

ソフトウェアマニュアル

マネジメント 32 ポートギガビットイーサネットスイッチ

【CGR-3291-NA2A】

2026 年 9 月

日本テレガートナー株式会社

CHAPTER 1. INTRODUCTION	17
1.1 PRODUCT DESCRIPTION.....	17
1.2 PANELS	17
CHAPTER 2. INSTALLATION	18
2.1 FIBER OR RJ-45 CONNECTIONS	18
2.2 MGMT PORT CONNECTION.....	18
2.3 CONSOLE PORT CONNECTION	18
2.3.1 RJ-45 Pin Assignment	19
2.3.2 Accessory Cable	19
2.4 ELECTRICAL INSTALLATION	19
2.5 RACK MOUNTING	20
2.6 LED INDICATORS & RESET TO DEFAULT BUTTON	21
CHAPTER 3. INTRODUCTION TO CLI	22
3.1 INTRODUCTION	22
3.2 ACCESS CONNECTION	22
3.2.1 Telnet Operation.....	22
3.2.2 CONSOLE Operation.....	22
3.3 CLI MODES.....	23
3.4 QUICK KEYS	23
3.5 COMMAND SYNTAX	24
3.6 BASIC CONFIGURATIONS	24
3.6.1 Configuring IPv4 Address	24
3.6.2 Enter Config Interface Mode	25
3.6.3 Save Configurations	26
3.6.4 Restart the Device.....	26
3.6.5 Load Factory Defaults	27
3.6.6 Show System and Software Information	27
3.6.7 Show Running Configurations.....	27
3.6.8 Show History Commands	28
3.6.9 Help	28
3.6.10 Logout	29
3.7 COMMANDS IN USER MODE	29
3.7.1 > clear ip arp	29
3.7.2 > clear lldp statistics.....	29
3.7.3 > clear statistics	29
3.7.4 > enable	30
3.7.5 > exit	30
3.7.6 > help	30
3.7.7 > logout.....	30
3.7.8 > ping ip	30
3.7.9 > ping ipv6.....	31
3.7.10 show commands	31
3.8 COMMANDS IN EXEC MODE.....	32
3.8.1 # clear access management statistics	32
3.8.2 # clear access-list ace statistics.....	32
3.8.3 # clear dot1x statistics	32
3.8.4 # clear ip arp	32
3.8.5 # clear ip dhcp detailed statistics.....	32
3.8.6 # clear ip dhcp relay statistics.....	33
3.8.7 # clear ip dhcp server binding <ip>	33
3.8.8 # clear ip dhcp server binding { automatic manual expired }.....	33
3.8.9 # clear ip dhcp server statistics.....	33
3.8.10 # clear ip dhcp snooping statistics	33
3.8.11 # clear ip igmp snooping	33
3.8.12 # clear ip statistics.....	33

3.8.13 # clear ipv6 mld snooping	34
3.8.14 # clear ipv6 neighbors	34
3.8.15 # clear ipv6 statistics	34
3.8.16 # clear lacp statistics	34
3.8.17 # clear lldp statistics	34
3.8.18 # clear logging	34
3.8.19 # clear mac address-table	34
3.8.20 # clear mvr	35
3.8.21 # clear spanning-tree	35
3.8.22 # clear statistics	35
3.8.23 # config terminal	35
3.8.24 # copy	35
3.8.25 # delete	36
3.8.26 # dir	37
3.8.27 # disable & # enable	37
3.8.28 # dot1x	37
3.8.29 # firmware swap	37
3.8.30 # firmware upgrade	38
3.8.31 # ip dhcp retry interface vlan	38
3.8.32 # ipv6 dhcp-client restart	38
3.8.33 # more	38
3.8.34 # ping ip	38
3.8.35 # ping ipv6	39
3.8.36 # reload cold	39
3.8.37 # reload defaults	39
3.8.38 # send	39
3.8.39 # terminal editing	40
3.8.40 # terminal exec-timeout	40
3.8.41 # terminal history size	40
3.8.42 # terminal length	41
3.8.43 # terminal width	41
3.8.44 # no port-security shutdown	41
3.8.45 # veriphy	41
3.8.46 show commands	42
3.9 COMMANDS IN CONFIG MODE	42
3.9.1 aaa	42
3.9.1.1 (config)# aaa accounting	42
3.9.1.2 (config)# aaa authentication login	42
3.9.1.3 (config)# aaa authorization	43
3.9.2 (config)# access management	43
3.9.3 (config)# access-list	44
3.9.3.1 (config)# access-list ace	44
3.9.3.2 (config)# access-list ace update	45
3.9.3.3 (config)# access-list rate-limiter	46
3.9.3.4 (config-if)# access-list action	46
3.9.