** *weight1 weight2 ... weight\_n*
- **no wrr-queue bandwidth**
  - *weight1...weight\_n* — Sets the bandwidth ratio by the WRR packet scheduler for the packet queues. Separate each value by spaces. (Range: 0 - 254)

## Default Configuration

The default WRR weight ratio is 1:2:8:16:32:64:128:255.

## Command Mode

Interface Configuration (Ethernet, port channel) mode.

## User Guidelines

- The ratio for each queue is defined by the queue weight divided by the sum of all queue weights (i.e., the normalized weight). This actually sets the bandwidth allocation of each queue.
- A weight of 0 means no bandwidth is allocated for the same queue, and the share bandwidth is divided among the remaining queues.
- All 8 queues are participating excluding the queues that are assigned as expedite queues. The weights of these queues are ignored in the ratio calculation.
- All 8 queues participate in the WRR exclude the expedite queues, in which case the corresponded weight is ignored (not used in the ratio calculation). The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced.

## Example

The following example assigns WRR weights to egress queues.

```
Console(config)# priority-queue num-of-queues 1
Console(config)# interface ethernet g1
Console(config-if)# wrr-queue bandwidth 20 30 50

Console(config)# priority-queue num-of-queues 0
Console(config)# interface ethernet g3
Console(config-if)# wrr-queue bandwidth 20 30 50 10
```

## priority-queue out num-of-queues

The `priority-queue out num-of-queues` Global Configuration mode command enables the egress queues to be expedite queues. Use the `no` form of this command to return to the default values.

### Syntax

- `priority-queue out num-of-queues number-of-queues`
- `no priority-queue out num-of-queues`
  - *number-of-queues* — Assign the number of queues to be expedite queues. The expedite queues would be the queues with higher indexes. (Range: 0 - 8)

### Default Configuration

All queues are expedite queues.

### Command Mode

Global Configuration mode.

### User Guidelines

- When configuring the `priority-queue out num-of-queues` command, the weighted round robin (WRR) weight ratios are affected because there are fewer queues participating in WRR.
- Queue 8 is taken as the highest index queue. Queue 7 is taken as the next highest queue. If four queues are selected then queues 8, 7, 6, and 5 are used, leaving queues 4, 3, 2, and 1 for WRR..



### Example

The following example sets queue 8, 7 to be expedite queues.

```
Console (config)# priority-queue out num-of-queues 2
```

## traffic-shape

The **traffic-shape** Interface Configuration (Ethernet, Port-Channel) mode command sets the shaper on an egress port. Use the **no** form of this command to disable the shaper.

### Syntax

- **traffic-shape** *committed-rate* [*committed -burst*]
- **no traffic-shape**
  - *committed-rate* — Specifies the average traffic rate (CIR) in kbps. (Range for GE ports is 64 - 1,000,000 kbps)
  - *committed-burst* — Specifies the excess burst size (CBS) in bytes. (Range for GE ports is 4KB – 16MB)

### Default Configuration

The default configuration is disabled.

### Command Mode

Interface Configuration (Ethernet, Port-Channel) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example sets the shaper on Ethernet port 1/g15 to 64kbps committed rate.

```
console(config)# interface ethernet g/g15  
console(config-if) traffic-shape 64
```

## rate-limit (Ethernet)

The **rate-limit** Interface Configuration (Ethernet) mode command limits the rate of the incoming traffic. Use the **no** form of this command to disable the rate limit.

## Syntax

- `rate-limit rate`
- `no rate-limit`
  - *rate* — Specifies the maximum of kilobits per second of ingress traffic on a port. (Range: 3.5M – 1G)

## Default Configuration

The default configuration is disabled.

## Command Mode

Interface Configuration (Ethernet) mode.

## User Guidelines

- The command can be enabled on a specific port only if `port storm-control broadcast enable` Interface Configuration command is not enabled on that port.

Note: For PowerConnect 5400 devices, the calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPC).

## Example

The following example limits the rate of the incoming traffic on Ethernet port 1/g15 to 1000kpbs.

```
console(config)# interface ethernet 1/g15
console(config-if) rate-limit 1000
```

## show qos interface

The `show qos interface` User EXEC mode command displays interface QoS data.

## Syntax

- `show qos interface [queuing | shapers | rate-limit] [ethernet interface-number | port-channel number]`
  - `queuing` — Displays the queue's strategy (WRR or EF) and the weight for WRR queues and the CoS to queue map and the EF priority.
  - `shapers` — Displays the shaper of the specified interface and the shaper for the queue on the specified interface.
  - `rate-limit` — Displays the rate-limit configuration.
  - `ethernet interface-number` — Valid Ethernet port number.
  - `port-channel number` — Valid port-channel number.

## Default Configuration

There is no default configuration for this command.

## Command Mode

User EXEC mode.

## User Guidelines

If no keyword is specified with the `show qos interface` command, the port QoS mode (DSCP trusted, CoS trusted, untrusted), default CoS value, attached to the port, attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

## Examples

The following example displays output from the `show qos interface g1 queuing` command.

```
Console# show qos interface ethernet g1 queuing
Ethernet  g1
wrr bandwidth weights and EF priority:

qid      weights      Ef      Priority
1        125          dis    N/A
2        125          dis    N/A
3        125          dis    N/A
4        125          dis    N/A

Cos-queue map:
cos      qid
0        2
1        1
2        1
3        2
4        3
5        3
6        4
7        4
```

## qos map dscp-queue

The `qos map dscp-queue` Global Configuration mode command modifies the DSCP to queue map. Use the `no` form of this command to return to the default map.

### Syntax

- `qos map dscp-queue dscp-list to queue-id`
- `no qos map dscp-queue [dscp-list ]`
  - *dscp-list* — Specify up to 8 DSCP values, separate each DSCP with a space. (Range: 0 - 63)
  - *queue-id* — Enter the queue number to which the DSCP value corresponds.

### Default Configuration

The following table describes the default map.

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-56	57-63
Queue-ID	1	2	3	4	5	6	7	8

### Command Mode

Global Configuration mode.

### User Guidelines

- Queue settings for 3, 11, 19, ... cannot be modified.

### Example

The following example maps DSCP values 33, 40 and 41 to queue 1.

```
Console (config)# qos map dscp-queue 33 40 41 to 1
```

## qos trust (Global)

The `qos trust` Global Configuration mode command can be used to configure the system to "trust" state. Use the `no` form of this command to return to the default state.

### Syntax

- `qos trust {cos | dscp}`
- `no qos trust`
  - `cos` — Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS is used.
  - `dscp` — Classifies ingress packets with the packet DSCP values.

### Default Configuration

CoS is the default trust mode.

### Command Mode

Global Configuration mode.

### User Guidelines

- Packets entering a quality of service (QoS) domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain.
- Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.
- To return to the untrusted state, use the **no qos** command to apply best effort service.

### Example

The following example configures the system to DSCP trust state.

```
Console (config)# qos trust dscp
```

## qos trust (Interface)

The **qos trust** Interface Configuration mode command enables each port trust state. Use the **no** form of this command to disable the trust state on each port.

### Syntax

- **qos trust**
- **no qos trust**

### Default Configuration

Each port is enabled.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- Use **no qos trust** to disable the trust mode on each port.  
Use **qos trust** to enable trust mode on each port.

### Example

The following example configures port g5 to default trust state (CoS).

```
Console (config)# interface ethernet g5
Console (config-if) qos trust
```

## qos cos

The `qos cos` Interface Configuration mode command configures the default port CoS value. Use the `no` form of this command to return to the default setting.

### Syntax

- `qos cos default-cos`
- `no qos cos`
  - *default-cos* — Specifies the default CoS value being assigned to the port. If the port is trusted and the packet is untagged then the default CoS value becomes the CoS value. (Range: 0 - 7)

### Default Configuration

Port CoS is 0.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- You can use the default value to assign a CoS value to all untagged packets entering the port.

### Example

The following example configures port g5 default CoS value to 3.

```
Console (config)# interface ethernet g5
Console (config-if) qos cos 3
```

## show qos map

The `show qos map` User EXEC mode command displays all the QoS maps. (CHECK WITH MARY)

### Syntax

- `show qos map [dscp-queue]`
  - *dscp-queue* — Displays the DSCP to queue map.

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode .

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the DSCP port-queue map.

```
console# show qos map
Dscp-queue map:
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 :    01 01 01 01 01 01 01 01 01 01 01
1 :    01 01 01 01 01 01 02 02 02 02
2 :    02 02 02 02 02 02 02 02 02 02
3 :    02 02 03 03 03 03 03 03 03 03
4 :    03 03 03 03 03 03 03 03 04 04
5 :    04 04 04 04 04 04 04 04 04 04
6 :    04 04 04 04
```

The following table describes the fields used above.

Column	Description
D1	Decimal Bit 1 of DSCP
D2	Decimal Bit 2 of DSCP
01 - 04	Queue numbers

$$(D1 \times 10) + D2 = \text{Value of DSCP}$$





# Radius Commands

## radius-server host

The `radius-server host` Global Configuration mode command specifies a RADIUS server host. Use the `no` form of this command to delete the specified RADIUS host.

### Syntax

- `radius-server host {ip-address | hostname} [auth-port auth-port-number] [timeout timeout] [retransmit retransmit] [deadtime deadtime] [key key] [source source] [priority priority] [usage type]`  
`no radius-server host ip-address`
  - *ip-address* — IP address of the RADIUS server host.
  - *hostname* — Hostname of the RADIUS server host. (Range: 1 - 158 characters)
  - *auth-port-number* — Port number for authentication requests. The host is not used for authentication if set to 0. If unspecified, the port number defaults to 1812. (Range: 0 - 65535)
  - *timeout* — Specifies the timeout value in seconds. If no timeout value is specified, the global value is used. (Range: 1 - 30)
  - *retransmit* — Specifies the re-transmit value. If no re-transmit value is specified, the global value is used. (Range: 1 - 10)
  - *deadtime* — Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests. (Range: 0 - 2000)
  - *key* — Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. If no key value is specified, the global value is used. (Range: 1 - 128 characters)
  - *source* — Specifies the source IP address to use for the communication. If no retransmit value is specified, the global value is used. 0.0.0.0 is interpreted as request to use the IP address of the outgoing IP interface.
  - *priority* — Determines the order in which the servers are used, where 0 is the highest priority. (Range: 0 - 65535)
  - *type* — Specifies the usage type of the server. Can be one of the following values: **login**, **802.1x** or **all**. If unspecified, defaults to **all**.

### Default Configuration

By default, no RADIUS host is specified.

### Command Mode

Global Configuration mode.

### User Guidelines

- To specify multiple hosts, multiple **radius-server host** commands can be used.
- If no host-specific timeout, retransmit, deadtime or key values are specified, the global values apply to each host.
- The address type of the source parameter must be the same as the ip-address parameter.

### Example

The following example specifies a RADIUS server host with the following characteristics:

- Server host IP address — 192.168.10.1
- Authentication port number — 20
- Timeout period — 20 seconds

```
Console (config)# radius-server host 192.168.10.1 auth-port 20
timeout 20
```

## radius-server key

The **radius-server key** Global Configuration mode command sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon. Use the **no** form of this command to reset to the default.

### Syntax

- **radius-server key** [*key-string*]
- **no radius-server key**
  - *key-string* — Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. The key can be up to 128 characters long.

### Default Configuration

The default is an empty string.

### Command Mode

Global Configuration mode.

## User Guidelines

- There are no user guidelines for this command.

## Example

The following example sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon to "dell-server".

```
Console (config)# radius-server key dell-server
```

## radius-server retransmit

The **radius-server retransmit** Global Configuration mode command specifies the number of times the software searches the list of RADIUS server hosts. Use the **no** form of this command to reset the default configuration.

## Syntax

- **radius-server retransmit** *retries*
- **no radius-server retransmit**
  - *retries* — Specifies the retransmit value. (Range: 1 - 10)

## Default Configuration

The default is 3 attempts.

## Command Mode

Global Configuration mode.

## User Guidelines

- There are no user guidelines for this command.

## Example

The following example configures the number of times the software searches the list of RADIUS server hosts to 5 attempts.

```
Console (config)# radius-server retransmit 5
```

## radius-server source-ip

The **radius-server source-ip** Global Configuration mode command specifies the source IP address used for communication with RADIUS servers. Use the **no** form of this command to return to the default.

### Syntax

- **radius-server source-ip** *source*
- **no radius source-server-ip** *source*
  - *source* — Specifies the source IP address.

### Default Configuration

The default IP address is the outgoing IP interface.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the source IP address used for communication with RADIUS servers to 10.1.1.1.

```
Console (config)# radius-server source-ip 10.1.1.1
```

## radius-server source-ipv6

The **radius-server source-ipv6** Global Configuration mode command specifies the source IPv6 address used for the IPv6 communication with RADIUS servers. Use the **no** form of this command to return to the default.

### Syntax

- **radius-server source-ipv6** *source*
- **no radius-server source-ipv6** *source*
  - *source* — Specifies the source IPv6 address.

### Default Configuration

The default IP address is the outgoing IP interface.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the source IPv6 address used for communication with RADIUS servers.

```
Console (config)# radius-server source-ipv6 3156::98
```

## radius-server timeout

The **radius-server timeout** Global Configuration mode command sets the interval for which a device waits for a server host to reply. Use the **no** form of this command to restore the default.

### Syntax

- **radius-server timeout** *timeout*
- **no radius-server timeout**
  - *timeout* — Specifies the timeout value in seconds. (Range: 1 - 30)

### Default Configuration

The default value is 3 seconds.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example sets the interval for which a device waits for a server host to reply to 5 seconds.

```
Console (config)# radius-server timeout 5
```

## radius-server deadtime

The `radius-server deadtime` Global Configuration mode command improves RADIUS response times when servers are unavailable. The command is used to cause the unavailable servers to be skipped. Use the `no` form of this command to reset the default value.

### Syntax

- `radius-server deadtime deadtime`
- `no radius-server deadtime`
  - *deadtime* — Length of time in minutes, for which a RADIUS server is skipped over by transaction requests. (Range: 0 - 2000)

### Default Configuration

The default dead time is 0 minutes.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example sets a dead time where a RADIUS server is skipped over by transaction requests for this period, to 10 minutes.

```
Console (config)# radius-server deadtime 10
```

## show radius-servers

The `show radius-servers` User EXEC mode command displays the RADIUS server settings.

### Syntax

- `show radius-servers`

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

## User Guidelines

- There are no user guidelines for this command.

## Examples

The following example displays the RADIUS server settings.

```
Console# show radius-servers

IP address      Port      Time      Retransmit  Dead      Source     Priority  Usage
                Auth      Out
-----      -
172.16.1.1     1645     Global    Global      Global    Global     1        All
172.16.1.2     1645     11        8           Global    Global     2        All

Global values
-----
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IP: 172.16.8.1
```





# RMON Commands

## show rmon statistics

The `show rmon statistics` User EXEC mode command displays RMON Ethernet Statistics.

### Syntax

- `show rmon statistics {ethernet interface number | port-channel port-channel-number}`
  - *interface* — Valid Ethernet port.
  - *port-channel-number* — Valid port-channel trunk index.

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- The following RMON Groups are supported - Ethernet Statistics (Group1), History (Group 2), Alarms (Group 3) and Events (Group 4).

## Example

The following example displays RMON Ethernet Statistics for port g1.

```
Console# show rmon statistics ethernet g1
Port g1
Dropped: 8
Octets: 878128 Packets: 978
Broadcast: 7 Multicast: 1
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 98 65 to 127 Octets: 0
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

The following table describes the significant fields shown in the display:

Field	Description
Dropped	The total number of events in which packets are dropped by the probe due to lack of resources. This number is not always the number of packets dropped; it is the number of times this condition has been detected.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including bad packets, Broadcast packets, and Multicast packets) received.
Broadcast	The total number of good packets received and directed to the Broadcast address. This does not include Multicast packets.
Multicast	The total number of good packets received and directed to a Multicast address. This number does not include packets directed to the Broadcast address.
CRC Align Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize Pkts	The total number of packets received less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.

Oversize Pkts	The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	The total number of packets received less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Octets	The total number of packets (including bad packets) received and transmitted that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to 1518 Octets	The total number of packets (including bad packets) received that are between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

## rmon collection history

The **rmon collection history** Interface Configuration mode command enables a Remote Monitoring (RMON) MIB history statistics group on an interface. Use the **no** form of this command to remove a specified RMON history statistics group.

## Syntax

- **rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]
- **no rmon collection history** *index*
  - *index* — The requested statistics index group. (Range: 1 - 65535)
  - **owner** *ownername* — Records the RMON statistics group owner name. If unspecified, the name is an empty string.
  - **buckets** *bucket-number* — A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. (Range: 1 - 50)
  - **interval** *seconds* — The number of seconds in each polling cycle. If unspecified, defaults to 1800. (Range: 1 - 3600)

## Default Configuration

This command has no default configuration.

## Command Mode

Interface Configuration (Ethernet, port-channel) mode.

## User Guidelines

- This command cannot be executed on multiple ports using the **interface range ethernet** command.

## Example

The following example enables a Remote Monitoring (RMON) MIB history statistics group on port g8 with the index number "1" and a polling interval period of 2400 seconds.

```
Console (config)# interface ethernet g8
Console (config-if)# rmon collection history 1 interval 2400
```

## show rmon collection history

The **show rmon collection history** User EXEC mode command displays the requested history group configuration.

## Syntax

- **show rmon collection history** [**ethernet** *interface* | **port-channel** *port-channel-number*]
  - *interface* — Valid Ethernet port.
  - *port-channel-number* — Valid port-channel trunk index.

## Default Configuration

This command has no default configuration.

**Command Mode**

User EXEC mode.

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example displays all RMON group statistics.

```
Console# show rmon collection history
```

Index	Interface	Interval	Requested Samples	Granted Samples	Owner
1	1	1000	50	50	CLI

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

## show rmon history

The `show rmon history` User EXEC mode command displays RMON Ethernet Statistics history.

### Syntax

- `show rmon history index {throughput | errors | other} [period seconds]`
  - *index* — The requested set of samples. (Range: 1 - 65535)
  - *throughput* — Displays throughput counters.
  - *errors* — Displays error counters.
  - *other* — Displays drop and collision counters.
  - *period seconds* — Specifies the requested period time to display. (Range: 1 - 4294967295)

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example displays RMON Ethernet Statistics history for "throughput" on index number 5.

```
Console# show rmon history 5 throughput
Sample Set: 1                               Owner: CLI
Interface: g1                               Interval: 1800
Requested samples: 50                       Granted samples: 50

Maximum table size: 500

Time                Octets    Packets  Broadcast  Multicast  %
-----            -
Jan 18 2002 21:57:00 303595962 357568    3289       7287      19.98%
Jan 18 2002 21:57:30 287696304 275686    2789       2789      20.17%
```

The following example displays RMON Ethernet Statistics history for "errors" on index number 5.

```
Console# show rmon history 5 errors
Sample Set: 1                      Owner: CLI
Interface: g1                      Interval: 1800
Requested samples: 50              Granted samples: 50

Maximum table size: 500

Time                               CRC Align  Undersize  Oversize  Fragments  Jabbers
-----
Jan 18 2002                        1          1          49        0          0
21:57:00
Jan 18 2002                        1          1          27        0          0
21:57:30
```

The following example displays RMON Ethernet Statistics history for "other" on index number 5.

```
Console# show rmon history 5 other
Sample Set: 1                      Owner: CLI
Interface: g1                      Interval: 1800
Requested samples: 50              Granted samples: 50

Maximum table size: 500

Time                               Dropped    Collisions
-----
Jan 18 2002                        3          0
21:57:00
Jan 18 2002                        3          0
21:57:30
```

The following table describes the significant fields shown in the display:

<b>Field</b>	<b>Description</b>
Time	Date and Time the entry is recorded.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The number of packets (including bad packets) received during this sampling interval.
Broadcast	The number of good packets received during this sampling interval that were directed to the Broadcast address.
Multicast	The number of good packets received during this sampling interval that were directed to a Multicast address. This number does not include packets addressed to the Broadcast address.
Utilization%	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Oversize	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Fragments	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (AlignmentError). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.
Collisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.



## rmon alarm

The **rmon alarm** Global Configuration mode command configures alarm conditions. Use the **no** form of this command to remove an alarm.

### Syntax

- **rmon alarm** *index variable interval rthreshold fthreshold revent fevent* [**type type**] [**startup direction**] [*owner name*]
- **no rmon alarm** *index*
  - *index* — The alarm index. (Range: 1 - 65535)
  - *variable* — The object identifier of the particular variable to be sampled.
  - *interval* — The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. (Range: 1 - 2147483648)
  - *rthreshold* — Rising Threshold. (Range: 1 - 4294967295)
  - *fthreshold* — Falling Threshold. (Range: 1 - 4294967295)
  - *revent* — The Event index used when a rising threshold is crossed. (Range: 1 - 65535)
  - *fevent* — The Event index used when a falling threshold is crossed. (Range: 1 - 65535)
  - **type type** — The sampling method for the selected variable and calculating the value to be compared against the thresholds. If the method is **absolute**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the method is **delta**, the selected variable value at the last sample is subtracted from the current value, and the difference compared with the thresholds.
  - **startup direction** — The alarm that may be sent when this entry is first set to valid. If the first sample (after this entry becomes valid) is greater than or equal to the *rthreshold*, and *direction* is equal to **rising** or **rising-falling**, then a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to the *fthreshold*, and *direction* is equal to **falling** or **rising-falling**, then a single falling alarm is generated.
  - *owner name* — Enter a name that specifies who configured this alarm. If unspecified, the name is an empty string.

### Default Configuration

The following parameters have the following default values:

- **type type** — If unspecified, the type is **absolute**.
- **startup direction** — If unspecified, the startup direction is **rising-falling**.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the following alarm conditions:

- Alarm index — 1000
- Variable identifier — dell
- Sample interval — 360000 seconds
- Rising threshold — 1000000
- Falling threshold — 1000000
- Rising threshold event index — 10
- Falling threshold event index — 20

```
Console (config)# rmon alarm 1000 dell 360000 1000000 1000000 10 20
```

## show rmon alarm-table

The `show rmon alarm-table` User EXEC mode command displays the alarms summary table.

### Syntax

- `show rmon alarm-table`

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the alarms summary table.

```
Console# show rmon alarm-table
```

Index	OID	Owner
1	1.3.6.1.2.1.2.2.1.10.1	CLI
2	1.3.6.1.2.1.2.2.1.10.1	Manager
3	1.3.6.1.2.1.2.2.1.10.9	CLI

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

## show rmon alarm

The `show rmon alarm` User EXEC mode command displays alarm configuration.

### Syntax

- `show rmon alarm number`
  - *number* — Alarm index. (Range: 1 - 65535)

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

## Example

The following example displays RMON 1 alarms.

```
Console# show rmon alarm 1
Alarm 1
-----
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

The following table describes the significant fields shown in the display:

Field	Description
OID	Monitored variable OID.
Last Sample Value	The statistic value during the last sampling period. For example, if the sample type is delta, this value is the difference between the samples at the beginning and end of the period. If the sample type is absolute, this value is the sampled value at the end of the period.
Alarm	Alarm index.
Owner	The entity that configured this entry.
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	The method of sampling the variable and calculating the value compared against the thresholds. If the value is <b>absolute</b> , the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is <b>delta</b> , the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.

Startup Alarm	The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising and falling, then a single falling alarm is generated.
Rising Threshold	A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	The event index used when a rising threshold is crossed.
Falling Event	The event index used when a falling threshold is crossed.

## rmon event

The **rmon event** Global Configuration mode command configures an event. Use the **no** form of this command to remove an event.

### Syntax

- **rmon event** *index type* [**community text**] [**description text**] [**owner name**]
- **no rmon event** *index*
  - *index* — The event index. (Range: 1 - 65535)
  - *type* — The type of notification that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of **log**, an entry is made in the log table for each event. In the case of **trap**, an SNMP trap is sent to one or more management stations.
  - **community text** — If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string. (Range: 0-127 characters)
  - **description text** — A comment describing this event. (Range: 0-127 characters)
  - **owner name** — Enter a name that specifies who configured this event. If unspecified, the name is an empty string. (Range: 0-127 characters)

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures an event with the trap index of 10.

```
Console (config)# rmon event 10 log
```

## show rmon events

The `show rmon events` User EXEC mode command displays the RMON event table.

### Syntax

- `show rmon events`

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the RMON event table.

```
Console# show rmon events
```

Index	Description	Type	Community	Owner	Last time sent
1	Errors	Log		CLI	Jan 18 2002 23:58:17
2	High Broadcast	Log-Trap	device	Manager	Jan 18 2002 23:59:48

The following table describes the significant fields shown in the display:

<b>Field</b>	<b>Description</b>
Index	An index that uniquely identifies the event.
Description	A comment describing this event.
Type	The type of notification that the device generates about this event. Can have the following values: <b>none</b> , <b>log</b> , <b>trap</b> , <b>log-trap</b> . In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

## show rmon log

The `show rmon log` User EXEC mode command displays the RMON logging table.

### Syntax

- `show rmon log [event]`
  - *event* — Event index. (Range: 0 - 65535)

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the RMON logging table.

```
Console# show rmon log

Maximum table size: 500

Event      Description      Time
-----      -
1          Errors           Jan 18 2002 23:48:19
1          Errors           Jan 18 2002 23:58:17
2          High Broadcast   Jan 18 2002 23:59:48

Console# show rmon log

Maximum table size: 500 (800 after reset)

Event      Description      Time
-----      -
1          Errors           Jan 18 2002 23:48:19
1          Errors           Jan 18 2002 23:58:17
2          High Broadcast   Jan 18 2002 23:59:48
```

The following table describes the significant fields shown in the display:

Field	Description
Event	An index that uniquely identifies the event.
Description	A comment describing this event.
Time	The time this entry created.



## rmon table-size

The `rmon table-size` Global Configuration mode command configures the maximum RMON tables sizes. Use the `no` form of this command to return to the default configuration.

### Syntax

- `rmon table-size {history en.tries | log entries}`
- `no rmon table-size {history | log}`
  - `history entries` — Maximum number of history table entries. (Range: 20 - 32767)
  - `log entries` — Maximum number of log table entries. (Range: 20 - 32767)

### Default Configuration

History table size is 270.

Log table size is 200.

### Command Mode

Global Configuration mode.

### User Guidelines

- The configured table size is effective after the device is rebooted.

### Example

The following example configures the maximum RMON history table sizes to 1000 entries.

```
Console (config)# rmon table-size history 1000
```



# SNMP Commands

## snmp-server community

The `snmp-server community` command sets up the community access string to permit access to the Simple Network Management Protocol command. Use the `no` form of this command removes the specified community string.

### Syntax

- `snmp-server community` *community* [`ro` | `rw` | `su`] [*ipv4-address* | *ipv6-address*] [`view view-name`]
- `snmp-server community-group` *community group-name* [*ipv4-address* | *ipv6-address*]
- `no snmp-server community` *community* [*ipv4-address* | *ipv6-address*]
  - *community* — Community string that acts like a password and permits access to the SNMP protocol. (Range: 1- 20 characters)
  - `ro` — Specifies read-only access (Default)
  - `rw` — Specifies read-write access
  - `su` — Specifies SNMP administrator access
  - `view view-name` — Name of a previously defined view. The view defines the objects available to the community. It's not relevant for `su`, which has an access to the whole MIB. If unspecified, all the objects except of the community-table and SNMPv3 user and access tables are available. (Range: 1 - 30 characters)
  - *ipv4-address* — Management station IPv4 address. Default is all IP addresses.
  - *ipv6-address* — Management station IPv6 address. Default is all IP addresses.
  - *group-name* — Specifies the name of a group configured using the command 'snmp-server group' with v1 or v2 parameter (no specific order of the 2 command configurations). The group defines the objects available to the community. (Range: 1 - 30 characters)

### Default Configuration

There are no default communities defined.

### Command Mode

Global Configuration mode.

## User Guidelines

- The **view-name** parameter cannot be specified for **su**, which has access to the whole MIB.
- The **view-name** parameter can be used to restrict the access rights of a community string. When it is specified:
  - An internal security name is generated.
  - The internal security name for SNMPv1 and SNMPv2 security models is mapped to an internal group name.
  - The internal group name for SNMPv1 and SNMPv2 security models is mapped to a view-name (read-view and notify-view always, and for **rw** for write-view also)
- The **group-name** parameter can also be used to restrict the access rights of a community string. When it is specified:
  - An internal security name is generated.
  - The internal security name for SNMPv1 and SNMPv2 security models is mapped to the group name.
- The **no snmp-server community** command is used to remove a community or a community group.

## Examples

The following example sets up the community access string "public" to permit administrative access to SNMP protocol, at an administrative station with the IP address 192.168.1.20.

```
Console (config)# snmp-server community public su 192.168.1.20
```

## snmp-server view

The **snmp-server view** Global Configuration mode command creates or updates a view entry. Use the **no** form of this command to remove the specified Simple Network Management Protocol (SNMP) server view entry.

### Syntax

- **snmp-server view** *view-name oid-tree* {**included** | **excluded**}
- **no snmp-server view** *view-name* [*oid-tree*]
  - *view-name* — Label for the view record that you are updating or creating. The name is used to reference the record. (Range: 1 - 30 characters)
  - *oid-tree* — Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as *1.3.6.2.4*, or a word, such as *system*. Replace a single subidentifier with the asterisk (\*) wildcard to specify a subtree family; for example *1.3.\*.4*.
  - **included** — The view type is included.
  - **excluded** — The view type is excluded.

### Default Setting

'Default' and 'DefaultSuper' views exists.

### Command Mode

Global Configuration mode.

### User Guidelines

- You can enter this command multiple times for the same view record.
- The number of views is limited to 64.
- "Default" and "DefaultSuper" views exist. Those views are used by the software internally and can't be deleted or modified.

### Example

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
Console (config)# snmp-server view user-view system included
Console (config)# snmp-server view user-view system.7 excluded
Console (config)# snmp-server view user-view ifEntry.*.1 include
```

## snmp-server filter

The **snmp-server filter** Global Configuration mode command creates or updates a filter entry. Use the **no** form of this command to remove the specified Simple Network Management Protocol (SNMP) server filter entry.

Syntax

- **snmp-server filter** *filter-name* *oid-tree* {**included** | **excluded**}
- **no snmp-server filter** *filter-name* [*oid-tree*]
  - *filter-name* — Label for the filter record that you are updating or creating. The name is used to reference the record. (Range: Up to 30 characters).
  - *oid-tree* — Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as *1.3.6.2.4*, or a word, such as *system*. Replace a single subidentifier with the asterisk (\*) wildcard to specify a subtree family; for example *1.3.\*.4*.
  - **included** — The filter type is included.
  - **excluded** — The filter type is excluded.

### Default Configuration

There are no default communities defined.

### Command Modes

Global Configuration mode.

### User Guidelines

- You can enter this command multiple times for the same filter record. Later lines take precedence when an object identifier is included in two or more lines. .

### Example

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
Console (config)# snmp-server view user-view system included
Console (config)# snmp-server view user-view system.7 excluded
Console (config)# snmp-server view user-view ifEntry.*.1 included
```

## snmp-server contact

The `snmp-server contact` Global Configuration mode command sets up a system contact. To remove the system contact information, use the `no` form of the command.

### Syntax

- `snmp-server contact text`
- `no snmp-server contact`
  - *text* — Character string, up to 160 characters, describing the system contact information.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- Do not include spaces in the text string.

### Example

The following example displays setting up the system contact point as "Dell\_Technical\_Support".

```
Console (config)# snmp-server contact Dell_Technical_Support
```

## snmp-server location

The `snmp-server location` Global Configuration mode command sets up information on where the device is located. To remove the location string use, the `no` form of this command.

### Syntax

- `snmp-server location text`  
`no snmp-server location`
- *text* — Character string, up to 160 characters, describing the system location.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- Do not include spaces in the text string.

### Example

The following example sets the device location as "New\_York".

```
Console (config)# snmp-server location New_York
```

## snmp-server enable traps

The `snmp-server enable traps` Global Configuration mode command enables the switch to send SNMP traps. To disable SNMP traps use the `no` form of the command.

### Syntax

- `snmp-server enable traps`
- `no snmp-server enable traps`

### Default Configuration

Sending SNMP traps enabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

## Examples

The following example displays the command to enable SNMP traps.

```
Console (config)# snmp-server enable traps
```

## snmp-server trap authentication

The **snmp-server trap authentication** Global Configuration mode command enables the switch to send Simple Network Management Protocol traps when authentication fails. Use the **no** form of this command to disable SNMP authentication failed traps.

### Syntax

- snmp-server trap authentication
- no snmp-server trap authentication

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

## Examples

The following example displays the command to enable authentication failed SNMP traps.

```
Console (config)# snmp-server trap authentication
```

## snmp-server host

The **snmp-server host** Global Configuration mode command specifies the recipient of Simple Network Management Protocol notification operation. Use the **no** form of this command to remove the specified host.



## Syntax

- **snmp-server host** {*ip4-address* | *ip6-address* | *hostname*} *community-string* [**traps** | **informs**] [**1** | **2**] [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]
- **no snmp-server host** {*ip4-address* | *ip6-address* | *hostname*} [**traps** | **informs**]
  - *ip4-address* — The host IPv4 address (the targeted recipient).
  - *ip6-address* — The host IPv6 address (the targeted recipient). When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the usage guidelines for the interface name syntax.
  - *hostname* — Hostname of the host. (Range: 1 - 158 characters)
  - *community-string* — Password-like community string sent with the notification operation. (Range: 1 - 20 characters)
  - **traps** — Sends SNMP traps to this host (Default).
  - **informs** — Sends SNMP informs to this host. Not applicable to SNMPv1.
  - **1** — SNMPv1 traps will be used.
  - **2** — SNMPv2 traps will be used (Default).
  - **udp-port** *port* — UDP port of the host to use. The default is 162. (Range: 1 - 65535)
  - **filter** *filtername* — A string that is the name of the filter that define the filter for this host. If unspecified, does not filter anything. (Range: Up to 30 characters).
  - **timeout** *seconds* — Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range: 1 - 300)
  - **retries** *retries* — Maximum number of times to resend an inform request, when response is not received for generated message. The default is 3. (Range: 0 - 255)

## Default Configuration

This command has no default configuration.

## Command Mode

Global Configuration mode.

## User Guidelines

- The command logical key is the pair (ip-address/hostname, traps/informs).
- When configuring an SNMPv1 or SNMPv2 notification recipient, a notification view for that recipient is automatically generated for all the MIB.
- When configuring an SNMPv1 notification recipient, the **Inform** option cannot be selected.

- If a trap and inform are defined on the same target, and an inform was sent, the trap is not sent.
  - The IPv6Z address format: `<ipv6-link-local-address>%<interface-name>`
    - *interface-name* — `vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name> | 0`
    - *integer* — `<decimal-number> | <integer><decimal-number>`
    - *decimal-number* — `0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9`
    - *physical-port-name* — Designated port number, for example g1.
- If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is the same as not defining an egress interface.

### Example

The following example specifies the recipient of Simple Network Management Protocol notification operation.

```
Console (config)# snmp-server host 10.1.1.1 management 2
```

## snmp-server set

The `snmp-server set` Global Configuration mode command sets SNMP MIB value by the CLI.

### Syntax

- `snmp-server set variable-name name1 value1 [name2 value2 ...]`
  - *variable-name* — MIB variable name.
  - *name value* — List of name and value pairs. In case of scalar MIBs there is only a single pair of name values. In case of entry in a table the first pairs are the indexes, followed by one or more fields.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- Although the CLI can set any required configuration, there might be a situation where a SNMP user sets a MIB variable that does not have an equivalent command. In order to generate configuration files that support those situations, the `snmp-server set` command is used.
- This command is context sensitive.

## Examples

The following example sets the scalar MIB "sysName" to have the value "dell".

```
Console (config)# snmp-server set sysName sysname dell
```

The following example sets the entry MIB "rndCommunityTable" with keys 0.0.0.0 and "public". The field rndCommunityAccess gets the value "super" and the rest of the fields get their default values.

```
Console (config)# snmp-server set rndCommunityTable  
rndCommunityMngStationAddr 0.0.0.0 rndCommunityString public  
rndCommunityAccess super
```

## snmp-server group

The **snmp-server group** Global Configuration mode command configures a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views. Use the **no** form of this command to remove a specified SNMP group.

### Syntax

- **snmp-server group** *groupname* {v1 | v2 | v3 {noauth | auth | priv} [notify *notifyview* ] } [read *readview*] [write *writeview*]
- **no snmp-server group** *groupname* [v1 | v2 | v3 [noauth | auth | priv]]
  - *groupname* — The name of the group. (Range: Up to 30 characters)
  - v1 — SNMP Version 1 security model.
  - v2 — SNMP Version 2 security model.
  - v3 — SNMP Version 3 security model.
  - noauth — Specifies no authentication of a packet. Applicable only to SNMP Version 3 security model.
  - auth — Specifies authentication of a packet without encrypting it. Applicable only to SNMP Version 3 security model.
  - priv — Specifies authentication of a packet with encryption. Applicable only to SNMP Version 3 security model.
  - read *readview* — A string that is the name of the view that enables you only to view the contents of the agent. If unspecified, all the objects except of the community-table and SNMPv3 user and access tables are available. (Range: Up to 30 characters)
  - write *writeview* — A string that is the name of the view that enables you to enter data and configure the contents of the agent. If unspecified, nothing is defined for the write view. (Range: Up to 30 characters)
  - notify *notifyview* — A string that is the name of the view that enables you to specify an inform or a trap. If unspecified, nothing is defined for the notify view. (Range: Up to 30 characters)

## Default Configuration

No group entry exists.

## Command Mode

Global Configuration mode.

## User Guidelines

- The Router context is translated to "" context in the MIB.

## Example

The following example configures a new Simple Network Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views

```
Console (config)# snmp-server group user-group v3 priv read user-view
```

## snmp-server user

The `snmp-server user` Global Configuration mode command configures a new SNMP Version 3 user. Use the `no` form of the command to remove a user.

## Syntax

- `snmp-server user username groupname [remote engineid-string ] [ auth-md5 password | auth-sha password | auth-md5-key md5-des-keys | auth-sha-key sha-des-keys ]`  
`no snmp-server user username [remote engineid-string ]`
  - *username* — The name of the user on the host that connects to the agent. (Range: Up to 30 characters)
  - *groupname* — The name of the group to which the user belongs. (Range: Up to 30 characters)
  - *remote engineid-string* — Specifies the engine ID of remote SNMP entity to which the user belongs. The engine ID is concatenated hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. (Range: 5 - 32 characters)
  - *auth-md5* — The HMAC-MD5-96 authentication level. The user should enter password.
  - *auth-sha* — The HMAC-SHA-96 authentication level. The user should enter password.
  - *password* — A password (not to exceed 32 characters) for authentication and generation of DES key for privacy. (Range: Up to 30 characters)
  - *auth-md5-key* — The HMAC-MD5-96 authentication level. The user should enter authentication and privacy keys.

- *md5-des-keys* — Concatenated hexadecimal string of the MD5 key (MSB) and the privacy key (LSB). If authentication is only required you should enter 16 bytes, if authentication and privacy are required you should enter 32 bytes. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. (Range: 16 - 32 characters)
- **auth-sha-key** — The HMAC-SHA-96 authentication level. The user should enter authentication and privacy keys.
- *sha-des-keys* — Concatenated hexadecimal string of the SHA key (MSB) and the privacy key (LSB). If authentication is only required you should enter 20 bytes, if authentication and privacy are required you should enter 36 bytes. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. (Range: 20 - 36 characters)

#### Default Configuration

No group entry exists.

#### Command Mode

Global Configuration mode.

#### User Guidelines

- If **auth-md5** or **auth-sha** is specified, both authentication and privacy are enabled for the user. When you enter a **show running-config** command, you will not see a line for this user. To see if this user has been added to the configuration, type the **show snmp user** command.  
An SNMP EngineID should be defined in order to add users to the device.  
Changing or removing the value of `snmpEngineID` deletes the SNMPv3 users database.

#### Example

The following example configures a new SNMP Version 3 user.

```
Console (config)# snmp-server user
```

## snmp-server v3-host

The **snmp-server v3-host** Global Configuration mode command specifies the recipient of Simple Network Management Protocol Version 3 notifications. Use the **no** form of this command to remove the specified host.

## Syntax

- `snmp-server v3-host {ip4-address | ip6-address | hostname} | hostname} username [traps | informs] {noauth | auth | priv} [udp-port port] [filter filtername] [timeout seconds] [retries retries]`
- `no snmp-server v3-host {ip4-address | ip6-address | hostname} username [traps | informs]`
  - *ip4-address* — The host IPv4 address (the targeted recipient).
  - *ip6-address* — The host IPv6 address (the targeted recipient). When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the usage guidelines for the interface name syntax.
  - *hostname* — Specifies the name of the host. (Range:1-158 characters)
  - *username* — Specifies the name of the user to use to generate the notification. (Range: 1 - 24)
  - **traps** — Indicates that SNMP traps are sent to this host.
  - **informs** — Indicates that SNMP informs are sent to this host.
  - **noauth** — Indicates no authentication of a packet.
  - **auth** — Indicates authentication of a packet without encrypting it.
  - **priv** — Indicates authentication of a packet with encryption.
  - *port* — Specifies the UDP port of the host to use. If unspecified, the default UDP port number is 162. (Range: 1-65535)
  - *filtername* — Specifies a string that defines the filter for this host. If unspecified, nothing is filtered. (Range: 1-30 characters)
  - *seconds* — Specifies the number of seconds to wait for an acknowledgment before resending informs. If unspecified, the default timeout period is 15 seconds. (Range: 1-300)
  - *retries* — Specifies the maximum number of times to resend an inform request. If unspecified, the default maximum number of retries is 3. (Range: 0 - 255)

## Default Setting

This command has no default configuration.

## Command Mode

Global Configuration mode.

## User Guidelines

- The command logical key is the pair (ip-address/hostname, traps/informs).
  - A user and notification view are not automatically created. Use the **snmp-server user**, **snmp-server group** and **snmp-server view** Global Configuration mode commands to generate a user, group and notify group, respectively.
  - The IPv6Z address format: `<ipv6-link-local-address>%<interface-name>`
    - *interface-name* — **vlan**<integer> | **ch**<integer> | **isatap**<integer> | <physical-port-name> | 0
    - *integer* — <decimal-number> | <integer><decimal-number>
    - *decimal-number* — 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
    - *physical-port-name* — Designated port number, for example g1.
- If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is the same as not defining an egress interface.

## Example

The following example configures an SNMPv3 host.

```
Console(config)# snmp-server v3-host 192.168.0.20 john noauth
```

## snmp-server engineID local

The **snmp-server engineID local** Global Configuration mode command specifies the Simple Network Management Protocol (SNMP) engineID on the local device. Use the **no** form of this command to remove the configured engine ID.

## Syntax

- **snmp-server engineID local** {*engineid-string* | **default**}
- **no snmp-server engineID local**
  - *engineid-string* — Specifies a character string that identifies the engine ID. (Range: 5 - 32 characters)
  - **default** — The engine ID is created automatically based on the device MAC address.

## Default Setting

The engine ID is not configured.

If SNMPv3 is enabled using this command, and the default is specified, the default engine ID is defined per standard as:

- First 4 octets — first bit = 1, the rest is IANA Enterprise number.
- Fifth octet — set to 3 to indicate the MAC address that follows.
- Last 6 octets — MAC address of the device.

## Command Mode

Global Configuration mode.

## User Guidelines

- To use SNMPv3, you have to specify an engine ID for the device. You can specify your own ID or use a default string that is generated using the MAC address of the device.

If the SNMPv3 engine ID is deleted or the configuration file is erased, SNMPv3 cannot be used. By default, SNMPv1/v2 are enabled on the device. SNMPv3 is enabled only by defining the Local Engine ID.

If you want to specify your own ID, you do not have to specify the entire 32-character engine ID if it contains trailing zeros. Specify only the portion of the engine ID up to the point where just zeros remain in the value. For example, to configure an engine ID of 1234000000000000000000, you can specify `snmp-server engineID local 1234`.

Since the engine ID should be unique within an administrative domain, the following is recommended:

- For a standalone device, use the default keyword to configure the engine ID.
- For a stackable system, configure the engine ID and verify its uniqueness.

Changing the value of the engine ID has the following important side-effect. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The user's command line password is then destroyed, as required by RFC 2274. As a result, the security digests of SNMPv3 users become invalid if the local value of the engine ID change, and the users will have to be reconfigured.

You cannot specify an engine ID that consists of all 0x0, all 0xF or 0x000000001.

The **show running-config** Privileged EXEC mode command does not display the SNMP engine ID configuration. To see the SNMP engine ID configuration, enter the `snmp-server engine ID local` Global Configuration mode command.



### Example

The following example specifies the Simple Network Management Protocol (SNMP) engineID on the local device.

```
Console(config) # snmp-server engineID local default
```

## show snmp engineid

The `show snmp engineID` Privileged EXEC mode command displays the ID of the local Simple Network Management Protocol (SNMP) engine.

### Syntax

- `show snmp engineID`

### Default Setting

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the SNMP engine ID.

```
Console# show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
```

## show snmp

The `show snmp` Privileged EXEC mode command displays the SNMP status.

### Syntax

- `show snmp`

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the SNMP communications status.

```
console# sh snmp

Traps are enabled.
Authentication trap is enabled.

Version 1,2 notifications
Target      Type      Community Version  UDP Port  Filter  TO sec  Retries
Address                                           name
-----
Version 3 notifications
Target      Type      Username Security UDP Port  Filter  TO sec  Retries
Address                                           Level   name
-----
System Contact:

System Location:

console#
```

## show snmp views

The `show snmp views` Privileged EXEC mode command displays the configuration of views.

### Syntax

- `show snmp views [viewname]`
  - *viewname* — The name of the view. Range: Up to 30 characters

### Default Configuration

There is no default configuration for this command.

### Command Modes

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command

### Example

The following example displays the configuration of views use the show snmp views Privileged EXEC command.

```
Console # show snmp views
```

Name	OID Tree	Type
user-view	1.3.6.1.2.1.1	Included
user-view	1.3.6.1.2.1.1.7	Excluded
user-view	1.3.6.1.2.1.2.2.1.*.1	Included

## show snmp groups

The show snmp groups Privileged EXEC mode command displays the configuration of groups.

### Syntax

- show snmp groups [*groupname*]
  - *groupnam* — The name of the group.

### Default Configuration

There is no default configuration for this command.

### Command Modes

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the configuration of views use the show snmp views Privileged EXEC command.

```
Console # show snmp groups
```

Name	Security			Views		
	Model	Level	Context	Read	Write	Notify
user-group	V3	priv	-	Default		-
managers-group	V3	priv	-	Default	Default	-
managers-group	V3	priv	-	Default		-

```
Console # show snmp groups user-group
```

Name: user-group  
Security Model: V3  
Security Level: priv  
Security Context: -  
Read View: Default  
Write View: ""  
Notify View: ""

## show snmp filters

The show snmp filters Privileged EXEC mode command displays the configuration of filters.

### Syntax

- show snmp filters [*filtername*]
  - *filternam* — The name of the view. Range: Up to 30 character

## Default Configuration

There is no default configuration for this command.

## Command Modes

Privileged EXEC mode.

## User Guidelines

- There are no user guidelines for this command.

## Example

The following example displays the configuration of filters use the `show snmp filters` Privileged EXEC command.

```
Console # show snmp filters
```

Name	OID Tree	Type
user-filter	1.3.6.1.2.1.1	Included
user-filter	1.3.6.1.2.1.1.7	Excluded
user-filter	1.3.6.1.2.1.2.2.1.*.1	Included

## show snmp users

To display the configuration of groups use the `show snmp users` Privileged EXEC command.

## Syntax

- `show snmp users [username]`
  - *username* — The name of the user. Range: Up to 30 character

## Default Configuration

There is no default configuration for this command.

## Command Modes

Privileged EXEC mode.

## User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the configuration of groups use the `show snmp users` Privileged EXEC command.

```
Console # show snmp users

Name          group name          Auto Method      Remote
John          1.3.6.1.2.1.1      md5
John          1.3.6.1.2.1.1.7    md5              08009009020C0B099
                                                C075879

Console # show snmp users John

Name: John
Group name: user-group
Auth Method: md5
Remote:

Name: John
Group name: user-group
Auth Method: md5
Remote: 08009009020C0B099C075879
```

# Spanning-Tree Commands

## spanning-tree

The `spanning-tree` Global Configuration mode command enables spanning-tree functionality. Use the `no` form of this command to disable spanning-tree functionality.

### Syntax

- `spanning-tree`
- `no spanning-tree`

### Default Configuration

Spanning-tree is enabled.

### Command Modes

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enables spanning-tree functionality.

```
Console(config)# spanning-tree
```

## spanning-tree mode

The `spanning-tree mode` Global Configuration mode command configures the spanning-tree protocol. Use the `no` form of this command to return to the default configuration.

### Syntax

- `spanning-tree mode {stp | rstp | mstp}`
- `no spanning-tree mode`
  - `stp` — STP is the Spanning Tree operative mode.
  - `rstp` — RSTP is the Spanning Tree operative mode.
  - `mstp` — MSTP is enabled

### Default Configuration

STP configured.

### Command Modes

Global Configuration mode.

### User Guidelines

- In RSTP mode, the switch would use STP when the neighbor switch is using STP.
- In MSTP mode the switch would use RSTP when the neighbor switch is using RSTP, and would use STP when the neighbor switch is using STP

### Example

The following example configures the spanning-tree protocol to RSTP.

```
Console(config)# spanning-tree mode rstp
```

## spanning-tree forward-time

The `spanning-tree forward-time` Global Configuration mode command configures the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. Use the **no** form of this command to reset the default forward time.

### Syntax

- `spanning-tree forward-time seconds`
- `no spanning-tree forward-time`
  - *seconds* — Time in seconds. (Range: 4 - 30)

### Default Configuration

The default forwarding-time for IEEE Spanning-tree Protocol (STP) is 15 seconds.

### Command Modes

Global Configuration mode.



### User Guidelines

- When configuring the Forward-Time the following relationship should be kept:
  - $2 * (\text{Forward-Time} - 1) \geq \text{Max-Age}$

### Example

The following example configures spanning-tree bridge forward time to 25 seconds.

```
Console(config)# spanning-tree forward-time 25
```

## spanning-tree hello-time

The `spanning-tree hello-time` Global Configuration mode command configures the spanning-tree bridge hello time, which is how often the switch Broadcasts hello messages to other switches. Use the `no` form of this command to reset the default hello time.

### Syntax

- `spanning-tree hello-time` *seconds*
- `no spanning-tree hello-time`
  - *seconds* — Time in seconds. (Range: 1 - 10)

### Default Configuration

The default hello time for IEEE Spanning-Tree Protocol (STP) is 2 seconds.

### Command Modes

Global Configuration mode.

### User Guidelines

- When configuring the Hello-Time the following relationship should be kept:
  - $\text{Max-Age} \geq 2 * (\text{Hello-Time} + 1)$

### Example

The following example configures spanning-tree bridge hello time to 5 seconds.

```
Console(config)# spanning-tree hello-time 5
```

## spanning-tree max-age

The `spanning-tree max-age` Global Configuration mode command configures the spanning-tree bridge maximum age. Use the `no` form of this command to reset the default maximum age.

### Syntax

- `spanning-tree max-age seconds`
- `no spanning-tree max-age`
  - `seconds` -Time in seconds. (Range: 6 - 40)

### Default Configuration

The default max-age for IEEE STP is 20 seconds.

### Command Modes

Global Configuration mode

### User Guidelines

- When configuring the Max-Age the following relationships should be kept:
  - $2 * (\text{Forward-Time} - 1) \geq \text{Max-Age}$
  - $\text{Max-Age} \geq 2 * (\text{Hello-Time} + 1)$

### Example

The following example configures the spanning-tree bridge maximum-age to 10 seconds.

```
Console(config)# spanning-tree max-age 10
```

## spanning-tree priority

The `spanning-tree priority` Global Configuration mode command configures the spanning-tree priority. The priority value is used to determine which bridge is elected as the root bridge. Use the `no` form of this command to reset the default spanning-tree priority.

### Syntax

- `spanning-tree priority priority`
- `no spanning-tree priority`
  - `priority` — Priority of the bridge. (Range: 0 - 65535 in steps of 4096)

### Default Configuration

The default bridge priority for IEEE STP is 32768.

### Command Modes

Global Configuration mode.

### User Guidelines

- The priority value must be a multiple of 4096.
- The bridge with the lowest priority is elected to be the Root Bridge.

### Example

The following example configures spanning-tree priority to 12288.

```
Console(config)# spanning-tree priority 12288
```

## spanning-tree disable

The **spanning-tree disable** Interface Configuration mode command disables spanning-tree on a specific port. To enable spanning-tree on a port use, the **no** form of this command.

### Syntax

- **spanning-tree disable**
- **no spanning-tree disable**

### Default Configuration

By default, all ports are enabled for spanning-tree.

### Command Modes

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- When STP is disabled, the device will not forward STP BPDU's based on the Forward BPDU's setting.

### Example

The following example disables spanning-tree on g5.

```
Console (config)# interface ethernet g5  
Console (config-if)# spanning-tree disable
```

## spanning-tree cost

The **spanning-tree cost** Interface Configuration mode command configures the spanning-tree path cost for a port. Use the **no** form of this command to reset the default port path cost.

### Syntax

- **spanning-tree cost** *cost*
- **no spanning-tree cost**
  - *cost* — The port path cost. (Range: 1 - 200,000,000)

### Default Configuration

For the default short pathcost method, the cost values are: port channel - 4; 1000 mbps - 4; 100 mbps - 19; 10 mbps - 100.

### Command Modes

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- The method used (long or short) is set by using the **spanning-tree pathcost method** command.

### Example

The following example configures the spanning-tree cost on g5 to 35000.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree cost 35000
```

## spanning-tree port-priority

The **spanning-tree port-priority** Interface Configuration mode command configures port priority. Use the **no** form of this command to reset the default port priority.

### Syntax

- **spanning-tree port-priority** *priority*
- **no spanning-tree port-priority**
  - *priority* — The port priority. (Range: 0 - 240 in multiples of 16)

### Default Configuration

The default port-priority for IEEE STP is 128.

### Command Modes

Interface Configuration (Ethernet, port-channel) mode.

## User Guidelines

- There are no user guidelines for this command.

## Example

The following example configures the spanning priority on g5 to 96.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree port-priority 96
```

## spanning-tree portfast

The `spanning-tree portfast` Interface Configuration mode command enables PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire. Use the `no` form of this command to disable PortFast mode.

## Syntax

- `spanning-tree portfast`
- `no spanning-tree portfast`

## Default Configuration

PortFast mode is disabled.

## Command Modes

Interface Configuration (Ethernet, port-channel) mode.

## User Guidelines

- This feature should be used only with interfaces connected to end stations. Otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operations.

## Example

The following example enables PortFast on g5.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree portfast
```

## spanning-tree link-type

The `spanning-tree link-type` Interface Configuration mode command overrides the default link-type setting. Use the `no` form of this command to reset the default.

### Syntax

- `spanning-tree link-type {point-to-point | shared}`
- `no spanning-tree link-type`
  - `point-to-point` — Specifies the port link type as point-to-point.
  - `shared` — Specifies that the port link type is shared.

### Default Configuration

There is no default configuration for this command.

### Command Modes

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- The switch derives the link type of a port from the duplex mode. A full-duplex port is considered a point-to-point link, and a half-duplex port is considered a shared link.

### Example

The following example enables shared spanning-tree on `g5`.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree link-type shared
```

## spanning-tree mst priority

The `spanning-tree mst priority` Global Configuration mode command configures the device priority for the specified spanning-tree instance. Use the `no` form of this command to return to the default configuration.

### Syntax

- `spanning-tree mst instance-id priority priority`
- `no spanning-tree mst instance-id priority`
  - *instance-id* — Displays the ID of the spanning-tree instance. (Range: 1 - 15)
  - *priority* — Displays the device priority for the specified spanning-tree instance. (Range: 0 - 61440 in multiples of 4096)

### Default Setting

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

### Command Mode

Global Configuration mode.

### User Guidelines

- The device with the lowest priority is selected as the root of the spanning tree.

### Example

The following example configures the spanning tree priority of instance 1 to 4096.

```
Console (config) # spanning-tree mst 1 priority 4096
```

## spanning-tree mst max-hops

The `spanning-tree mst priority` Global Configuration mode command configures the number of hops in an MST region before the BPDU is discarded and the port information is aged out. Use the `no` form of this command to return to the default configuration.

### Syntax

- `spanning-tree mst max-hops hop-count`
- `no spanning-tree mst max-hops`
  - *hop-count* — Number of hops in an MST region before the BPDU is discarded. (Range: 1 - 40)

### Default Setting

The default number of hops is 20.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
Console (config) # spanning-tree mst max-hops 10
```

## spanning-tree mst port-priority

The `spanning-tree mst port-priority` Interface Configuration mode command configures port priority for the specified MST instance. Use the `no` form of this command to return to the default configuration.

### Syntax

- `spanning-tree mst instance-id port-priority priority`
- `no spanning-tree mst instance-id port-priority`
  - *instance-ID* — ID of the spanning tree instance. (Range: 1 - 15)
  - *priority* — The port priority. (Range: 0 - 240 in multiples of 16)

### Default Setting

The default port priority for IEEE Multiple Spanning Tree Protocol (MSTP) is 128.

### Command Modes

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the port priority of port g1 to 142.

```
Console(config)# interface ethernet g1  
Console(config-if)# spanning-tree mst 1 port-priority 142
```

## spanning-tree mst cost

The `spanning-tree mst cost` Interface Configuration mode command configures the path cost for multiple spanning tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. Use the `no` form of this command to return to the default configuration.

### Syntax

- `spanning-tree mst instance-id cost cost`
- `no spanning-tree mst instance-id cost`
  - *instance-ID* — ID of the spanning -tree instance. (Range: 1 - 15)
  - *cost* — The port path cost. (Range: 1 - 200,000,000)



### Default Setting

Default path cost is determined by port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

### Command Modes

Interface Configuration (Ethernet, port-channel) mode.

### Default Configuration

There is no default configuration for this command.

### Example

The following example configures the MSTP instance 1 path cost for Ethernet port g9 to 4.

```
Console(config) # interface ethernet 1/g9
Console(config-if) # spanning-tree mst 1 cost 4
```

## spanning-tree mst configuration

The `spanning-tree mst configuration` Global Configuration mode command enables configuring an MST region by entering the Multiple Spanning Tree (MST) mode.

### Syntax

- `spanning-tree mst configuration`

### Default Setting

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- All devices in an MST region must have the same VLAN mapping, configuration revision number and name.

## Example

The following example configures an MST region.

```
Console(config)# spanning-tree mst configuration
Console(config-mst) # instance 1 add vlan 10-20
Console(config-mst) # name region1
Console(config-mst) # revision 1
```

## instance (mst)

The `instance` MST Configuration mode command maps VLANs to an MST instance.

### Syntax

- `instance instance-id {add | remove} vlan vlan-range`
  - *instance-ID* — ID of the MST instance. (Range: 1 - 16)
  - *vlan-range* — VLANs to be added to or removed from the specified MST instance. To specify a range of VLANs, use a hyphen. To specify a series of VLANs, use a comma. (Range: 1 - 4094)

### Default Setting

VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

### Command Modes

MST Configuration mode.

### User Guidelines

- All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.  
For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

## Example

The following example maps VLANs 10-20 to MST instance 1.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# instance 1 add vlan 10-20
```

## name (mst)

The **name** MST Configuration mode command defines the configuration name. Use the **no** form of this command to return to the default setting.

### Syntax

- **name** *string*
- **no name**
  - *string* — MST configuration name and is case-sensitive. (Range: 1 - 32 characters)

### Default Setting

The default name is a bridge ID.

### Command Mode

MST Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example defines the configuration name as region1.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # name region 1
```

## revision (mst)

The **revision** MST Configuration command defines the configuration revision number. Use the **no** form of this command return to the default configuration.

### Syntax

- **revision** *value*
- **no revision**
  - *value* — Configuration revision number. (Range: 0 - 65535)

### Default Setting

The default configuration revision number is 0.

### Command Mode

MST Configuration mode.

## User Guidelines

- There are no user guidelines for this command.

## Example

The following example sets the configuration revision to 1.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # revision 1
```

## show (mst)

The `show MST Configuration` mode command displays the current or pending MST region configuration.

## Syntax

- `show {current | pending}`
  - *current* — Indicates the current region configuration.
  - *pending* — Indicates the pending region configuration.

## Default Setting

This command has no default configuration.

## Command Mode

MST Configuration mode.

## User Guidelines

- The pending MST region configuration takes effect only after exiting the MST Configuration mode.

## Example

The following example displays a pending MST region configuration.

```
Console(config-mst)# show pending
Pending MST configuration
Name:
Region1
Revision: 1
Instance      Vlans Mapped      State
-----
0             1-9,21-4094      Enabled
1             10-20             Enabled
```

## exit (mst)

The **exit** MST Configuration mode command exits the MST Configuration mode and applies all configuration changes.

### Syntax

- exit

### Default Setting

This command has no default configuration.

### Command Mode

MST Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example exits the MST Configuration mode and saves changes.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # exit
```

## abort (mst)

The **abort** MST Configuration mode command exits the MST Configuration mode without applying the configuration changes.

### Syntax

- abort

### Default Setting

This command has no default configuration.

### Command Mode

MST Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example exits the MST Configuration mode without saving changes.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # abort
```

## spanning-tree pathcost method

The **spanning-tree pathcost method** Global Configuration mode command sets the default path cost method. Use the **no** form of this command to revert to the default setting.

### Syntax

- **spanning-tree pathcost method** {long | short}
- **no spanning-tree pathcost method**
  - *long* — Specifies 1 through 200,000,000 range for port path costs.
  - *short* — Specifies 0 through 65,535 range for port path costs.

### Default Configuration

Short

### Command Mode

Global Configuration mode.

### User Guidelines

- The cost is set using the **spanning-tree cost** command.

### Example

The following example sets the default path cost method to "long".

```
Console# spanning-tree pathcost method long
```

## spanning-tree bpdu

The **spanning-tree bpdu** Global Configuration mode command defines BPDU handling when spanning-tree is disabled on an interface. Use the **no** form of this command to revert to the default setting.

### Syntax

- `spanning-tree bpdn {filtering | flooding}`
- `no spanning-tree bpdn`
  - `filtering` — Filter BPDU packets when spanning-tree is disabled on an interface.
  - `flooding` — Flood BPDU packets when spanning-tree is disabled on an interface.

### Default Configuration

The default definition is flooding.

### Command Modes

Global Configuration mode.

### User Guidelines

- The command is relevant when spanning-tree is disabled globally or on a single interface.

### Example

The following example defines BPDU packet flooding when spanning-tree is disabled on an interface.

```
Console(config)# spanning-tree bpdn flooding
```

## clear spanning-tree detected-protocols

The `clear spanning-tree detected-protocols` Privileged EXEC mode command restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.

### Syntax

- `clear spanning-tree detected-protocols [ethernet interface number | port-channel port-channel-number]`
  - *interface* — A valid Ethernet port.
  - *port-channel-number* — A port-channel index.

### Default Configuration

If no interface is specified, the action is applied to all interfaces.

### Command Modes

Privileged EXEC mode.

### User Guidelines

- This feature should be used only when working in RSTP mode.

### Example

The following example restarts the protocol migration process (forces the renegotiation with neighboring switches) on g1.

```
Console# clear spanning-tree detected-protocols ethernet g1
```

## show spanning-tree

The `show spanning-tree` Privileged EXEC mode command displays spanning-tree configuration.

### Syntax

- `show spanning-tree` [ `ethernet` *interface-number* | `port-channel` *port-channel-number* ] [ `instance` *instance-id* ]
- `show spanning-tree` [ `detail` ] [ `active` | `blockedports` ] [ `instance` *instance-id* ]
- `show spanning-tree mst-configuration`
  - `detail` — Display detailed information.
  - `active` — Display active ports only.
  - `blockedports` — Display blocked ports only.
  - `mst-configuration` — Display the MST configuration identifier.
  - *interface-number* — Ethernet port number. (Range: Valid Ethernet port)
  - *port-channel-number* — Port channel index. (Range: Valid Ethernet port)
  - *instance-id* — ID associated with a spanning-tree instance.

### Default Configuration

This command has no default configuration.

### Command Modes

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.



## Examples

The following example displays spanning-tree information.

```
Console# show spanning-tree

Spanning tree enabled mode RSTP
Default port cost method: long
Root ID      Priority      32768
             Address      00:01:42:97:e0:00
             Path Cost   2000
             Root Port   1(g1)
             Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID    Priority 36864
             Address 00:02:4b:29:7a:00
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interfaces
Name        State          Prio.Nbr   Cost     Sts     Role    PortFast Type
-----
1          Enabled        128.1      20000    FWD     Root    No      P2p (RSTP)
2          Enabled        128.2      20000    FWD     Desg    No      Shared (STP)
3          Disabled       128.3      20000
4          Enabled        128.4      20000    BLK     Altn    No      Shared (STP)
5          Enabled        128.5      20000    DIS -   -

console# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
```

```

Root ID      Priority      36864
            Address      00:02:4b:29:7a:00
            This switch is the
            Root.
            Hello Time 2 Max Age 20 sec Forward Delay
            sec          15 sec

```

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
1	Enabled	128.1	20000	FWD	Desg	No	P2p (RSTP)
2	Enabled	128.2	20000	FWD	Desg	No	Shared (STP)
3	Disabled	128.3	20000				
4	Enabled	128.4	20000	FWD	Desg	No	Shared (STP)
5	Enabled	128.5	20000	DIS	-		

```
Console# show spanning-tree
```

```
Spanning tree disabled (BPDU filtering) mode RSTP
```

```
Default port cost method: long
```

```

Root ID      Priority      N/A
            Address      N/A
            Path Cost   N/A
            Root Port   N/A
            Hello Time  Max Age N/A Forward
            N/A          Delay N/A

```

```
Bridge ID Priority      36864
          Address      00:02:4b:29:7a:00
          Hello Time   Max Age 20 sec Forward
          2 sec       Delay 15 sec
```

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
g1	Enabled	128.1	20000				
g2	Enabled	128.2	20000				
g3	Disabled	128.3	20000				
g4	Enabled	128.4	20000				
g5	Enabled	128.5	20000				

```
Console# show spanning-tree active
```

```
Spanning tree enabled mode RSTP
```

```
Default port cost method: long
```

```
Root ID Priority      32768
          Address      00:01:42:97:e0:00
          Path Cost     20000
          Root Port     1 (g1)
          Hello Time   Max Age 20 sec Forward
          2 sec       Delay 15 sec
```

```
Bridge ID  Priority      36864
           Address      00:02:4b:29:7a:00
           Hello Time 2 Max Age 20 sec Forward
           sec          Delay 15 sec
```

#### Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
g1	Enabled	128.1	20000	FWD	Root	No	P2p (RSTP)
g2	Enabled	128.2	20000	FWD	Desg	No	Shared (STP)
g4	Enabled	128.4	20000	BLK	Altn	No	Shared (STP)

```
onsole# show spanning-tree blockedports
```

```
Spanning tree enabled mode RSTP
```

```
Default port cost method: long
```

```
Root ID  Priority      32768
          Address      00:01:42:9
          7:e0:00
          Path Cost    20000
          Root Port    1 (g1)
          Hello Time 2 Max Age 20 sec Forward
          sec          Delay 15 sec
```

```
Bridge ID  Priority      36864
           Address      00:02:4b:29:7a:00
           Hello Time 2 Max Age 20 sec Forward Delay
           sec          15 sec
```

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
1/4	Enabled	128.4	19	BLK	Altn	No	Shared (STP)

Console# show spanning-tree detail

Spanning tree enabled mode RSTP

Default port cost method: long

Root ID      Priority      32768  
              Address      00:01:42:97:e0:00  
              Path Cost      20000  
              Root Port      1 (g1)  
              Hello Time    Max Age 20 sec    Forward Delay  
              2 sec            15 sec

Bridge ID    Priority      36864  
              Address      00:02:4b:29:7a:00  
              Hello Time    Max Age 20 sec    Forward Delay 15 sec  
              2 sec

Number of topology changes 2 last change  
occurred 2d18h ago

Times: hold 1, topology change 35,  
notification 2

hello 2, max age 20, forward delay 15

State: Forwarding	Role: Root
Port id: 128.1	Port cost: 20000
Type: P2p (configured: auto) RSTP	Port Fast: No (configured:no)
Designated bridge Priority: 32768	Address: 00:01:42:97:e0:00
Designated port id: 128.25	Designated path cost: 0
Guard root: Disabled	
Number of transitions to forwarding state: 1	
BPDU: sent 2, received 120638	
Port 2 (1/2) enabled	
State: Forwarding	Role: Designated
Port id: 128.2	Port cost: 20000
Type: Shared (configured: auto) STP	Port Fast: No (configured:no)
Designated bridge Priority: 32768	Address: 00:02:4b:29:7a:00
Designated port id: 128.2	Designated path cost: 20000
Guard root: Disabled	
Number of transitions to forwarding state: 1	
BPDU: sent 2, received 170638	
Port 3 (1/3) disabled	
State: N/A	Role: N/A
Port id: 128.3	Port cost: 20000
Type: N/A (configured: auto)	Port Fast: N/A (configured:no)
Designated bridge Priority: N/A	Address: N/A
Designated port id: N/A	Designated path cost: N/A
Guard root:Disabled	
Number of transitions to forwarding state: N/A	
BPDU: sent N/A, received N/A	

```

Port 4 (1/4) enabled
State: Blocking                               Role: Alternate
Port Identifier: 128.4                         Port cost: 20000
Type: Shared (configured: auto) STP           Port Fast: No (configured:no)
Designated bridge Priority: 28672             Address: 00:30:94:41:62:c8
Designated port id: 128.25                    Designated path cost: 20000
Guard root:Disabled
Number of transitions to forwarding
state: 1
BPDU: sent 2, received 120638
Port 5 (1/5) enabled
State: Disabled                               Role: N/A
Port id: 128.5                                Port cost: 20000
Type: N/A (configured: auto)                  Port Fast: N/A (configured:no)
Designated bridge Priority: N/A                Address: N/A
Designated port id: N/A                       Designated path cost: N/A
Guard root:Disabled
Number of transitions to forwarding
state: N/A
BPDU: sent N/A, received N/A
Console# show spanning-tree mst-configuration

Name: Region1
Revision: 1

Instance          Vlans Mapped          State
0                 1-9,21-4094           Enabled
1                 10-20                 Enabled

```

```

Console# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long

##### MST 0 Vlans Mapped: 1-9
CST Root ID          Priority          32768
                    Address          00:01:42:97:e0:00
                    Path Cost       20000
                    Root Port       1 (g1)
                    Hello Time 2 sec      Max Age 20 sec  Forward
                                        Delay 15 sec

IST Master ID        Priority          32768
                    Address          00:02:4b:29:7a:00
Hello Time 2 sec. Max Age 20 sec Forward Delay 15 sec Max hops 20
Interfaces
Name State  Prio.Nbr  Cost  Sts  Role  PortFast Type
1    Enabled 128.1    20000 FWD   Root  No    P2p Bound (RSTP)
2    Enabled 128.2    20000 FWD   Desg  No    Shared Bound (STP)
3    Enabled 128.3    20000 FWD   Desg  No    P2p
4    Enabled 128.4    20000 FWD   Desg  No    P2p

##### MST 1 Vlans Mapped: 10-20
Root ID              Priority          24576
                    Address          00:02:4b:29:89:76
                    Path Cost       20000
                    Root Port       4(1/4)
                    Rem hops        19

```



```

Bridge ID                Priority                32768
                          Address                00:02:4b:29:7a:00
Number of topology changes 2 last change occurred 1d9h ago
Times: hold 1, topology change 2, notification 2
hello 2, max age 20, forward delay 15
Port 1 (g1) enabled
State: Forwarding                Role: Boundary
Port id: 128.1                    Port cost: 20000
Type: P2p (configured: auto) Boundary  Port Fast: No (configured:no)
RSTP
Designated bridge Priority: 32768    Address: 00:02:4b:29:7a:00
Designated port id: 128.1            Designated path cost: 20000
Guard root:Disabled
Number of transitions to forwarding
state: 1
BPDU: sent 2, received 120638
Port 2 (1/2) enabled
State: Forwarding                Role: Designated
Port id: 128.2                    Port cost: 20000
Type: Shared (configured: auto) Boundary  Port Fast: No (configured:no)
STP
Designated bridge Priority: 32768    Address: 00:02:4b:29:7a:00
Designated port id: 128.2            Designated path cost: 20000
Guard root: Disabled
Number of transitions to forwarding
state: 1
BPDU: sent 2, received 170638

```

```

Port 3 (1/3) disabled
State: Blocking                               Role: Alternate
Port id: 128.3                               Port cost: 20000
Type: Shared (configured: auto) Internal Port Fast: No (configured:no)
Designated bridge Priority: 32768           Address: 00:02:4b:29:1a:19
Designated port id: 128.78                 Designated path cost: 20000
Guard root: Disabled
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
Port 4 (1/4) enabled
State: Forwarding                           Role: Designated
Port id: 128.4                               Port cost: 20000
Type: Shared (configured: auto) Internal Port Fast: No
                                           (configured:no)
Designated bridge Priority: 32768           Address: 00:02:4b:29:7a:00
Designated port id: 128.2                 Designated path cost: 20000
Guard root:Disabled
Number of transitions to forwarding state:
1
BPDU: sent 2, received 170638
Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

##### MST 0 Vlans Mapped: 1-9

CST Root ID                               Priority           32768
                                           Address           00:01:42:97:e0:00

```

```

                Path Cost                20000
                Root Port                1 (g1)
                Hello Time 2 sec         Max Age 20 sec Forward
                Delay 15 sec
IST Master ID   Priority                32768
                Address                 00:02:4b:19:7a:00
                Path Cost                10000
                Rem hops                 19
Bridge ID      Priority                32768
                Address                 00:02:4b:29:7a:00
                Hello Time 2 sec         Max Age 20 sec Forward
                Delay 15 sec Max hops
                20

Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

##### MST 0 Vlans Mapped: 1-9

CST Root ID   Priority                32768
                Address                 00:01:42:97:e0:00
                This switch is root for
                CST
                Hello Time 2 sec         Max Age 20 sec Forward
                Delay 15 sec Max hops
                20
```

## Spanning-tree guard root

The `spanning-tree guard root` Interface Configuration mode command enables root guard on all spanning tree instances on the interface. Root guard restricts the interface to be the switch root port. Use the `no` form of this command to disable root guard on the interface.

### Syntax

- `spanning-tree guard root`
- `no spanning-tree guard root`

### Default Configuration

Root guard is disabled.

### Command Modes

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- Root guard can be enabled when the switch work in STP, RSTP and MSTP.  
When root guard is enabled, if spanning-tree calculations cause a port to be selected as the root port, the port transitions to the alternate state.

### Example

The following example enable root guard on port g8.

```
Console(config)# interface ethernet g8  
Console(config-if)# spanning-tree guard root
```

# SSH Commands

## ip ssh port

The `ip ssh port` Global Configuration mode command specifies the port to be used by the SSH server. Use the `no` form of this command to use the default port.

### Syntax

- `ip ssh port port-number`
- `no ip ssh port`
  - *port-number* — Port number for use by the SSH server. (Range: 1 - 65535)

### Default Configuration

The default value is 22.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example specifies the port to be used by the SSH server as 8080.

```
Console (config)# ip ssh port 8080
```

## ip ssh server

The `ip ssh server` Global Configuration mode command enables the device to be configured from a SSH server. Use the `no` form of this command to disable this function.

### Syntax

- `ip ssh server`
- `no ip ssh server`

### Default Configuration

SSH is enabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- If encryption keys are not generated, the SSH server is in standby until the keys are generated. To generate SSH server keys, use the commands **crypto key generate rsa**, and **crypto key generate dsa**.

### Example

The following example enables the device to be configured from a SSH server.

```
Console (config)# ip ssh server
```

## crypto key generate dsa

The **ip ssh server** Global Configuration mode command generates DSA key pairs.

### Syntax

- **crypto key generate dsa**

### Default Configuration

DSA key pairs do not exist.

### Command Mode

Global Configuration mode.

### User Guidelines

- DSA keys are generated in pairs: one public DSA key and one private DSA key. If the device already has DSA keys, a warning and prompt to replace the existing keys with new keys is displayed.
- This command is not saved in the startup configuration; however, the keys generated by this command are saved in the FLASH. The SSH keys can be displayed with the **show crypto key mypubkey dsa** command.
- This command may take a considerable period of time to execute.
- DSA key size is 2048 bits.

### Example

The following example generates DSA key pairs.

```
Console (config)# crypto key generate dsa
```

## crypto key generate rsa

The `crypto key generate rsa` Global Configuration mode command generates RSA key pairs.

### Syntax

- `crypto key generate rsa`

### Default Configuration

RSA key pairs do not exist.

### Command Mode

Global Configuration mode.

### User Guidelines

- RSA keys are generated in pairs: one public RSA key and one private RSA key. If the device already has RSA keys, a warning and prompt to replace the existing keys with new keys is displayed.
- The maximum supported size for the RSA key is 2048 bits.
- This command is not saved in the startup configuration; however, the keys generated by this command are saved in the FLASH. The SSH keys can be displayed with the `show crypto key mypubkey rsa` command.
- This command may take a considerable period of time to execute.

### Example

The following example generates RSA key pairs.

```
Console (config)# crypto key generate rsa
```

## ip ssh pubkey-auth

The `ip ssh pubkey-auth` Global Configuration mode command enables public key authentication for incoming SSH sessions. Use the `no` form of this command to disable this function.

### Syntax

- `ip ssh pubkey-auth`
- `no ip ssh pubkey-auth`

### Default Configuration

The function is disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enables public key authentication for incoming SSH sessions.

```
Console (config)# ip ssh pubkey-auth
```

## crypto key pubkey-chain ssh

The `crypto key pubkey-chain ssh` Global Configuration mode command enters SSH Public Key-chain Configuration mode. The mode is used to manually specify other device public keys such as SSH client public keys.

### Syntax

- `crypto key pubkey-chain ssh`

### Default Configuration

By default, there are no keys.

### Command Mode

Global Configuration mode.

### User Guidelines

- Use this command to enter Public Key-chain Configuration mode.
- This command can also be used when you need to manually specify SSH client's public keys.

### Example

The following example enters the SSH Public Key-chain Configuration mode.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)#
```

## user-key

The `user-key` SSH Public Key Chain Configuration mode command specifies which SSH public key is manually configured and enters the SSH Public Key-chain Configuration mode command. Use the `no` form of this command to remove a SSH public key.



## Syntax

- `user-key username {rsa | dsa}`
- `no user-key username`
  - `username` — Specifies the remote SSH client username, which can be up to 48 characters long.
  - `rsa` — RSA key.
  - `dsa` — DSA key.

## Default Configuration

By default, there are no keys.

## Command Mode

SSH Public Key Chain Configuration mode.

## User Guidelines

- Follow this command with the `key-string` command to specify the key.

## Example

The following example enables a SSH public key to be manually configured for the SSH public key chain called "bob".

```
Console(config-pubkey-chain)# user-key bob rsa  
Console(config-pubkey-key)# key-string row key-string  
AAAAB3NzaC1yc2EAAAADAQABAAQACvTnRwPWl
```

# key-string

The `key-string` SSH Public Key-String Configuration mode command manually specifies a SSH public key.

## Syntax

- `key-string row key-string`
  - `row` — Specify SSH public key row by row
  - `key-string` — UU-encoded DER format is the same format in `authorized_keys` file used by OpenSSH.

## Default Configuration

By default, the keys do not exist.

## Command Mode

SSH Public Key-string Configuration mode.

## User Guidelines

- Use the **key-string row** command to specify the SSH public key row by row. Each row must begin with the **key-string row** command. This command is useful for configuration files.
- UU-encoded DER format is the same format in authorized\_keys file used by OpenSSH.

## Example

The following example enters public key strings for SSH public key clients called 'bob'.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAQACvTnRwPWl
Al4kpbqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfzSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJjk67IOU/zfwOllg
kTwm175QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licg1k02LYciz
+Z4TrEU/9FJxwPivQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaTlwefWwX6f+
Rmt5nhhqAtN/4oJfcel66DqVX1gWmN
zNR4DYDvSzg01DnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

## show ip ssh

The **show ip ssh** Privileged EXEC mode command displays the SSH server configuration.

### Syntax

- **show ip ssh**

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the SSH server configuration.

```
Console# show ip ssh
SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.
SSH Public Key Authentication is enabled.
Active incoming sessions:
IP address  SSH          Version      Cipher      Auth Code
           username
-----  -
172.16.0.1  John Brown 2.0 3      DES        HMAC-SH1
```

The following table describes the significant fields shown in the display:

Field	Description
IP address	Client address
SSH username	User name
Version	SSH version number
Cipher	Encryption type (3DES, Blowfish, RC4)
Auth Code	Authentication Code (HMAC-MD5, HMAC-SHA1)

## show crypto key mypubkey

The `show crypto key mypubkey` Privileged EXEC mode command displays the SSH public keys on the device.

### Syntax

- `show crypto key mypubkey [rsa | dsa]`
  - `rsa` — RSA key.
  - `dsa` — DSA key.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the SSH public keys on the device.

```
Console# show crypto key mypubkey rsa
RSA key data:
005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B
55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C
73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301
87685768
Fingerprint(Hex): 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
Fingerprint(Bubble Babble): yteriuwt jgkljhglk yewiury hdskjfryt
gfhkjglk
```

## show crypto key pubkey-chain ssh

The `show crypto key pubkey-chain ssh` Privileged EXEC mode command displays SSH public keys stored on the device.

### Syntax

- `show crypto key pubkey-chain ssh [username username] [fingerprint bubble-babble | hex]`
  - *username* — Specifies the remote SSH client username.
  - *bubble-babble* — Fingerprints in Bubble Babble format.
  - *hex* — Fingerprint in Hex format. If fingerprint is unspecified, it defaults to Hex format.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example displays all SSH public keys stored on the device.

```
Console# show crypto key pubkey-chain ssh
Username  Fingerprint
-----  -
bob       9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
john      98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8
```

The following example displays the SSH public called "bob".

```
Console# show crypto key pubkey-chain ssh username bob
Username: bob
Key: 005C300D 06092A86
```



# Syslog Commands

## logging on

The **logging on** Global Configuration mode command controls error messages logging. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the process that generated the messages. Use the **no** form of this command to disable the logging process.

### Syntax

- **logging on**
- **no logging on**

### Default Configuration

Logging is enabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server. Logging on and off for these destinations can be individually configured using the **logging buffered**, **logging file**, and **logging** Global Configuration mode commands. However, if the **logging on** command is disabled, no messages are sent to these destinations. Only the console receives messages.

### Example

The following example shows how logging is enabled.

```
Console (config)# logging on
```

## logging

The **logging** Global Configuration mode command logs messages to a syslog server. Use the **no** form of this command to delete the syslog server with the specified address from the list of syslogs.

## Syntax

- **logging** {*ip4-address* | *ip6-address* | *hostname*} [**port** *port*] [**severity level**] [**facility facility**] [**description text**]
- **no logging** {*ip4-address* | *ip6-address* | *hostname*}
  - *ip4-address* — Host IPv4 address to be used as a syslog server.
  - *ip6-address* — Host IPv6 address to be used as a syslog server. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the usage guidelines for the interface name syntax.
  - *hostname* — Hostname of the host to be used as a syslog server. (Range: 1 - 158 characters)
  - *port* — Port number for syslog messages. If unspecified, the port number defaults to 514. (Range: 1 - 65535)
  - **severity level** — Limits the logging of messages to the syslog servers to a specified level: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational** and **debugging**. If unspecified, the default level is **errors**.
  - *facility* — The facility that is indicated in the message. Can be one of the following values: **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, **local7**. If unspecified, the port number defaults to **local7**.
  - *text* — Syslog server description. (Range: 1 - 64 characters)

## Default Configuration

As described in the field descriptions.

## Command Mode

Global Configuration mode.

## User Guidelines

- Multiple syslog servers can be used.
- If no specific severity level is specified, the global values apply to each server.
- The IPv6Z address format: `<ip6-link-local-address>%<interface-name>`
  - *interface-name* — **vlan**<integer> | **ch**<integer> | **isatap**<integer> | <physical-port-name> | 0
  - *integer* — <decimal-number> | <integer><decimal-number>
  - *decimal-number* — 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
  - *physical-port-name* — Designated port number, for example g1.

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is the same as not defining an egress interface.



### Example

The following example limits logged messages sent to the syslog server with IP address 10.1.1.1 to severity level **critical**.

```
Console (config)# logging 10.1.1.1 severity critical
```

## logging console

The **logging console** Global Configuration mode command limits messages logged to the console based on severity. Use the **no** form of this command to disable logging to the console terminal.

### Syntax

- **logging console** *level*
- **no logging console**
  - *level* — Limits the logging of messages displayed on the console to a specified level: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, **debugging**.

### Default Configuration

The default is **informational**.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example limits messages logged to the console based on severity level "errors".

```
Console (config)# logging console errors
```

## logging buffered

The **logging buffered** Global Configuration mode command limits syslog messages displayed from an internal buffer based on severity. Use the **no** form of this command to cancel the buffer use.

### Syntax

- **logging buffered** *level*
- **no logging buffered**
  - *level* — Limits the message logging to a specified level buffer: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, **debugging**.

### Default Configuration

The default level is **informational**.

### Command Mode

Global Configuration mode.

### User Guidelines

- All the syslog messages are logged to the internal buffer. This command limits the commands displayed to the user.

### Example

The following example limits syslog messages displayed from an internal buffer based on the severity level "debugging".

```
Console (config)# logging buffered debugging
```

## logging buffered size

The **logging buffered size** Global Configuration mode command changes the number of syslog messages stored in the internal buffer. Use the **no** form of this command to return the number of messages stored in the internal buffer to the default value.

### Syntax

- **logging buffered size** *number*
- **no logging buffered size**
  - *number* — Numeric value indicating the maximum number of messages stored in the history table. (Range: 20 - 400)

### Default Configuration

The default number of messages is 200.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example changes the number of syslog messages stored in the internal buffer to 300.

```
Console (config)# logging buffered size 300
```

## clear logging

The `clear logging` Privileged EXEC mode command clears messages from the internal logging buffer.

### Syntax

- `clear logging`

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example clears messages from the internal syslog message logging buffer.

```
Console# clear logging
Clear logging buffer [y/n] y
```

## logging file

The `logging file` Global Configuration mode command limits syslog messages sent to the logging file based on severity. Use the `no` form of this command to cancel the buffer.

### Syntax

- `logging file level`
- `no logging file`
  - *level* — Limits the logging of messages to the buffer to a specified level: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational** and **debugging**.

### Default Configuration

The default severity level is **errors**.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example limits syslog messages sent to the logging file based on the severity level 'alerts'.

```
Console (config)# logging file alerts
```

## clear logging file

The **clear logging file** Privileged EXEC mode command clears messages from the logging file.

### Syntax

- clear logging file

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example clears messages from the logging file.

```
Console# clear logging file
Clear Logging File [y/n]y
```

## aaa logging

The **aaa logging** Global Configuration mode command controls logging of AAA events. To disable logging use the **no** form of the command.

### Syntax

- aaa logging login
- no aaa logging login
  - login — Log messages related to successful login events, unsuccessful login events and other login related events.

### Default Configuration

The logging of AAA events is enabled.

**Command Mode**

Global Configuration mode.

**User Guidelines**

- Other types of AAA events are not subject to this command.

**Example**

The following example enables logging messages related to AAA login events.

```
Console(config)# aaa logging login
```

## file-system logging

The `file-system logging` Global Configuration mode command controls logging file system events. To disable logging use the `no` form of the command.

**Syntax**

- `file-system logging copy`
- `no file-system logging copy`
- `file-system logging delete-rename`
- `no file-system logging delete-rename`
  - `copy` — Log messages related to file copy operations.
  - `delete-rename` — Log messages related to file deletion and renaming.

**Default Configuration**

Logging file system events enabled.

**Command Mode**

Global Configuration mode.

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example enables logging messages related to file copy operations.

```
Console(config)# file-system logging copy
```

## management logging

The **management logging** Global Configuration mode command controls logging of management access lists events. To disable logging use the **no** form of the command.

### Syntax

- **management logging deny**
- **no management logging deny**
  - **deny** — Log messages related to management ACLs deny actions.

### Default Configuration

Logging of management access lists events enabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- Other types of management ACLs events are not subject to this command.

### Example

The following example enables logging messages related to deny actions of management ACLs.

```
Console(config)# management logging deny
```

## show logging

The **show logging** Privileged EXEC mode command displays the state of logging and the syslog messages stored in the internal buffer.

### Syntax

- **show logging**

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the show logging settings.

```
Console# show logging
Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped
(severity).
Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.
File logging: level notifications. File Messages: 0 Dropped (severity).
Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped
(severity).
Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped
(severity).
2 messages were not logged (resources)
Application filtering control
Application          Event                Status
AAA                  Login                Enabled
File system          Copy                 Enabled
File system          Delete-Rename        Enabled
Management ACL       Deny                 Enabled
```

Buffer log:

```
11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0,
changed state to up
```

```
11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg/0, changed
state to up
```

```
11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg/1, changed
state to up
```

```
11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/2, changed
state to up
```

```
11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg/3, changed
state to up
```

```
11-Aug-2002 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console
```

```
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
```

```
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/0, changed state to down
```

```
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet g/1, changed state to down
```

```
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/2, changed state to down
```

```
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/3, changed state to down
```

## show logging file

The `show logging file` Privileged EXEC command displays the state of logging and the syslog messages stored in the logging file.

### Syntax

- `show logging file`

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.



## User Guidelines

- There are no user guidelines for this command.

## Example

The following example displays the show logging file settings.

```
Console# show logging file
Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped
(severity).
Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.
File logging: level notifications. File Messages: 0 Dropped (severity).
Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped
(severity).
Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped
(severity).
2 messages were not logged (resources)
Application filtering control
Application          Event                Status
AAA                  Login                Enabled
File system          Copy                 Enabled
File system          Delete-Rename        Enabled
Management ACL       Deny                 Enabled
```

File log:

```
11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0,
changed state to up
11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg/0, changed
state to up
11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg/1, changed
state to up
11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg/2, changed
state to up
11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg/3, changed
state to up
11-Aug-2002 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/0, changed state to down
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet g/1, changed state to down
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet g/2, changed state to down
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet g/3, changed state to down
```

## show syslog-servers

The show syslog-servers Privileged EXEC mode command displays the syslog servers settings.

### Syntax

- show syslog-servers

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the syslog server settings.

```
Console# show syslog-servers
```

IP address	Port	Severity	Facility	Description
-----	----	-----	-----	-----
192.180.2.275	14	Informational	local	7
192.180.2.285	14	Warning	local	7



# System Management

## ping

The **ping** User EXEC mode command sends ICMP echo request packets to another node on the network.

### Syntax

- **ping** *ip-address* | *hostname* [**size** *packet\_size*] [**count** *packet\_count*] [**timeout** *time\_out*]
- **ping ipv6** {*ipv6-address* | *hostname*} [**size** *packet\_size*] [**count** *packet\_count*] [**timeout** *time\_out*]
  - **ipv6** — IPv6 checks the network connectivity.
  - *ip4-address* — Destination host IPv4 address.
  - *ipv6-address* — Unicast or multicast IPv6 address to ping. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the usage guidelines for the interface name syntax.
  - *hostname* — hostname to ping. (Range: 1 - 158 characters)
  - *packet\_size* — Number of bytes in a packet. The actual packet size is eight bytes larger than the size specified because the switch adds header information. (Range: 56 - 1472 bytes)
  - *packet\_count* — Number of packets to send. If 0 is entered it pings until stopped. (Range: 0 - 65535 packets)
  - *time\_out* — Timeout in milliseconds to wait for each reply. (Range: 50 - 65535 milliseconds).

### Default Configuration

**timeout** *time\_out* — The default is 2000 milliseconds.

### Command Mode

User EXEC mode.

## User Guidelines

Press **Esc** to stop pinging. Following are sample results of the **ping** command:

- **Destination (host/network) unreachable** — The gateway for this destination indicates an unreachable destination.
- **Destination does not respond** — If the host does not respond, a “no answer from host” appears in ten seconds.

The IPv6Z address format: `<ipv6-link-local-address>%<interface-name>`

- *interface-name* — `vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name> | 0`
- *integer* — `<decimal-number> | <integer><decimal-number>`
- *decimal-number* — `0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9`
- *physical-port-name* — Designated port number, for example `g1`.

When using the `ping ipv6` command to check network connectivity of a directly attached host using its link local address, the egress interface may be specified in the IPv6Z format. If the egress interface is not specified, the default interface is selected. Specifying `interface zone=0` is the same as not defining an egress interface.

When using the `ping ipv6` command with a multicast address, the information displayed is taken from all received echo responses.

## Examples

The following example displays a ping to IP address 10.1.1.1.

```
Console> ping 10.1.1.1
Pinging 10.1.1.1 with 64 bytes of data:

64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

The following example displays an address 180.50.1.1 which does not have connectivity.

```
Console# ping 180.50.1.1
Pinging 180.50.1.1 with 56 bytes of data:
PING: net-unreachable
PING: net-unreachable
PING: net-unreachable
```

## traceroute

The **traceroute** User EXEC mode command discovers the routes that packets will actually take when traveling to their destination.

### Syntax

- **traceroute** *ip-address* [*hostname* [*size packet\_size*] [*ttl max-ttl*] [*count packet\_count*] [*timeout time\_out*] [*source ip-address*] [*tos tos*]
- **traceroute ipv6** {*ipv6-address* | *hostname*} [*size packet\_size*] [*ttl max-ttl*] [*count packet\_count*] [*timeout time\_out*] [*source ip-address*] [*tos tos*]
  - **ipv6** — IPv6 checks the network connectivity.
  - *ip4-address* — Destination host IPv4 address. (Range: Valid IP Address)
  - *ip6-address* — Unicast or multicast IPv6 address to ping. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the usage guidelines for the interface name syntax.
  - *hostname* — Hostname of the destination host. (Range: 1 - 158 characters)
  - *size packet\_size* — Number of bytes in a packet. (Range: 40 - 1472)
  - *ttl max-ttl* — The largest TTL value that can be used. The **traceroute** command terminates when the destination is reached or when this value is reached. (Range: 1 - 255)
  - *count packet\_count* — The number of probes to be sent at each TTL level. (Range: 1 - 10)
  - *timeout time\_out* — The number of seconds to wait for a response to a probe packet. (Range: 1 - 60)
  - *source ip-address* — One of the interface addresses of the device to use as a source address for the probes. The device will normally pick what it feels is the best source address to use. (Range: Valid IP Address)
  - *tos tos* — The Type-Of-Service byte in the IP Header of the packet. (Range: 0 - 255)

### Default Configuration

*size packet\_size* — The default is 40 bytes.

*ttl max-ttl* — The default is 30.

`count` *packet\_count* — The default count is 3.

`timeout` *time\_out* — The default is 6 seconds.

### Command Mode

User EXEC mode.

### User Guidelines

- The **traceroute** command works by taking advantage of the error messages generated by a device when a datagram exceeds its time-to-live (TTL) value.
- The **traceroute** command starts by sending probe datagrams with a TTL value of one. This causes the first device to discard the probe datagram and send back an error message. The **traceroute** command sends several probes at each TTL level and displays the round-trip time for each.
- The **traceroute** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A "time exceeded" error message indicates that an intermediate device has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (\*).
- The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with **Esc**.

### Examples

```
console> traceroute umaxpl.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxpl.physics.lsa.umich.edu (141.211.101.64)
 0  i2-gateway.stanford.edu (192.68.191.83)  0 msec 0 msec 0 msec
 1  STAN.POS.calren2.NET (171.64.1.213)  0 msec 0 msec 0 msec
 2  SUNV--STAN.POS.calren2.net (198.32.249.73)  1 msec 1 msec 1 msec
 3  Abilene--QSV.POS.calren2.net (198.32.249.162)  1 msec 1 msec 1 msec
 4  kscyng-snvang.abilene.ucaid.edu (198.32.8.103)  33 msec 35 msec 35 msec
 5  iplsng-kscyng.abilene.ucaid.edu (198.32.8.80)  47 msec 45 msec 45 msec
 6  so-0-2-0x1.aal.mich.net (192.122.183.9)  56 msec 53 msec 54 msec
 7  atm1-0x24.michnet8.mich.net (198.108.23.82)  56 msec 56 msec 57 msec
 8  * * *
 9
10  A-ARB3-LSA-NG.c-SEB.umnet.umich.edu (141.211.5.22)  58 msec 58 msec 58 msec
11  umaxpl.physics.lsa.umich.edu (141.211.101.64)  62 msec 63 msec 63 msec
```



The following table describes the significant fields shown in the display

Field	Description
1	Indicates the sequence number of the router in the path to the host.
i2-gateway.stanford.edu	Host name of this device.
192.68.191.83	IP address of this device.
1 msec 1 msec 1 msec	Round-trip time for each of the probes that are sent.

The following table describes the characters that can appear in the **tracert** command output.

Field	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an Access List is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

## telnet

The **telnet** User EXEC mode command is used to log in to a host that supports Telnet.

### Syntax

- **telnet** *ip-address* | *hostname* [*port*] [*keyword1*.....]
  - *ip-address* — IP address of the destination host. (Range: 1 - 160 characters)
  - *hostname* — Hostname of the destination host. (Range: Valid IP Address)
  - *port* — A decimal TCP port number, or one of the keywords from the ports table in the usage guidelines. The default is the Telnet port (decimal23) on the host.
  - *keyword* — Can be one or more keywords from the keywords table in the User Guidelines.

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

## User Guidelines

- The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter Esc and then a command character.

## Special Telnet Command characters

Escape Sequence	Purpose
Ctrl-shift-6 b	Break
Ctrl-shift-6 c	Interrupt Process (IP)
Ctrl-shift-6 h	Erase Character (EC)
Ctrl-shift-6 o	Abort Output (AO)
Ctrl-shift-6 t	Are You There? (AYT)
Ctrl-shift-6 u	Erase Line (EL)
Ctrl-shift-6 x	Suspends the Session

At any time during an active Telnet session, the Telnet commands can be listed by pressing the Ctrl-shift-6 key, followed by a question mark at the system prompt: Ctrl-shift-6?

A sample of this list follows.

```
Console> 'Ctrl-shift-6' ?
[Special telnet escape help]
Esc B sends telnet BREAK
Esc C sends telnet IP
Esc H sends telnet EC
Esc O sends telnet AO
Esc T sends telnet AYT
Esc U sends telnet EL
Esc x suspends the session (return to system command prompt)
```

Several concurrent Telnet sessions can be opened and switched between them. To open a subsequent session, the current connection needs to be suspended, by pressing the escape sequence 'Ctrl-Shift-6' and 'x' to return to the system command prompt. Then open a new connection with the telnet command.

## Keywords Table

Options	Description
/echo	Enables local echo
/quiet	Prevents onscreen display of all messages from the software.
/source-interface	Specifies the source interface.
/stream	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
Ctrl-shift-6 x	Return to System Command Prompt

## Ports Table

Keyword	Description	Port number
bgp	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513

lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

### Example

```
Console> telnet 176.213.10.50
Esc U sends telnet EL
```

## resume

The **resume** User EXEC mode command is used to switch to another open Telnet session.

### Syntax

- **resume** [*connection*]
- *connection* — The connection number. The default is the most recent connection

### Default Configuration

There is no default configuration for this command.

### Command Mode

User EXEC mode.

## User Guidelines

- There are no user guidelines for this command.

## Examples

The following command switches to another open Telnet session.

```
Console> resume 176.213.10.50
```

# reload

The **reload** Privileged EXEC mode command reloads the operating system.

## Syntax

- **reload**

## Default Configuration

This command has no default configuration.

## Command Mode

Privileged EXEC mode.

## User Guidelines

- Caution should be exercised when resetting the device, to ensure that no other activity is being performed. In particular, the user should verify that no configuration files are being downloaded at the time of reset.

## Example

The following example reloads the operating system.

```
Console# reload
```

# hostname

The **hostname** Global Configuration mode command specifies or modifies the device host name. Use the **no** form of the command to remove the existing host name.

## Syntax

- **hostname** *name*
- **no hostname**
  - *name* — The device host name. Range (1-158 characters)

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example specifies the device host name.

```
Console (config)# hostname Dell
```

## service cpu-utilization

The `service cpu-utilization` Global Configuration mode command allows the software to measure CPU utilization. Use the `no` form of this command to disable measuring.

### Syntax

- `service cpu-utilization`
- `no service cpu-utilization`

### Default Configuration

The `service cpu-utilization` function is enabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example allows the software to measure CPU utilization.

```
console(config)# service cpu-utilization
```

## show cpu utilization

The `show cpu utilization` privileged EXEC mode command displays information about CPU utilization.

### Syntax

- `show cpu utilization`

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- Use the `service cpu-utilization` Global Configuration mode command to enable measuring CPU utilization.

### Example

The following example displays the cpu utilization.

```
Console# show cpu utilization
CPU utilization service is on.
CPU utilization
-----
five seconds: 5%; one minute: 3%; five minutes: 3%
```

## show users

The `show users` Privileged EXEC mode command displays information about the active users.

### Syntax

- `show users`

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

```
Console> show users
```

Username	Protocol	Location
Bob	Serial	
John	SSH	172.16.0.1
Robert	HTTP	172.16.0.8
Betty	Telnet	172.16.1.7

## show sessions

The show sessions User EXEC mode command lists the open Telnet sessions.

### Syntax

- show sessions  
This command has no arguments or keywords.

### Default Configuration

There is no default configuration for this command.

### Command Mode

User EXEC mode.

### User Guidelines

- 1 Open telnet session from PC 5400 to other device.
- 2 In the other device syntax, press **Ctrl-shift-t-X**
- 3 Enter the command **show session**. The number of sessions opened from PC 5400 is displayed.
- 4 Enter the command **resume [number of session]** to return to the relevant telnet session.



## Examples

The following table describes the significant fields shown in the display:

```
Console> show sessions
```

Connection	Host	Address	Port	Byte
1	Remote device	172.16.1.1	23	89
2	172.16.1.2	172.16.1.2	23	8

Field	Description
Connection	Connection number
Host	Remote host to which the device is connected through a Telnet session.
Address	IP address of the remote host.
Port	Telnet TCP port number
Byte	Number of unread bytes for the user to see on the connection.

## show system

The `show system` User EXEC mode command displays system information.

### Syntax

- `show system`

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

There are no user guidelines for this command.

## Example

The following example displays the system information.

```
console> show system
System Description:                Kenan 24
System Up Time (days,hour:min:sec): 00,05:19:48
System Contact:
System Name:                       RS1
System location:
System MAC Address:                00:00:b0:00:00:00
Sys Object ID:                    1.3.6.1.4.1.674.10895.3020
                                   PowerConnect 5400

Type:
Main Power Supply      ok
Status
Redundant Power       ok
Supply Status:
Fan 1 Status:         OK
Fan 2 Status:         OK
console>
```

## set system

The `set system` Privileged EXEC command activates/deactivates specified features.

### Syntax

- `set system {iscsi | dva}`
  - `iscsi` — The device supports iscsi and ACL.
  - `dva` — The device supports DVA and ACL.

### Default Configuration

By default the device supports iscsi.

### Command Mode

Privileged EXEC mode

### User Guidelines

- Only after reboot is the command implemented. During reboot the startup-config is deleted. It is highly recommended to backup the startup-config before executing this command.

### Example

The following example enables support for ACLs and DVA.

```
Console# set system dva
```

## show system mode

The `show system mode` User EXEC mode command displays information on features control.

### Syntax

- `show system mode {mode | defaults | id}`
  - `defaults` — Displays the system default configuration.
  - `id` — Displays the system identity information.

### Default Configuration

This command has no default setting.

### Command Mode

User EXEC mode

### User Guidelines

There are no user guidelines for this command.

### Example

The following example displays information on features control.

```
Console> show system mode
Feature          State
-----          -
ACL              Active
DVA              Active
ISCSI            Inactive
```

## show version

The `show version` User EXEC mode command displays the system version information.

### Syntax

- `show version`

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays a system version (this version number is only for demonstration purposes).

```
Console# show version
SW version 1.0.0.1 ( date Jun 26 2008 time 19:08:13 )
Boot version      ( date time )
HW version       1.0.0
console#
```

## asset-tag

The `asset-tag` Global Configuration mode command specifies the device asset tag. Use the **no** form of the command to remove the existing asset tag.

### Syntax

- `asset-tag tag`
- `no asset-tag`
  - *tag* — The device asset tag. (Range: 1- 16 characters)

### Default Configuration

This command has no default configuration. No asset tag is defined by default.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example specifies the device asset tag as "lqwepot".

```
Console (config)# asset-tag lqwepot
```

## show system id

The `show system id` User EXEC mode command displays the ID information.

### Syntax

- `show system id`

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- The tag information is on a device by device basis.

### Example

The following example displays the system service tag information.

```
Console> show system id  
Serial number : 123456789  
Service tag   :  
Asset tag     :
```



# TACACS Commands

## tacacs-server host

The `tacacs-server host` Global Configuration mode command specifies a TACACS+ host. Use the `no` form of this command to delete the specified name or address.

### Syntax

- `tacacs-server host {ip-address | hostname} [single-connection] [port port-number] [timeout timeout] [key key-string] [source source] [priority priority]`
- `no tacacs-server host {ip-address | hostname}`
  - *ip-address* — Name or IP address of the host.
  - *hostname* — Hostname of the tacacs server. (Range: 1 - 158 characters)
  - **single-connection** — Specify single-connection. Rather than have the device open and close a TCP connection to the daemon each time it must communicate, the `single-connection` option maintains a single open connection between the device and the daemon.
  - *port-number* — Specify a server port number. If unspecified, the port number defaults to 49. (Range: 0 - 65535)
  - *timeout* — Specifies the timeout value in seconds. If no timeout value is specified, the global value is used. (Range: 1 - 30)
  - *key-string* — Specifies the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the encryption used on the TACACS daemon. If no key string value is specified, the global value is used. (Range: 0 - 128 characters)
  - *source* — Specifies the source IP address to use for the communication. If no source value is specified, the global value is used.
  - *priority* — Determines the order in which the servers will be used, when 0 is the highest priority. If unspecified defaults to 0. (Range: 0 - 65535)

### Default Configuration

No TACACS host is specified.

### Command Mode

Global Configuration mode.

## User Guidelines

- Multiple `tacacs-server host` commands can be used to specify multiple hosts.
- If no host-specific timeout, key or source values are specified, the global values apply to each host.

## Example

The following example specifies a TACACS+ host.

```
Console (config)# tacacs-server host 172.16.1.1
```

## tacacs-server key

The `tacacs-server key` Global Configuration mode command sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon. Use the `no` form of this command to disable the key.

## Syntax

- `tacacs-server key key-string`
- `no tacacs-server key`
  - *key-string* — Specifies the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the encryption used on the TACACS daemon. (Range: 0 - 128 characters)

## Default Configuration

Empty string.

## Command Mode

Global Configuration mode.

## User Guidelines

- There are no user guidelines for this command.

## Examples

The following example sets the authentication encryption key.

```
Console (config)# tacacs-server key dell-s
```

## tacacs-server timeout

The `tacacs-server timeout` Global Configuration mode command sets the timeout value. Use the `no` form of this command to restore the default.



### Syntax

- `tacacs-server timeout timeout`
- `no tacacs-server timeout`
  - *timeout* — Specifies the timeout value in seconds. (Range: 1 - 30)

### Default Configuration

5 seconds.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example sets the timeout value as 30.

```
Console (config)# tacacs-server timeout 30
```

## tacacs-server source-ip

The `tacacs-server source-ip` Global Configuration mode command specifies the source IP address that will be used for the communication with TACACS servers. Use the `no` form of this command to return to default.

### Syntax

- `tacacs-server source-ip source`
- `no tacacs-server source-ip source`
  - *source* — Specifies the source IP address. (Range: Valid IP Address)

### Default Configuration

The IP address would be of the outgoing IP interface.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

## Examples

The following example specifies the source IP address.

```
Console (config)# tacacs-server source-ip 172.16.8.1
```

## show tacacs

The `show tacacs` Privileged EXEC mode command displays configuration and statistics for a TACACS+ server.

### Syntax

- `show tacacs [ip-address]`
  - *ip-address* — Host name or IP address of the host.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

## Examples

The following example displays configuration and statistic for a TACACS+ server.

```
Console# show tacacs
IP address      Status        Port          Single
Connection     TimeOut      Source IP     Priority
-----
172.16.1.1     Connected    49           No
Global values
-----
TimeOut: 3
Source IP: 172.16.8.1
```

# TIC Commands

## passwords min-length

The `passwords min-length` Global Configuration mode command configures the minimal length required for passwords in the local database. Use the `no` form of this command to remove a requirement.

### Syntax

- `passwords min-length length`
- `no passwords min-length`
  - *length* — The minimal length required for passwords.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- The setting is relevant to local users passwords, line passwords and enable passwords.
- The software checks the minimum length requirement when a password is defined in an unencrypted format, or when a user tries to login.
- Note that if a password is inserted in encrypted format, the minimum length requirement only gets checked when the user logs in.
- In a similar way; passwords defined before the minimum length is defined only require being checked when the user logs in.

### Example

The following example configures the length for passwords in the local database to 6 characters.

```
Console (config)# passwords min-length length 6
```

## password-aging

The **password-aging** Line Configuration mode command configures the aging time of line passwords. To disable password expiration time use the **no** form of this command.

### Syntax

- **password-aging** *days*
- **no password-aging**
  - *days* — The number of days before a password change is forced. (Range: 1-365)

### Default Configuration

Password aging is disabled.

### Command Mode

Line Configuration mode.

### User Guidelines

- The aging time is calculated from the day the password is defined (not from the day the aging is defined).
- After a password expires a user can login for another 3 times.
- 10 days before expiration a syslog message is generated.

### Example

The following example configures 5 days as the aging time of line passwords.

```
Console (config-line)# password-aging 5
```

## passwords aging

The **passwords aging** Global Configuration mode command configures the aging time of username passwords and enables passwords. To disable password expiration time use the **no** form of this command.

### Syntax

- **passwords aging** username *name* *days*
- **no passwords aging** username *name*
- **passwords aging enable-password** *level* *days*
- **no passwords aging enable-password** *level*
  - *name* — The name of the user. (Range: 1 - 20 characters)
  - *level* — The level for which the password applies. (Range: 1 - 15)
  - *days* — The number of days before a password change is forced. (Range: 1 - 365)

### Default Configuration

Password aging is disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- The aging time is calculated from the day the password was defined, and not from the day the aging was defined.
- After a password expires a user can login for another 3 times.
- 10 days before expiration a syslog message is generated.

### Example

The following example configures configures 40 days as the aging time of global passwords.

```
Console (config)# passwords aging username 40
```

### passwords history

The `passwords history` Global Configuration mode command configures the number of password changes that are required before a password in the local database can be reused. To remove the requirement use the `no` form of this command.

### Syntax

- `passwords history number`
- `no passwords history`
  - *number* — The number of password changes before a password can be reused. (Range: 1-10).

### Default Configuration

Passwords history is disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- The setting is relevant to local users passwords, line passwords and enable passwords.
- Password history is not checked during download of configuration.
- The history of passwords is kept even if the passwords history check is disabled.
- The history of passwords for a user is kept as long as the user is defined.

## Example

The following example configures the required number of password changes before a password can be reused to 3.

```
Console (config)#passwords history 3
```

## passwords history hold-time

The **passwords history hold-time** Global Configuration mode command configures the duration that a password is relevant for tracking passwords history. To return to default use the **no** form of this command.

### Syntax

- **passwords history hold-time** *days*
- **no passwords history hold-time**
  - *days* — The number of days for which a password is relevant for tracking passwords history. (Range: 1 - number of days the password's history is defined as the passwords history to be active).

### Default Configuration

Disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- The setting is relevant to local users passwords, line passwords and enable passwords.
- The passwords are not deleted from the history database when they are not relevant for the passwords history tracking. Increasing the hold time might 'return back' passwords.

## Example

The following example configures the duration that a password is relevant for tracking passwords history.

```
Console (config)# passwords history hold-time 10
```

## passwords lockout

The **passwords lockout** Global Configuration mode command enables lockout of a user account after a series of authentication failures. To disable lockout use the **no** form of this command.

## Syntax

- `passwords lockout` *number*
- `no passwords lockout`
  - *number* — The number of authentication failures before the user account is locked-out. (Range: 1-5).

## Default Configuration

Lockout is disabled.

## Command Mode

Global Configuration mode.

## User Guidelines

- The setting is relevant to local users passwords, line passwords and enable passwords.
- The account is not locked out for access from local console.
- A user that has privilege level 15 can release accounts that are locked out by using the `set username active`, `'set enable-password active'` and `'set line active'` privileged EXEC commands.
- Disabling lockout unlocks all users.
- Re-enabling lockout resets the authentication failures counters.
- Changing the authentication failures threshold does not reset the counters.

## Example

The following example enables lockout of a user account after a series of five failures.

```
Console (config)# passwords lockout 5
```

## aaa login-history file

The `aaa login-history file` Global Configuration mode command enables writing to login history file. To disable writing to the file use the `no` form of this command.

## Syntax

- `aaa login-history file`
- `no aaa login-history file`

## Default Configuration

Enabled.

## Command Mode

Global Configuration mode.

## User Guidelines

- The login history is still kept in the device internal buffer.

## Example

The following example enables writing to login history file.

```
Console (config)# aaa login-history file
```

## set username active

The `set username active` Privileged EXEC mode command reactivates a locked out user account.

## Syntax

- `set username name active`
  - *name* — The user name. (Range 1 - 20 characters)

## Default Configuration

This command has no default configuration.

## Command Mode

Privileged EXEC mode.

## Example

The following example reactivates a locked out user account for Bob.

```
Console# set username bob active
```

## set line active

The `set line active` Privileged EXEC mode command reactivates a locked out line.

## Syntax

- `set line {console | telnet | ssh} active`
  - `console` — Console terminal line.
  - `telnet` — Virtual terminal for remote console access (Telnet).
  - `ssh` — Virtual terminal for secured remote console access (SSH).

## Default Configuration

This command has no default configuration.



**Command Mode**

Privileged EXEC mode.

**Example**

The following example reactivates a locked out telnet line.

```
Console# set line telnet active
```

**set enable-password active**

The `set enable-password active` Privileged EXEC mode command reactivates a locked out local password.

**Syntax**

- `set enable-password level active`
  - *level* — The level for which the password applies. (Range 1 - 15)

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode.

**Example**

The following example reactivates a previously locked out local password at level 3.

```
Console# set enable-password 3 active
```

**show passwords configuration**

The `show passwords configuration` Privileged EXEC mode command displays information about the passwords management configuration.

**Syntax**

- `show passwords configuration`

**Default Configuration**

This command has no default configuration.

**Command Mode**

Privileged EXEC mode.

### Example

The following example displays information about password management in the local database.

---

```
Console# show passwords configuration
```

```
Minimal length: 8
```

```
History: 10
```

```
History hold time: 365 days
```

```
Lock-out: Disabled
```

#### Enable Passwords

Level	Aging	Expiry date	Lockout
-----	-----	-----	-----
1	90	Jan 18 2005	1
15	90	Jan 18 2005	0

#### Line Passwords

Level	Aging	Expiry date	Lockout
-----	-----	-----	-----
Console	-	-	-
Telnet	90	Jan 18 2005	LOCKOUT
SSH	90	Jan 21 2005	0

---

The following table describes the significant fields shown in the display:

Field	Description
Minimal length	The minimal length required for passwords in the local database.
History	The number of passwords changes required before a password in the local database can be reused.
History hold time	The duration that a password is relevant for tracking passwords history.
Lockout control	Control lockout of a user account after series of authentication failures.
Level	Configuration and status for local password of specific level.
Aging	The aging time in days of a password.
Expiry date	The expiry date of a password.

Lockout	If lockout control is enabled, it specifies how many times a user has failed to enter the correct password since the last successful login. If the password is locked out it specifies “LOCKOUT”.
Line	Configuration and status for specific line password.

### show users login-history

The **show users login-history** Privileged EXEC mode command displays information about the login history of users.

#### Syntax

- **show users login-history** [*username name*]
  - *name* — The name of the user. (Range 1 - 20 characters)

#### Default Configuration

This command has no default configuration.

#### Command Mode

Privileged EXEC mode.

#### Example

The following example displays the login history of users.

---

```
Console# show users login-history
```

Login Time	Username	Protocol	Location
-----	-----	-----	-----
Jan 18 2004 23:58:17	Robert	HTTP	172.16.1.8
Jan 19 2004 07:59:23	Robert	HTTP	172.16.0.8
Jan 19 2004 08:23:48	Bob	Serial	
Jan 19 2004 08:29:29	Robert	HTTP	172.16.0.8
Jan 19 2004 08:42:31	John	SSH	172.16.0.1
Jan 19 2004 08:49:52	Betty	Telnet	172.16.1.7

---



# Tunnel

## interface tunnel

The **interface tunnel** Global Configuration mode command enters tunnel interface configuration mode.

### Syntax

- **interface tunnel** *number*
  - *number* — Tunnel index. (Range: 1)

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enters tunnel interface configuration mode to configure tunnel 1.

```
Console (config)# interface tunnel 1
Console (config-tunnel)#
```

## tunnel mode ipv6ip

The **tunnel mode ipv6ip** Interface Tunnel Configuration mode command configures an IPv6 transition mechanism global support mode. Use the **no** form of this command to remove the IPv6 transition mechanism.

### Syntax

- `tunnel mode ipv6ip {isatap}`
- `no tunnel mode ipv6ip`
  - `isatap` — Automatic IPv6 over IPv4 ISATAP tunnel is enabled.

### Default Configuration

Disabled.

### Command Mode

Interface Tunnel Configuration mode.

### User Guidelines

- The system can be enabled to an ISATAP tunnel. When enabled, an automatic tunnel interface is created on each interface that is assigned with IPv4 address.



**NOTE:** On a specific interface (that is port/ VLAN), both native IPV6 and transition mechanisms can coexist. The host implementation selects the egress interface according to the scope of the destination IP address (for example ISATAP/ Native IPv6).

### Example

The following example configures an IPv6 transition mechanism global support mode.

```
Console (config)# interface tunnel 1
Console (config-tunnel)# tunnel mode ipv6ip
```

## tunnel isatap router

The `tunnel isatap router` Interface Tunnel Configuration mode command configures a global string that represents a specific automatic tunnel router domain name. Use the `no` form of this command to remove the string associated with the router domain name and return to the default.

### Syntax

- `tunnel isatap router router_name`
- `no tunnel isatap router`
  - *router\_name* — A string representing the router's domain name.

### Default Configuration

By default, 'ISATAP' string represents the corresponding automatic tunnel router's domain name.

### Command Mode

Interface Tunnel Configuration mode.

## User Guidelines

- The `ipv6 tunnel routers-dns` command determines the string that the host uses for automatic tunnel router lookup in IPv4 DNS procedure. By default, the string 'ISATAP' is used for the corresponding automatic tunnel types.
- Per tunnel only one string can represent the automatic tunnel router name. Using this command overwrites the existing entry.

## Example

The following example configures a global string "Dell\_Tunnel\_Router" to represent a specific automatic tunnel router domain name..

```
Console (config)# interface tunnel 1
Console (config-tunnel)# tunnel isatap router Dell_Tunnel_Router
```

## tunnel source

The `tunnel source` Interface Tunnel Configuration mode command sets the local (source) tunnel interface IPv4 address. Use the `no` form to delete the tunnel local address.

## Syntax

- `tunnel source { auto | ip-address ipv4-address }`
- `no tunnel source`
  - **auto** — The system minimum IPv4 address is used as the source address for packets sent on the tunnel interface. If the IPv4 address is changed then the local address of the tunnel interface is also changed.
  - *ip4-address* — Pv4 address to use as the source address for packets sent on the tunnel interface. The tunnel interface local address is not changed when the IPv4 address is moved to another interface.

## Default Configuration

No source address is defined.

## Command Mode

Interface Tunnel Configuration mode.

## User Guidelines

- The configured source IPv4 address is used for forming the tunnel interface identifier. The interface identifier is set to the 8 least significant bytes of the SIP field of the encapsulated IPv6 tunneled packets.

### Example

The following example sets the local (source) tunnel interface IPv4 address.

```
Console (config)# interface tunnel 1
Console (config-tunnel)# tunnel source auto
```

## tunnel isatap query-interval

The **tunnel isatap query-interval** Global Configuration mode command configures the interval between DNS Queries (before the IP address of the ISATAP router is known) for the automatic tunnel router domain name. Use the **no** form of this command to return to default.

### Syntax

- **tunnel isatap query-interval** *seconds*
- **no tunnel isatap query-interval**
  - *seconds* — Specify the number of seconds between DNS Queries. (Range: 10 – 3600)

### Default Configuration

10 seconds.

### Command Mode

Global Configuration mode.

### User Guidelines

- This command determines the interval of DNS queries before the IP address of the ISATAP router is known. When the IP address is known the robustness level that is set by the **tunnel isatap robustness** global configuration command determines the refresh rate.

### Example

The following example configures the interval between DNS Queries for the automatic tunnel router domain to 60 seconds.

```
Console (config)# tunnel isatap query-interval 60
```

## tunnel isatap solicitation-interval

The **tunnel isatap solicitation-interval** Global Configuration mode command configures the interval between ISATAP router solicitations messages (when there is no active ISATAP router). Use the **no** form of this command to return to default.



### Syntax

- **tunnel isatap solicitation-interval** *seconds*
- **no tunnel isatap solicitation-interval**
  - *seconds* — Specify the number of seconds between ISATAP router solicitations messages. (Range: 10 – 3600)

### Default Configuration

10 seconds.

### Command Mode

Global Configuration mode.

### User Guidelines

- This command determines the interval of Router Solicitation messages when there is no active ISATAP router. When there is an active ISATAP router, the robustness level that is set by the **tunnel isatap robustness** global configuration command determines the refresh rate.

### Example

The following example configures the interval between ISATAP router solicitations messages to 60 seconds.

```
Console (config)# tunnel isatap solicitation-interval 60
```

## tunnel isatap robustness

The **tunnel isatap robustness** Global Configuration mode command configures the number of DNS Query/Router Solicitation refresh messages that the device sends. Use the **no** form of this command to return to default.

### Syntax

- **tunnel isatap robustness** *number*
- **no tunnel isatap robustness**
  - *number* — Specify the number of refresh messages. (Range: 1 – 20)

### Default Configuration

3 times.

### Command Mode

Global Configuration mode.

### User Guidelines

- The DNS query interval (after the IP address of the ISATAP router is known) is the TTL that is received from the DNS divided by (Robustness + 1).
- The router solicitation interval (when there is an active ISATAP router) is the minimum-router-lifetime that is received from the ISATAP router divided by (Robustness + 1).

### Example

The following example configures the number of DNS Query/Router Solicitation refresh messages that the device sends to 6 times.

```
Console (config)# tunnel isatap robustness 6
```

## show ipv6 tunnel

The `show ipv6 tunnel` Privileged EXEC mode command displays information on the ISATAP tunnel.

### Syntax

- `show ipv6 tunnel`

### Default Configuration

This command has no default setting.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

**Example**

The following example displays information on the ISATAP tunnel.

```
Console> show ipv6 tunnel

Router DNS name: ISATAP
Router IPv4 address: 172.16.1.1
DNS Query interval: 10 seconds
Min DNS Query interval: 0 seconds
Router Solicitation interval: 10 seconds
Min Router Solicitation interval: 0 seconds
Robustness: 3
```



## User Interface

### enable

The `enable` User EXEC mode command enters the privileged EXEC mode.

#### Syntax

- `enable` [*privilege-level*]
  - *privilege-level* — Privilege level to enter the system. (Range: 1 - 15)

#### Default Configuration

The default privilege level is 15.

#### Command Mode

User EXEC mode.

#### User Guidelines

- There are no user guidelines for this command.

#### Example

The following example shows how to enter privileged mode:

```
Console> enable
enter password:
Console#
```

### disable

The `disable` Privileged EXEC mode command returns to User EXEC mode.

#### Syntax

- `disable` [*privilege-level*]
  - *privilege-level* — Privilege level to enter the system. (Range: 1 - 15)

### Default Configuration

The default privilege level is 1.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows how to return to normal mode.

```
Console# disable  
Console>
```

## login

The `login` User EXEC mode command changes a login username.

### Syntax

- `login`

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows how to enter privileged EXEC mode and login.

```
Console> login  
User Name:admin  
Password:*****  
  
Console#
```

# configure

The `configure` Privileged EXEC mode command enters the Global Configuration mode.

## Syntax

- `configure`  
This command has no keywords or arguments.

## Default Configuration

This command has no default configuration.

## Command Mode

Privileged EXEC mode.

## User Guidelines

- There are no user guidelines for this command.

## Example

In the following example, because no keyword is entered, a prompt is displayed. After the keyword is selected, a message confirming the command entry method is displayed.

```
Console# configure  
Console (config)#
```

# exit(configuration)

The `exit` command exits any configuration mode to the next highest mode in the CLI mode hierarchy.

## Syntax

- `exit`

## Default Configuration

This command has no default configuration.

## Command Mode

All command modes.

## User Guidelines

- There are no user guidelines for this command.

### Example

The following example changes the configuration mode from Interface Configuration mode to User EXEC mode.

```
Console(config-if)# exit  
Console(config)# exit  
Console#
```

## exit(EXEC)

The **exit** User EXEC mode command closes an active terminal session by logging off the device.

### Syntax

- **exit**

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC mode .

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example closes an active terminal session.

```
Console> exit
```

## end

The **end** Global Configuration mode command ends the current configuration session and returns to the privileged command mode.

### Syntax

- **end**

### Default Configuration

This command has no default configuration.



**Command Mode**

All Command modes.

**User Guidelines**

- There are no user guidelines for this command.

**Example**

The following example ends the current configuration session and returns to the previous command mode.

```
Console (config)# end
Console #
```

## help

The **help** command displays a brief description of the help system.

**Syntax**

- help

**Default Configuration**

This command has no default configuration.

**Command Mode**

All Command modes.

**User Guidelines**

- There are no user guidelines for this command.

## history

The **history** Line Configuration mode command enables the command history function. Use the **no** form of this command to disable the command history feature.

**Syntax**

- history
- no history

**Default Configuration**

The history function is enabled.

### Command Mode

Line Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enables the command history function for telnet.

```
Console (config)# line telnet
Console (config-line)# history
```

## terminal datadump

The **terminal datadump** EXEC mode command enables dumping of all the output from the show command without 'prompting'. Use the **no** form of this command to disable dumping.

### Syntax

- terminal datadump
- no terminal datadump

### Default Configuration

Data dump is disabled.

### Command Mode

Privilege EXEC command mode.

### User Guidelines

- By default when output continues beyond what is displayed on the screen, the CLI displays a **--More--** prompt. Pressing Return displays the next line; pressing the Spacebar displays the next output screen. The datadump feature enables the dumping of all the output immediately after entering the show command for the current terminal session.

### Example

The following example enables dumping of all the output from show command without 'prompting'.

```
console# terminal datadump
```

## history size

The **history size** Line Configuration mode command changes the command history buffer size for a particular line. Use the **no** form of this command to reset the command history buffer size to the default.

### Syntax

- **history size** *number-of-commands*
- **no history size**
  - *number-of-commands* — Number of commands that the system records in its history buffer.  
(Range: 10 - 256)

### Default Configuration

The default history buffer size is 10.

### Command Mode

Line Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example changes the command history buffer size to 100 entries for a particular line.

```
Console (config-line)# history size 100
```

## debug-mode

The **debug-mode** Privilege EXEC mode command switches the mode to debug.

### Syntax

- **debug-mode**

### Default Configuration

This command has no default configuration.

### Command Mode

Privilege EXEC command mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enables the debug command interface.

```
console(config)#
console# debug
>debug
Enter DEBUG Password: *****
DEBUG>
```

## show history

The `show history` User EXEC mode command lists the commands entered in the current session.

### Syntax

- `show history`

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC command mode.

### User Guidelines

- The commands are listed from the first to the latest command.
- The buffer is kept unchanged when entering to configuration mode and returning back.
- The command in the buffer includes the commands that were not executed.

### Example

The following example displays all the commands entered while in the current privileged EXEC mode.

```
Console# show history
show version
show clock
show history
```

## show privilege

The `show privilege` User EXEC mode command displays the current privilege level.

### Syntax

- `show privilege`

### Default Configuration

This command has no default configuration.

### Command Mode

User EXEC command mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the current privilege level.

```
Console# show privilege  
Current privilege level is 15
```

## do

The `do` EXEC-level command executes a Global Configuration mode or any configuration submode.

### Syntax

- `do command`

### Default Configuration

This command has no default configuration.

### Command Mode

All configuration modes.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays VLAN information.

```
Console (Config)# do show vlan
```

VLAN	Name	Ports	Type	Authorization
1	default	g1-2 g1-4	Other	Required
10	VLAN0010	g3-4	dynamic	Required
11	VLAN0011	g1-2	static	Required
20	VLAN0020	g3-4	static	Required
21	VLAN0021		static	Required
30	VLAN0030		static	Required
31	VLAN0031		static	Required
91	VLAN0011	g1-2	static	Not Required
3978	Guest VLAN	g17	static	Guest

# VLAN Commands

## vlan database

The `vlan database` Global Configuration mode command enters the VLAN Database Configuration mode.

### Syntax

- `vlan database`

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example enters the VLAN database mode.

```
Console (config)# vlan database
Console (config-vlan)#
```

## vlan

Use the `vlan` VLAN Configuration mode command to create a VLAN. Use the `no` form of this command to delete a VLAN.

### Syntax

- `vlan {vlan-range}`
- `no vlan {vlan-range}`
  - *vlan-range* — A list of valid VLAN IDs to be added. List separate, non-consecutive VLAN IDs separated by commas (without spaces); use a hyphen to designate a range of IDs. (Range: 2 - 4094)

### Default Configuration

This command has no default configuration.

### Command Mode

VLAN Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example VLAN number 1972 is created.

```
Console (config)# vlan database  
Console (config-vlan)# vlan 1972
```

## interface vlan

The **interface vlan** Global Configuration mode command enters the Interface Configuration (VLAN) mode.

### Syntax

- **interface vlan** *vlan-id*
  - *vlan-id* — The ID of an existing VLAN (excluding GVRP dynamic VLANs).

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the VLAN 1 IP address of 131.108.1.27 and subnet mask 255.255.255.0.

```
Console (config)# interface vlan 1  
Console (config-if)# ip address 131.108.1.27 255.255.255.0
```



## interface range vlan

The **interface range vlan** Global Configuration mode command enters the Interface Configuration mode to configure multiple VLANs.

### Syntax

- **interface range vlan** {*vlan-range* | **all**}
  - *vlan-range* — A list of valid VLAN IDs to add. Separate non consecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs.
  - **all** — All existing static VLANs.

### Default Configuration

This command has no default configuration.

### Command Mode

Global Configuration mode.

### User Guidelines

- Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, an error message is displayed and execution continues on other interfaces.

### Example

The following example groups VLAN 221 until 228 and VLAN 889 to receive the same command.

```
Console (config)# interface range vlan 221-228,889
Console (config-if)#
```

## name

The **name** Interface Configuration mode command adds a name to a VLAN. Use the **no** form of this command to remove the VLAN name.

### Syntax

- **name** *string*
- **no name**
  - *string* — Unique name, up to 32 characters in length, to be associated with this VLAN.

### Default Configuration

No name is defined.

### Command Mode

Interface Configuration (VLAN) mode.

### User Guidelines

- The VLAN name should be unique.

### Example

The following example names VLAN number 19 with the name "Marketing".

```
Console (config)# interface vlan 19
Console (config-if)# name Marketing
```

## switchport access vlan

The `switchport access vlan` Interface Configuration mode command configures the VLAN ID when the interface is in access mode. Use the `no` form of this command to reconfigure the default.

### Syntax

- `switchport access vlan vlan-id`
- `no switchport access vlan`
  - *vlan-id* — VID of the VLAN to which the port is configured.

### Default Configuration

VID=1.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- The command automatically removes the port from the previous VLAN, and adds it to the new VLAN.

### Example

The following example configures a VLAN ID of 23 to the untagged layer 2 VLAN interface number g8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport access vlan 23
```

## switchport trunk allowed vlan

The `switchport trunk allowed vlan` Interface Configuration mode command adds or removes VLANs, to or from a trunk port.

### Syntax

- `switchport trunk allowed vlan {add vlan-list | remove vlan-list}`
  - `add vlan-list` — List of VLAN IDs to add. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
  - `remove vlan-list` — List of VLAN IDs to remove. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designate a range of IDs.

### Default Configuration

This command has no default configuration.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows how to add VLANs 2 and 5 to 8 to the allowed list of g8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport trunk allowed vlan add 2,5-8
```

## switchport trunk native vlan

The `switchport trunk native vlan` Interface Configuration mode command defines the port as a member of the specified VLAN, and the VLAN ID as the 'port default VLAN ID (PVID)'. Use the `no` form of this command to configure the default VLAN ID.

### Syntax

- `switchport trunk native vlan vlan-id`
- `no switchport trunk native vlan`
  - *vlan-id* — Valid VLAN ID of the native VLAN.

### Default Configuration

If default VLAN is enabled, then the VID=1, otherwise VID = 4095.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- This command has the following consequences: incoming untagged frames are assigned to this VLAN and outgoing traffic in this VLAN on this port is sent untagged (despite the normal situation where traffic sent from a trunk-mode port is all tagged).
- The command adds the port as a member in the VLAN. If the port is already a member in the VLAN (not as a native), it should be first removed from the VLAN.

### Example

The following example g8, in trunk mode, is configured to use VLAN number 123 as the "native" VLAN.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport trunk native vlan 123
```

## switchport general allowed vlan

The `switchport general allowed vlan` Interface Configuration mode command adds or removes VLANs from a general port.

### Syntax

- `switchport general allowed vlan add vlan-list [tagged | untagged]`
- `switchport general allowed vlan remove vlan-list`
  - **add *vlan-list*** — List of VLAN IDs to add. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
  - **remove *vlan-list*** — List of VLAN IDs to remove. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
  - **tagged** — Sets the port to transmit tagged packets for the VLANs. If the port is added to a VLAN without specifying tagged or untagged the default is tagged.
  - **untagged** — Sets the port to transmit untagged packets for the VLANs.

### Default Configuration

This command has no default configuration.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- You can use this command to change the egress rule (e.g. from tagged to untagged), without first removing the VLAN from the list.

### Example

The following example shows how to add VLANs 2, 5, and 6 to the allowed list.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general allowed vlan add 2,5,6
tagged
```

## switchport general pvid

The `switchport general pvid` Interface Configuration mode command configures the PVID when the interface is in general mode. Use the `no` form of this command to configure the default value.

### Syntax

- `switchport general pvid vlan-id`
- `no switchport general pvid`
  - *vlan-id* — PVID (Port VLAN ID). The *vlan-id* may belong to a non-existent VLAN.

### Default Configuration

VLAN ID=1

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- This command has the following consequences: incoming untagged frames are assigned to this VLAN and outgoing traffic in this VLAN on this port is sent untagged (despite the normal situation where traffic sent from a trunk-mode port is all tagged).

### Example

The following example shows how to configure the PVID for `g8`, when the interface is in general mode.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general pvid 234
```

## switchport general ingress-filtering disable

The `switchport general ingress-filtering disable` Interface Configuration mode command disables port ingress filtering. Use the `no` form of this command to enable ingress filtering on a port.

### Syntax

- `switchport general ingress-filtering disable`
- `no switchport general ingress-filtering disable`

### Default Configuration

Ingress filtering is enabled.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example shows how to enable port ingress filtering on g8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general ingress-filtering disable
```

## switchport general acceptable-frame-type tagged-only

The `switchport general acceptable-frame-type tagged-only` Interface Configuration mode command discards untagged frames at ingress. Use the `no` form of this command to enable untagged frames at ingress.

### Syntax

- `switchport general acceptable-frame-type tagged-only`
- `no switchport general acceptable-frame-type tagged-only`

### Default Configuration

All frame types are accepted at ingress.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

## User Guidelines

- There are no user guidelines for this command.

## Example

The following example configures g8 to discard untagged frames at ingress.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general acceptable-frame-type
tagged-only
```

## switchport forbidden vlan

The `switchport forbidden vlan` Interface Configuration mode command forbids adding specific VLANs to a port. This may be used to prevent GVRP from automatically making these VLANs active on the selected ports. To revert to allowing the addition of specific VLANs to the port, use the `remove` parameter for this command.

## Syntax

- `switchport forbidden vlan {add vlan-list | remove vlan-list}`
  - `add vlan-list` — List of VLAN IDs to add to the "forbidden" list. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
  - `remove vlan-list` — List of VLAN IDs to remove from the "forbidden" list. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

## Default Configuration

All VLANs allowed.

## Command Mode

Interface Configuration (Ethernet, port-channel) mode.

## User Guidelines

- There are no user guidelines for this command.

## Example

The following example forbids adding VLANs number 234 till 256, to g8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport forbidden vlan add 234-256
```

## switchport mode

Use the **switchport mode** Interface Configuration command to configure the VLAN membership mode of a port. Use the **no** form of this command to reset the mode to the appropriate default for the device.

### Syntax

- `switchport mode { access | trunk | general | customer }`
- `no switchport mode`
  - **customer** — The port is connected to customer equipment. Used when the switch is in a provider network.
  - **access** — Untagged layer 2 VLAN interface
  - **trunk** — Trunking layer 2 VLAN interface
  - **general** — Full 802.1q support VLAN interface

### Default Configuration

Depends on the specific box.

### Command Modes

Interface Configuration (Ethernet, port-channel)mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the VLAN membership mode of a port. Use the **no** form of this command to reset the mode to the appropriate default for the device.

```
console# config
console(config)# interface ethernet g1
console(config-if)# switchport mode customer
```

## switchport customer vlan

The **switchport customer vlan** Interface Configuration (Ethernet, port-channel) mode command sets the port's VLAN when the interface is in customer mode. Use the **no** form of this command to restore the default configuration.

### Syntax

- `switchport customer vlan vlan-id`
- `no switchport customer vlan`



### Default Configuration

No VLAN is configured.

### Command Modes

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- There are no user guidelines for this command.

Example

**The following example sets the port's VLAN when the interface is in customer mode.**

```
Console(config)# switchport customer vlan vlan-id
```

## map protocol protocols-group

The `map protocol protocols-group` VLAN Configuration mode command maps a protocol to a protocol group. Protocol groups are used for protocol-based VLAN assignment. Use the **no** form of this command to delete a protocol from a group.

### Syntax

- `map protocol protocol [encapsulation] protocols-group group`
- `no map protocol protocol encapsulation`
  - *protocol* — The protocol is a 16 or 40 bits protocol number or one of the following names; ip, arp, ipv6, and ipx. The protocol number is in Hex format. (Range: 0600 - FFFF)
  - *encapsulation* — One of the following values: **ethernet**, **rfc1042** or **llcOther**. If no option is indicated the default is **ethernet**.
  - *group* — Protocol group number. (Range: 1 - 2147483647)

### Default Configuration

This command has no default configuration.

### Command Mode

VLAN Configuration mode.

### User Guidelines

There are no user guidelines for this command.

### Example

The following example maps protocol ip-arp to the group named "213".

```
Console (config)# vlan database  
Console (config-vlan)# map protocol ip-arp protocols-group 213
```

## switchport general map protocols-group vlan

The `switchport general map protocols-group vlan` Interface Configuration mode command sets a protocol-based classification rule. Use the `no` form of this command to delete a classification.

### Syntax

- `switchport general map protocols-group group vlan vlan-id`
- `no switchport general map protocols-group group`
  - *group* — Group number as defined in the `map protocol protocols-group` command. (Range: 1 - 2147483647)
  - *vlan-id* — Define the VLAN ID in the classifying rule.

### Default Configuration

This command has no default configuration.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example sets a protocol-based classification rule of protocol group 1 to VLAN 8.

```
Console (config)# interface ethernet g8  
Console (config-if)# switchport general map protocols-group 1 vlan 8
```

## switchport protected

The `switchport protected` Interface Configuration mode command overrides the FDB decision, and sends all the Unicast, Multicast and Broadcast traffic to an uplink port. Use the **no** form of this command to disable overriding the FDB decision.

### Syntax

- `switchport protected {ethernet port | port-channel port-channel-number }`
- `no switchport protected`
  - *port* — Specifies the uplink port (Ethernet port).
  - *port-channel-number* — Specifies the uplink port (Port-channel).

### Default Configuration

The default configuration is **disabled**.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

Packets to the device MAC address are sent to the device and not forwarded to the uplink.

### Example

The following example overrides the FDB decision, and sends all the Unicast, Multicast and Broadcast traffic to specified ethernet port.

```
Console(config)# interface ethernet g/g5
Console(config-if)# switchport protected ethernet g/g6
```

## ip internal-usage-vlan

The `ip internal-usage-vlan` Interface Configuration mode command reserves a VLAN as the internal usage VLAN of an interface. Use the **no** form of this command to reset to default.

### Syntax

- `ip internal-usage-vlan vlan-id`
- `no ip internal-usage-vlan`
  - *vlan-id* — VLAN ID of the internal usage VLAN.

### Default Configuration

This command has no default configuration.

### Command Mode

Interface Configuration (Ethernet, Port Channel) mode.

### User Guidelines

- An internal usage VLAN is required when an IP interface is defined on Ethernet port or Port Channel.
- Using this command the user can define the internal usage VLAN of a port.
- If an internal-usage is not defined for a Port, and the user defines an IP interface, the software selects one of the unused VLANs.
- If a VLAN ID was chosen by the software for internal usage, and the user uses that VLAN ID for static or dynamic VLAN, he should either remove the IP interface, creates the VLAN, and recreate the IP interface, or use this command to define explicit internal usage VLAN.
- This command cannot be used with the command **interface range ethernet**.

### Examples

The following example reserves a VLAN as the internal usage VLAN of an interface.

```
Console (config)# ip internal-usage-vlan 10
```

## show vlan

The **show vlan** Privileged EXEC mode command displays VLAN information.

### Syntax

- **show vlan** [**tag** *vlan-id* | **name** *vlan-name*]
  - *vlan-id* — A valid VLAN ID
  - *vlan-name* — A valid VLAN name string. (Range: 1 - 32 characters)

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

## Example

The following example displays all VLAN information.

```
Console# show vlan
```

Vlan	Name	Ports	Type	Authorization
1	default	g1-2	other	Required
10	VLAN0010	g1-4	dynamic	Required
11	VLAN0011	g3-4	static	Required
20	VLAN0020	g1-2	static	Required
21	VLAN0021	g3-4	static	Required
30	VLAN0030		static	Required
31	VLAN0031		static	Not Required

## show vlan internal usage

The `show vlan internal usage` Privileged EXEC mode command displays a list of VLANs being used internally by the switch.

### Syntax

- `show vlan internal usage`

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays all VLAN information.

```
Console# show vlan internal usage
```

Usage	VLAN	Reserved	IP Address
g21	1007	No	Active
g22	1008	Yes	Inactive
g23	1009	Yes	Active

## show vlan protocols-groups

The show vlan protocols-groups Privileged EXEC mode command displays protocols-groups information.

### Syntax

- show vlan protocols-groups

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays protocols-groups information.

```
Console# show vlan protocols-groups
```

Encapsulation	Protocol	Group Id
-----	-----	-----
ethernet	08 00	213
ethernet	08 06	213
ethernet	81 37	312
ethernet	81 38	312
rfc1042	08 00	213
rfc1042	08 06	213

## show interfaces switchport

The `show interfaces switchport` Privileged EXEC mode command displays switchport configuration.

### Syntax

- `show interfaces switchport {ethernet interface | port-channel port-channel-number}`
  - *Interface* — Specific interface, such as ethernet g8.
  - *port-channel-number* — Valid port-channel trunk index.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays switchport configuration individually for g1.

```
Console# show interface switchport ethernet g1
Port g1:
Port mode: General
GVRP Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress Untagged VLAN (NATIVE) : 1
Port is member in:
Vlan          Name                Egress rule      Type
----          -
1             default            untagged         System
8             VLAN008            tagged           Dynamic
11            VLAN011            tagged           Static

Forbidden VLANS:
VLAN          Name
----          -
73            Out

Classification rules:
Group ID      VLAN
-----      -
219           372
```



# Voice VLAN

## voice vlan id

The `voice vlan id` Global Configuration mode command enables the Voice VLAN, and configures the Voice VLAN id. Use the `no` form of this command to disable the Voice VLAN.

### Syntax

- `voice vlan id vlan-id`
- `no voice vlan id`
  - *vlan-id* — Specify the Voice VLAN ID.

### Default Configuration

Voice VLAN is not defined.

### Command Mode

Global Configuration mode.

### User Guidelines

- The Voice VLAN feature is only active if the specified VLAN is already created. If the Voice VLAN feature is not active, all the Voice VLAN parameters are kept as shadow parameters.

### Example

The following example configures the Voice VLAN.

```
Console (config)# voice vlan id vlan-id
```

## voice vlan oui-table

The `voice vlan oui-table` Global Configuration mode command configures the Voice OUI table. Use the `no` form of this command to return to default.

## Syntax

- `voice vlan oui-table {add mac-address-prefix [description text] | remove mac-address-prefix}`
- `no voice vlan oui-table`
  - `mac-address-prefix` — Specify the MAC address prefix to be entered to the list.
  - `description text` — An optional text that describes the OUI.

## Default Configuration

OUI	Description
0001e3	Siemens_AG_phone
00036b	Cisco_phone
000fe2	H3C_Aolynk
0060b9	Philips_and_NEC_AG_phone
00d01e	Pingtel_phone
00e075	Polycom/Veritel_phone
00e0bb	3Com_phone

## Command Mode

Global Configuration mode.

## User Guidelines

- There are no user guidelines for this command.

## Example

The following example configures the Voice OUI table.

```
Console (config)# voice vlan oui-table {add mac-address-prefix [description text] | remove mac-address-prefix}
```

## voice vlan cos

The `voice vlan cos` Global Configuration mode command sets the Voice VLAN Class Of Service. Use the `no` form of this command to return to default.

### Syntax

- `voice vlan cos cos [remark]`
- `no voice vlan cos`
  - *cos* — Specify the Voice VLAN Class Of Service.
  - *remark* — Specify that the L2 User Priority would be remarked.

### Default Configuration

CoS: 6

Remarked

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command

### Example

The following example configures Voice vlan cos.

```
Console (config)# voice vlan cos cos [remark]
```

## voice vlan aging-timeout

The `voice vlan aging-timeout` Global Configuration mode command sets the Voice VLAN aging timeout. Use the `no` form of this command to return to default.

### Syntax

- `voice vlan aging-timeout minutes`
- `no voice vlan aging-timeout`
  - *minutes* — Specify the aging timeout in minutes. (Range: 1- 43200 minutes)

### Default Configuration

Voice VLAN aging timeout is 1440.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures Voice vlan aging-timeout.

```
Console (config)# voice vlan aging-timeout minutes
```

## voice vlan enable

The **voice vlan enable** Interface Configuration mode command enables automatic Voice VLAN configuration for a port. Use the **no** form of this command to disable automatic Voice VLAN configuration.

### Syntax

- **voice vlan enable**
- **no voice vlan enable**

### Default Configuration

Automatic Voice VLAN configuration disabled.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- The port is added to the Voice VLAN when a packet with a source MAC address that is a telephony MAC address (defined by the Voice VLAN OUI-table Global Configuration command) is trapped on the port.



**NOTE:** The packet VLAN ID can be the Voice VLAN ID, or any other VLAN. The port joins the Voice VLAN as a tagged port. If the time since the last MAC address with telephony MAC address has aged out, exceeds the timeout limit (configured by the Voice VLAN aging-timeout Global Configuration command), the port is removed from the Voice VLAN.

### Example

The following example enables automatic Voice VLAN configuration for a port.

```
Console (config)#voice vlan enable
```

## voice vlan secure

Use the `voice vlan secure` Interface Configuration command to configure the secure mode for the Voice VLAN. Use the `no` form of this command to disable the secure mode.

### Syntax

- `voice vlan secure`
- `no voice vlan secure`

### Default Configuration

Not secured.

### Command Mode

Interface Configuration (Ethernet, port-channel) mode.

### User Guidelines

- Use this command to specify that packets classified to the Voice VLAN with a source MAC address that is not a telephony MAC address (defined by the `Voice vlan OUI-table` Global Configuration command) is discarded.
- This command is relevant only to ports added to the Voice VLAN automatically.

### Example

The following example configures the current port in security mode. See User Guidelines.

```
Console (config-interface)#voice vlan secure
```

## show voice vlan

Use the `show voice vlan EXEC` command to display the Voice VLAN status.

### Syntax

- `show voice vlan [ ethernet interface | port-channel port-channel-number ]`
  - *interface* — Ethernet interface
  - *port-channel-number* — Port Channel interface

## Default Configuration

OUI	Description
0001e3	Siemens_AG_phone
00036b	Cisco_phone
000fe2	H3C_Aolynk
0060b9	Philips_and_NEC_AG_ph one
00d01e	Pingtel_phone
00e075	Polycom/Veritel_phone
00e0bb	3Com_phone

### Command Mode

EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the Voice VLAN configuration.

```
Console # show voice vlan
Aging timeout: 1440 minutes
OUI table
MAC Address-Prefix      Description
00:01:e3                 Siemens_AG_phone_____
00:03:6B                 Cisco_phone_____
00:0f:e2                 H3C_Aolynk_____
00:60:b9                 Philips_and_NEC_AG_phone
00:d0:1e                 Pingtel_phone_____
00:e0:75                 Polycom/Veritel_phone__
00:e0:bb                 Com_phone_____
```

Voice VLAN VLAN ID: 8

CoS: 6

Remark: Yes

Interface	Enabled	Secure	Activated
g1	Yes	Yes	Yes
g2	Yes	Yes	No
g3	Yes	Yes	Yes
g4	Yes	Yes	Yes
g5	No	No	
g6	No	No	
g7	No	No	
g8	No	No	
g9	No	No	





# Web Server

## ip http server

The `ip http server` Global Configuration mode command enables the device to be configured from a browser. Use the `no` form of this command to disable this function.

### Syntax

- `ip http server`
- `no ip http server`

### Default Configuration

HTTP server is disabled by default.

### Command Mode

Global Configuration mode.

### User Guidelines

- Only a user with access level 15 can use the web server.

### Example

The following example enables the device to be configured from a browser.

```
Console (enable)# ip http server
```

## ip http port

The `ip http port` Global Configuration mode command specifies the TCP port for use by a web browser to configure the device. Use the `no` form of this command to use the default TCP port.

### Syntax

- `ip http port port-number`
- `no ip http port`
  - *port-number* — Port number for use by the HTTP server. (Range: 0 - 65535)

### Default Configuration

This default port number is 80.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command. However, specifying 0 as the port number will effectively disable HTTP access to the device.

### Example

The following example shows how the http port number is configured to 100.

```
Console (config)# ip http port 100
```

## ip http exec-timeout

The `ip http exec-timeout` Global Configuration mode command sets the interval the system waits for user input before automatically logging off. Use the `no` form of this command to return to default.

### Syntax

- `ip http exec-timeout minutes [seconds]`
- `no ip http exec-timeout`

### Parameters

- *minutes* — Integer that specifies the number of minutes. (Range: 0 - 65535)
- *seconds* — Additional time intervals in seconds. (Range: 0 - 59)

### Default Configuration

The default configuration is 10 minutes.

### Command Mode

Global Configuration mode.

### User Guidelines

- This command also configures the exec-timeout for HTTPS in case the the HTTPS timeout was not set. To specify no timeout, enter the command `ip https exec-timeout 0 0`.

### Example

The following example the interval the system waits for user input before automatically logging off to 3 minutes 30 seconds.

```
Console (config)# ip http exec-timeout 3 30
```

## ip https server

The **ip https server** Global Configuration mode command enables the device to be configured from a secured browser. Use the **no** form of this command to disable this function.

### Syntax

- `ip https server`
- `no ip https server`

### Default Configuration

The default for the device is disabled.

### Command Mode

Global Configuration mode.

### User Guidelines

- You must use the `crypto certificate generate` command to generate the HTTPS certificate.

### Example

The following example enables the device to be configured from a browser.

```
Console (config)# ip https server
```

## ip https port

The **ip https port** Global Configuration mode command configures a TCP port for use by a secure web browser to configure the device. Use the **no** form of this command to use the default port.

### Syntax

- `ip https port port-number`
- `no ip https port`
  - *port-number* — Port number for use by the HTTP server. (Range: 0 - 65535)

### Default Configuration

This default port number is 443.

### Command Mode

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example configures the https port number to 100.

```
Console (config)# ip https port 100
```

## ip https exec-timeout

The `ip https exec-timeout` Global Configuration mode command sets the interval the system waits for user input before automatically logging off. Use the `no` form of this command to return to default.

### Syntax

- `ip https exec-timeout minutes [seconds]`
- `no ip https exec-timeout`

### Parameters

- *minutes* — Integer that specifies the number of minutes. (Range: 0 - 65535)
- *seconds* — Additional time intervals in seconds. (Range: 0 - 59)

### Default Configuration

The default configuration is the exec-timeout that was set by the `ip http exec-timeout` command.

### Command Mode

Global Configuration mode.

### User Guidelines

- This command also configures the exec-timeout for HTTPS in case the the HTTPS timeout was not set. To specify no timeout, enter the command `ip https exec-timeout 0 0`.

### Example

The following example the interval the system waits for user input before automatically logging off to 3 minutes 30 seconds.

```
Console (config)# ip https exec-timeout 3 30
```

## crypto certificate generate

The `crypto certificate generate` Global Configuration mode command generates a HTTPS certificate.

### Syntax

- `crypto certificate` [*number*] `generate` [`key-generate` [*length*]] [`passphrase` *string*] [`cn` *common-name*] [`or organization`] [`loc` *location*] [`st` *state*] [`cu` *country*] [`duration` *days*]
  - *number* — Specifies the certificate number. If unspecified, defaults to 1. (Range: 1 - 2)
  - `key-generate` — Regenerate SSL RSA key.
  - *length* — Specifies the SSL RSA key length. If unspecified, length defaults to 1024. (Range: 512 - 2048)
  - `passphrase string` — Passphrase that is used for exporting the certificate in PKCS12 file format. If unspecified the certificate is not exportable. (Range: 512 - 2048)
  - `cn common-name` — Specifies the fully qualified URL or IP address of the device. If unspecified, defaults to the lowest IP address of the device (where the certificate is generated). (Range: 1 - 64)
  - `or organization` — Specifies the organization name. (Range: 1 - 64)
  - `loc location` — Specifies the location or city name. (Range: 1 - 64)
  - `st state` — Specifies the state or province name. (Range: 1 - 64)
  - `cu country` — Specifies the country name. (Range: 2 - 2)
  - `duration days` — Specifies number of days a certification would be valid. If unspecified defaults to 365 days. (Range: 30 - 3650)

### Default Configuration

The Certificate and the SSL RSA key pairs do not exist.

### Command Mode

Global Configuration mode.

### User Guidelines

- The command is not saved in the device configuration; however, the certificate and keys generated by this command are saved in the private configuration, which is never displayed to the user or backed up to another device.
- Use this command to generate self-signed certificate for your device.
- When you export an RSA key pair to a PKCS#12 file, the RSA key pair is as secure as the passphrase. Therefore, keep the passphrase secure.

## Example

The following example regenerates a HTTPS certificate.

```
Console(config)# crypto certificate generate key-generate
```

## crypto certificate request

The **crypto certificate request** Privileged EXEC mode command generates and displays certificate requests for HTTPS.

### Syntax

- **crypto certificate** *number* **request** *common- name* [*or organization*] [*loc location*] [*st state*] [*cu country*]
  - *number* — Specifies the certificate number. (Range: 1 - 2)
  - *common- name* — Specifies the fully qualified URL or IP address of the device. (Range: 1 - 64)
  - *or organization* — Specifies the organization name. (Range: 1 - 64)
  - *loc location* — Specifies the location or city name. (Range: 1 - 64)
  - *st state* — Specifies the state or province name. (Range: 1 - 64)
  - *cu country* — Specifies the country name. (Range: 1 - 2)

### Default Configuration

There is no default configuration for this command.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.
- Before generating a certificate request you must first generate a self-signed certificate using the **crypto certificate generate** Global Configuration mode command.
- After receiving the certificate from the Certification Authority, use the **crypto certificate import** Global Configuration mode command to import the certificate into the device. This certificate would replace the self-signed certificate.

## Examples

The following example generates and displays a certificate request for HTTPS.

```
Console# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAXCzAJBgNVBAGTAkNDMQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
DgKoZlIhvcNAQkBFgFsmIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ
HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDekb2ymCu6K
aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QV1+8Ubx3GyCm
/oW93BSOFwxwEsp58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH
MRDjEyMwgICCAgICAICAQIMA0GCSqGSIb3DQEBAQUAA4GBAGb8UgIx7rB05m+2
m5ZZPhIwl8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa
g+uNpyTkDt3ZVU72pjz/fa8TF0n3
-----END CERTIFICATE REQUEST-----

CN= router.gm.com
O= General Motors
C= US
```

## crypto certificate import

The **crypto certificate import** Global Configuration mode command imports a certificate signed by Certification Authority for HTTPS.

### Syntax

- **crypto certificate number import**
  - **number** — Specifies the certificate number. (Range: 1 - 2)

### Default Configuration

There is no default configuration for this command.

### Command Mode

Global Configuration mode.

## User Guidelines

- Use this command to enter an external certificate (signed by Certification Authority) to the device. To end the session, enter a new line, enter "." (period) and add another new line.
- The imported certificate must be based on a certificate request created by the **crypto certificate request** Privileged EXEC mode command.
- If the public key found in the certificate does not match the device's SSL RSA key, the command will fail.
- This command is not saved in the device configuration; however, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another device).

## Examples

The following example imports a certificate signed by Certification Authority for HTTPS.

```
Console(config)# crypto certificate 1 import
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIaKEAp4HS
nnH/xQSGA2ffkRBWu2XIxb7n8VPsTmlxyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFaf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlmjBSb290JTIwQ2VydG1maWVyLENOPXNlcnZl
-----END CERTIFICATE-----

Certificate imported successfully.
Issued to: router.gm.com
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```



## ip https certificate

The `ip https certificate` Global Configuration mode command configures the active certificate for HTTPS. Use the `no` form of this command to return to default.

### Syntax

- `ip https certificate number`
- `no ip https certificate`
  - *number* — Specifies the certificate number. (Range: 1 - 2)

### Default Configuration

Certificate number 1.

### Command Mode

Global Configuration mode.

### User Guidelines

- The `crypto certificate generate` command should be used in order to generate HTTPS certificates.

### Example

The following example configures the active certificate for HTTPS.

```
Console (config)# ip https certificate 1
```

## crypto certificate import pkcs12

The `crypto certificate import pkcs12` Privileged EXEC mode command, imports the certificate and the RSA keys within a PKCS12 file.

### Syntax

- `crypto certificate number import pkcs12 passphrase`
  - *number* — Specifies the certificate number. (Range: 1 - 2)
  - *passphrase* — Passphrase that is used to encrypt the PKCS12 file for export. (Range: 8 - 96)

### Default Configuration

There is no default configuration for this command.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- The passphrase that was exported by the `crypto certificate export pkcs12` command should be used. Please note that this passphrase would be saved for later exports.

## Example

The following example imports the certificate and RSA keys.

```
Console (config)# crypto certificate 1 import pkcs12 passphrase
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F
45 D4
subject=/C=us/ST= /L= /CN= /O= /OU=
issuer= /C=us/ST= /L= /CN= /O= /OU=
-----BEGIN CERTIFICATE-----
MIIBfDCCASYCAQAwDQYJKoZIhvcNAQEEBQAwSTELMAkGA1UEBhMCdXMxCjAIBgNV
BAGTASAxCjAIBgNVBACjAIBgNVBAMTASAxCjAIBgNVBAoTASAxCjAIBgNV
BAsTASAwHhcNMDQwMjA2MTU1NDQ4WhcNMDUwMjA2MTU1NDQ4WjBjBMQswCQYDVQGG
EwJlczEKMAgGA1UECBMIDEKMAgGA1UEBxMBIDEKMAgGA1UEAxMBIDEKMAgGA1UE
ChMBIDEKMAgGA1UECxBMIDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCZXP/tk3e/
jrulfZw8q8T2oS5ymrEIES/sRJE8uahTBjqKulVHqRYJR3VYa/03HSJ741w5MzPI
iuWZzrbbuXAxAgMBAAEwDQYJKoZIhvcNAQEEBQADQQBQ+GTLen1p1kARxI4C1fTU
efig3ffZ/tjW5q1t1r5F6zNv/GuXWw7rGzmRyoMXDcYp1TaA4gAIFQCpFGqiSbAx
-----END CERTIFICATE-----
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F
45 D4
Key Attributes: <No Attributes>
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,085DCBF3A41D2669
dac0m9jqEp1DM50sIDb8Jq1jxW/1P0kqSxuMhc25OdBE/1fPBg9VSvV1ARaYt16W
bX67UyJ8t7HHF3AowjcWzElQ5GJgSQ0VemsqsRQzjpCTb090rx+cNwVfIvjoedgQ
Mt15+fKIAcqsfEgEGJNXQ4jEzsXAkwfQLFfgt4703IpkUn0AxrQzutJDOcC28Uxp
raMVTVS1SkJIvaPuXJxdZ279tDMwZffILBfKCGACT5V5/4WEqDkrF+uuF9/oxm2
5SVL8TvUmXB/3hX4UoaXtxAhuyOdhh1kyyZSpw9BPPR/8bc/wUYERh7+7JXLKHpD
ueeu3znfIX4dDeti8B3xYvvE8kGZjxFN1cC3zc3JsD0IVulLkyiAa93P4LPEvAwG
Fw1LqmGiiqw9JM/tzc6kYkZXylFzCrSVf2exp+/tEvM=
-----END RSA PRIVATE KEY-----
```

## show crypto certificate mycertificate

The `show crypto certificate mycertificate` Privileged EXEC mode command allows you to view the SSL certificates of your device.

### Syntax

- `show crypto certificate mycertificate [number]`
  - number — Specifies the certificate number. (Range: 1- 2)

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode .

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the certificate.

```
Console# show crypto certificate mycertificate 1
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTmlxyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCA4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFaf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASKwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTJwU29mdHdhcmU1MjBSb290JTJwQ2VydGlmaWVyeLENOPXN1cnZl
-----END CERTIFICATE-----

Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

## show ip http

The `show ip http` Privileged EXEC mode command displays the HTTP server configuration.

### Syntax

- `show ip http`

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the HTTP server configuration.

```
Console# show ip http
HTTP server enabled. Port: 80
```

## show ip https

The `show ip https` Privileged EXEC mode command displays the HTTPS server configuration.

### Syntax

- `show ip https`

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays the HTTP server configuration.

```
Console# show ip https
HTTPS server enabled.  Port: 443

Certificate 1 is active
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788

Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
```



## 802.1x Commands

### aaa authentication dot1x

The `aaa authentication dot1x` Global Configuration mode command specifies one or more authentication, authorization, and accounting (AAA) methods for use to authenticate interfaces running IEEE 802.1X. Use the `no` form of this command to return to default.

#### Syntax

- `aaa authentication dot1x default method1 [method2...]`
- `no aaa authentication dot1x default`
  - *method1 [method2...]* — At least one from the following table:

Keyword	Description
Radius	Uses the list of all RADIUS servers for authentication
None	Uses no authentication

#### Default Configuration

The default behavior of the "aaa authentication" for dot1.x is "failed to authenticate". If the 8021.x calls the AAA for authentication services it will receive a fail status.

#### Command Mode

Global Configuration mode.

#### User Guidelines

- The additional methods of authentication are used only if the previous method returns an error, for example the authentication server is down, and not if the request for authenticate is denied access. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line.
- The radius server must support MD-5 challenge and EAP type frames.

## Examples

The following example uses the `aaa authentication dot1x default` command with no authentication.

```
Console (config)# aaa authentication dot1x default none
```

## dot1x system-auth-control

The `dot1x system-auth-control` Global Configuration mode command enables 802.1x globally. Use the `no` form of this command to disable 802.1x globally.

Syntax

- `dot1x system-auth-control`
- `no dot1x system-auth-control`
  - This command has no arguments or keywords.

### Default Configuration

802.1x globally disabled.

### Command Modes

Global Configuration mode.

### User Guidelines

- There are no user guidelines for this command.

## Examples

The following example enables 802.1x globally.

```
Console(config)# dot1x system-auth-control
```

## dot1x port-control

The `dot1x port-control` Interface Configuration mode command enables manual control of the authorization state of the port. Use the `no` form of this command to return to the default setting.



## Syntax

- `dot1x port-control {auto | force-authorized | force-unauthorized}`
- `no dot1x port-control`
  - **auto** — Enable 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 switch and the client.
  - **force-authorized** — Disable 802.1X authentication on the interface and cause the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1X-based authentication of the client.
  - **force-unauthorized** — Deny all access through this interface by forcing the port to transition to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

## Default Configuration

force-authorized.

## Command Mode

Interface Configuration (Ethernet) mode.

## User Guidelines

- It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in auto state that are connected to end stations), in order to get immediately to the forwarding state after successful authentication.

## Examples

The following example enables 802.1X authentication on the interface.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x port-control auto
```

## dot1x re-authentication

The `dot1x re-authentication` Interface Configuration mode command enables periodic re-authentication of the client. Use the `no` form of this command to return to the default setting.

## Syntax

- `dot1x re-authentication`
- `no dot1x re-authentication`

This command has no arguments or keywords.

### Default Configuration

Periodic re-authentication is disabled.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- It is recommended to use re-authentication because if re-authentication is not defined, once a port is authenticated, it will remain in this state until the port is down or a log-off message is sent by client.

### Examples

The following example enables periodic re-authentication of the client.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x re-authentication
```

## dot1x timeout re-authperiod

The `dot1x timeout re-authperiod` Interface Configuration mode command sets the number of seconds between re-authentication attempts. Use the `no` form of this command to return to the default setting.

### Syntax

- `dot1x timeout re-authperiod seconds`
- `no dot1x timeout re-authperiod`
  - *seconds* — Number of seconds between re-authentication attempts. (Range: 300 - 4294967295)

### Default Configuration

3600 seconds between re-authentication attempts.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example sets the number of seconds between re-authentication attempts, to 3600.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x timeout re-authperiod 3600
```

## dot1x re-authenticate

The `dot1x re-authenticate` Privileged EXEC mode command manually initiates a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.

### Syntax

- `dot1x re-authenticate [ethernet interface]`
  - interface — Valid Ethernet port. (Full syntax: unit/port)

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

There are no user guidelines for this command.

### Examples

- The following command manually initiates a re-authentication of the 802.1X-enabled port.

```
Console# dot1x re-authenticate ethernet g8
```

## dot1x timeout quiet-period

The `dot1x timeout quiet-period` Interface Configuration mode command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password). Use the `no` form of this command to return to the default setting.

### Syntax

- `dot1x timeout quiet-period seconds`
- `no dot1x timeout quiet-period`
  - *seconds* — Time in seconds that the switch remains in the quiet state following a failed authentication exchange with the client. (Range: 0 - 65535 seconds)

### Default Configuration

Switch remains in quiet state following a failed authentication exchange for 60 seconds.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- During the quiet period, the switch does not accept or initiate any authentication requests.
- The default value of this command should only be changed to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.
- If it is necessary to provide a faster response time to the user, a smaller number than the default should be entered.

### Examples

The following example sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange, to 3600.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x timeout quiet-period 3600
```

## dot1x timeout tx-period

The `dot1x timeout tx-period` Interface Configuration mode command sets the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP) - request/identity frame, from the client, before resending the request. Use the `no` form of this command to return to the default setting.

### Syntax

- `dot1x timeout tx-period` *seconds*
- `no dot1x timeout tx-period`
  - *seconds* — Time in seconds that the switch should wait for a response to an EAP -request/identity frame from the client before resending the request. (Range: 30-65535 seconds)

### Default Configuration

Switch waits 30 seconds for response to EAP request/identity frame from client before resending the request.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

## Examples

The following command sets the number of seconds that the switch waits for a response to an EAP - request/identity frame, to 3600 seconds.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x timeout tx-period 3600
```

## dot1x max-req

The **dot1x max-req** Interface Configuration mode command sets the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP) - request/identity frame (assuming that no response is received) to the client, before restarting the authentication process. Use the **no** form of this command to return to the default setting.

### Syntax

- **dot1x max-req** *count*
- **no dot1x max-req**
  - *count* — Number of times that the switch sends an EAP - request/identity frame before restarting the authentication process. (Range: 1 - 10)

### Default Configuration

Maximum number of times switch sends EAP request/identity frame to the client before restarting the authentication process is **twice**.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

## Examples

The following example sets the number of times that the switch sends an EAP - request/identity frame, to 6.

```
Console (config)# interface ethernet g8
Console (config-if)# dot1x max-req 6
```

## dot1x timeout supp-timeout

The `dot1x timeout supp-timeout` Interface Configuration mode command sets the time for the retransmission of an Extensible Authentication Protocol (EAP)-request frame to the client. Use the `no` form of this command to return to the default setting.

### Syntax

- `dot1x timeout supp-timeout seconds`
- `no dot1x timeout supp-timeout`
  - *seconds* — Time in seconds that the switch should wait for a response to an EAP-request frame from the client before resending the request. (Range: 1 - 65535 seconds)

### Default Configuration

30 seconds for retransmission of EAP request frame to client.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

### Examples

The following example sets the time for the retransmission of an EAP-request frame to the client, to 3600 seconds.

```
console config-if(Config-VLAN)# dot1x timeout supp-timeout 3600
```

## dot1x timeout server-timeout

The `dot1x timeout server-timeout` Interface Configuration mode command sets the time for the retransmission of packets to the authentication server. Use the `no` form of this command to return to the default setting.

### Syntax

- `dot1x timeout server-timeout seconds`
- `no dot1x timeout server-timeout`
  - *seconds* — Time in seconds that the switch should wait for a response from the authentication server before resending the request. (Range: 1 - 65535 seconds)

### Default Configuration

30 seconds for the retransmission of packets to authentication server.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- There are no user guidelines for this command.

### Examples

The following example sets the time for the retransmission of packets to the authentication server., to 3600 seconds.

```
Console (config)# dot1x timeout server-timeout 3600
```

## dot1x send-async-request-id

Use the `dot1x send-async-request-id` interface configuration command to enable 802.1x switch to request asynchronously the responses from supplicants on port. This request causes the stations, which don't start 802.1x authentication automatically, to start it in response to Switch message. In case enabled the message would be sent according to `dot1x timeout tx-period`. Use the `no` form of this command to return to the default setting.

```
dot1x send-async-request-id
```

```
no dot1x send-async-request-id
```

### Syntax Description

This command has no arguments or keywords

### Parameters range

None

### Default

`no` by default

### Command Modes

Interface configuration (Ethernet)

### Usage Guidelines

The command causes 802.1x switch to send Extensible Authentication Protocol (EAP)-request/identity frame from the authenticator (switch) each `tx-period` automatically. It is recommended to activate this command only in case there is at least one device with not full 802.1x functionality connected to port (for example Windows EX with Service Pack 2). In addition it is recommended to increase `dot1x timeout tx-period` to reduce the overhead during the processing of supplicant responses on switch.

## Examples

```
Console(config-if)# dot1x send-async-request-id
Console(config-if)#
```

## show dot1x

The `show dot1x` Privileged EXEC mode command displays 802.1X status for the switch or for the specified interface.

### Syntax

- `show dot1x [ethernet interface]`
  - *interface* — The full syntax is: *port*.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

## Examples

The following example displays 802.1X status for the switch.

```
Console# show dot1x
```

Interface	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Username
g1	Auto	Authorized	Ena	3600	Bob
g2	Auto	Authorized	Ena	3600	John
g3	Auto	Unauthorized	Ena	3600	Clark
g4	Force-auth	Authorized	Dis	3600	n/a



```
Console# show dot1x ethernet g3
```

```
Interface      Admin Mode   Oper Mode      Reauth          Reauth Period  Username
              Admin Mode   Oper Mode      Control
g3             Auto        Unauthorized    Ena             3600           Clark
State: held
Quiet period: 60
Tx period: 30
Max req: 2
Login Time: n/a
Last Authentication: n/a
MAC Address: 00:08:78:32:98:78
Authentication Method: Remote
Termination Cause: Supplicant logoff
```

The following table describes the significant fields shown in the display:

Field	Description
Interface	The interface number.
Admin mode	The admin mode of the port. Possible values are: Force-auth, Force-unauth, Auto
Oper mode	The oper mode of the port. Possible values are: Authorized, Unauthorized.
Reauth Control	Reauthentication control.
Reauth Period	Reauthentication period.
Username	The User-Name representing the identity of the Supplicant.
State	The current value of the Authenticator PAE state machine.
Quiet period	The number of seconds that the switch remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
Tx period	The number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request.
Max req	The maximum number of times that the switch sends an Extensible Authentication Protocol (EAP)-request/identity frame (assuming that no response is received) to the client before restarting the authentication process.

Login Time	How long the user is logged in.
Last Authentication	Time since last authentication.
Mac address	The supplicant MAC address.
Authentication Method	The authentication method used to establish the session.
Termination Cause	The reason for the session termination.

## show dot1x users

The `show dot1x users` Privileged EXEC mode command displays 802.1X users for the switch.

### Syntax

- `show dot1x users [username username]`
  - *username* — Supplicant username . (Range: 1 - 160 characters)

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following example displays 802.1X users.

```
console# show dot1x users
```

Username	Session Time	Last Auth	Auth Method	MAC Address	Interface
Bob	1d3h	58m	Remote	00:08:3b:79:87:87	g1
John	8h19m	2m	None	00:08:3b:89:31:27	g2

The following table describes the significant fields shown in the display.

Field	Description
Username	The User-Name representing the identity of the Supplicant.
Login Time	How long the user is logged in.
Last Authentication	Time since last authentication.
Authentication Method	The authentication method used to establish the session.
Mac address	The supplicant MAC address.
Interface	The interface that the user is using.

## show dot1x statistics

The `show dot1x statistics` Privileged EXEC mode command displays 802.1X statistics for the specified interface.

### Syntax

- `show dot1x statistics ethernet interface`
  - *interface* — The full syntax is: *port*.

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

## Examples

The following example displays 802.1X statistics for the specified interface.

```
Switch# show dot1x statistics ethernet g1

EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 0008.3b79.8787
```

The following table describes the significant fields shown in the display:

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	The number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	The number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
EapolReqIdFramesTx	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.

EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

## ADVANCED FEATURES

### dot1x auth-not-req

The `dot1x auth-not-req` VLAN Configuration mode command enables unauthorized users access to that VLAN. Use the `no` form of this command to disable the access.

#### Syntax

- `dot1x auth-not-req`
- `no dot1x auth-not-req`

This command has no arguments or keywords.

#### Default Configuration

User should be authorized to access the VLAN.

#### Command Mode

Interface Configuration (VLAN) mode.

#### User Guidelines

- An access port cannot be a member in an unauthenticated VLAN.
- The native VLAN of a trunk port cannot be an unauthenticated VLAN.
- For a general port, the PVID can be the Unauthenticated VLAN (although only tagged packets would be accepted in Unauthorized state).

#### Examples

The following example enables unauthorized users access to the VLAN.

```
console config-if(Config-VLAN)# dot1x auth-not-req
```

## dot1x multiple-hosts

The `dot1x multiple-hosts` Interface Configuration mode command allows multiple hosts (clients) on an 802.1X-authorized port with the `dot1x port-control` Interface Configuration mode command set to `auto`. Use the `no` form of this command to return to the default setting.

### Syntax

- `dot1x multiple-hosts`
- `no dot1x multiple-hosts`

This command has no arguments or keywords.

### Default Configuration

Multiple hosts are disabled. If a port would join a port-channel, the state would be multiple hosts as long as the port is member in the port-channel.

Multiple-hosts must be enabled if the user disables ingress-filtering on this port.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- This command enables the attachment of multiple clients to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized, all attached clients are denied access to the network.
- For unauthenticated VLANs multiple hosts are always enabled.

### Examples

The following command allows multiple hosts (clients) on an 802.1X-authorized port.

```
console config-if(Config-VLAN)#dot1x multiple-hosts
```

## dot1x single-host-violation

The `dot1x single-host-violation` Interface Configuration mode command configures the action to be taken when a station of which the MAC address is not the supplicant MAC address, attempts to access the interface. Use the `no` form of this command to return to default.

## Syntax

- `dot1x single-host-violation {forward | discard | discard-shutdown} [trap seconds]`
- `no port dot1x single-host-violation`
  - **forward** — Forward frames with source addresses not the supplicant address, but do not learn the address.
  - **discard** — Discard frames with source addresses not the supplicant address.
  - **discard-shutdown** — Discard frames with source addresses not the supplicant address. The port is also shutdown.
  - **trap seconds** — Send SNMP traps, and specifies the minimum time between consecutive traps. (Range: 1 - 1000000)

## Default Configuration

Discard frames with source addresses not the supplicant address. No traps.

## Command Mode

Interface Configuration (Ethernet) mode.

## User Guidelines

- The command is relevant when Multiple hosts is disabled and the user has been successfully authenticated.

## Examples

The following example uses the forward action to forward frames with source addresses.

```
console config-if(Config-VLAN)# dot1x single-host-violation
forward trap 100
```

## dot1x guest-vlan

The `dot1x guest-vlan` Interface Configuration mode command defines a Guest VLAN. Use the `no` form of this command to return to default.

## Syntax

- `dot1x guest-vlan`
- `no dot1x guest-vlan`

## Default Configuration

No VLAN is defined as a Guest VLAN.

### Command Mode

Interface Configuration (VLAN) mode.

### User Guidelines

- Use the **dot1x guest-vlan enable** Interface Configuration command to enable unauthorized users on an interface an access to the Guest VLAN. If the Guest VLAN is defined and enabled, the port automatically joins the Guest VLAN when the port is unauthorized, and leaves the Guest VLAN when the port becomes authorized. To get this functionality, the port should not be statically a member in the Guest VLAN.

### Examples

The following example

```
console config-if(Config-VLAN)#
```

## dot1x guest-vlan enable

The **dot1x guest-vlan enable** Interface Configuration mode command enables unauthorized users on the interface access to the Guest VLAN. Use the **no** form of this command to disable the access.

### Syntax

- **dot1x guest-vlan enable**
- **no dot1x guest-vlan enable**

### Default Configuration

Disabled.

### Command Mode

Interface Configuration (Ethernet) mode.

### User Guidelines

- There is one global Guest VLAN in the switch, defined by the **dot1x guest-vlan interface VLAN** configuration command.

### Examples

The following example enables unauthorized users on the interface access to the Guest VLAN.

```
console config-if(Config-VLAN)# dot1x guest-vlan enable
```



## dot1x mac-authentication

The `dot1x mac-authentication` Interface Configuration mode command enables authentication based on the station's MAC address. Use the `no` form of this command to disable MAC authentication.

### Syntax

- `dot1x mac-authentication {mac-only | mac-and-802.1x}`
- `no dot1x mac-authentication`
  - `mac-only` — Enable authentication based on the station's MAC address only. 802.1X frames are ignored.
  - `mac-and-802.1x` — Enable 802.1X authentication and MAC address authentication on the interface.

### Default Configuration

Disabled.

### Command Mode

Interface configuration (Ethernet) mode

### User Guidelines

- Guest VLAN must be enabled, when MAC authentication is enabled.
- Static MAC addresses cannot be authorized. Do not change authenticated MAC address to static address.
- It is not recommended to delete authenticated MAC addresses.
- Reauthentication must be enabled when working in this mode.

### Example

The following command enables authentication based on the station's MAC address.

```
console config-if(Config)# dot1x mac-authentication mac-only
```

## dot1x traps mac-authentication failure

The `dot1x traps mac-authentication failure` Global Configuration mode command enables sending traps when a MAC address was failed in authentication of the 802.1X MAC authentication access control. Use the `no` form of this command to disable the traps.

### Syntax

- `dot1x traps mac-authentication failure`
- `no dot1x traps mac-authentication failure`

### Default Configuration

This command has no default configuration.

### Command Mode

Global configuration mode.

### User Guidelines

- There are no user guidelines for this command.

### Example

The following command enables sending traps when a MAC address was failed in authentication of the 802.1X MAC authentication access control.

```
console config-if(Config)# dot1x traps mac-authentication failure
```

## dot1x radius-attributes vlan

The **dot1x radius-attributes vlan** Interface Configuration mode command enables user-based VLAN assignment. Use the **no** form of this command to disable user-based VLAN assignment.

### Syntax

- **dot1x radius-attributes vlan**
- **no dot1x radius-attributes vlan**

### Default Configuration

Disabled.

### Command Mode

Interface configuration (Ethernet) mode

### User Guidelines

- The **dot1x radius-attributes vlan** command configuration is allowed only when the port is Forced Authorized.
- RADIUS attributes are supported only in the multiple sessions mode (multiple hosts with authentication).
- When RADIUS attributes are enabled and the RADIUS Accept message does not contain as an attribute the supplicant's VLAN, then the supplicant is rejected.
- Packets to the supplicant are sent untagged.

- After successful authentication the port remains member in the unauthenticated VLANs and in the Guest VLAN. Other static VLAN configuration is not applied on the port.
- If the supplicant VLAN does not exist on the switch, the supplicant is rejected.

### Examples

The following command enables user-based VLAN assignment.

```
console config-if(Config)# dot1x radius-attributes vlan
```

## show dot1x advanced

The `show dot1x advanced` Privileged EXEC mode command displays 802.1X advanced features for the switch or for the specified interface.

### Syntax

- `show dot1x advanced [ethernet interface]`
  - *interface* — Ethernet interface

### Default Configuration

This command has no default configuration.

### Command Mode

Privileged EXEC mode.

### User Guidelines

- There are no user guidelines for this command.

## Examples

The following example displays 802.1X advanced features for the switch.

```
Console# show dot1x advanced
```

```
Guest VLAN: 100
```

```
Guest VLAN timeout
```

```
Unauthenticated VLANs:
```

Interface	Multiple Hosts	Guest VLAN	MAC Authentication	Assignment	Async-reqId
g1	Authenticate	Enabled	Disabled	Enabled	True
g2	Authenticate	Disabled	Disabled	Disabled	False
g3	Authenticate	Disabled	Disabled	Disabled	False
g4	Authenticate	Disabled	Disabled	Disabled	False
g5	Authenticate	Disabled	Disabled	Disabled	False
g6	Authenticate	Disabled	Disabled	Disabled	False
g7	Authenticate	Disabled	Disabled	Disabled	False
g8	Authenticate	Disabled	Disabled	Disabled	False
g9	Authenticate	Disabled	Disabled	Disabled	False
g10	Authenticate	Disabled	Disabled	Disabled	False
g11	Authenticate	Disabled	Disabled	Disabled	False
g12	Authenticate	Disabled	Disabled	Disabled	False
g13	Authenticate	Enabled	Disabled	Enabled	False
g14	Authenticate	Disabled	Disabled	Disabled	False
g15	Authenticate	Disabled	Disabled	Disabled	False
g16	Authenticate	Disabled	Disabled	Disabled	False
g17	Authenticate	Disabled	Disabled		
g18	Authenticate	Disabled	Disabled		
g19	Authenticate	Disabled	Disabled		
g20	Authenticate	Disabled	Disabled		
g21	Authenticate	Disabled	Disabled		
g22	Authenticate	Disabled	Disabled		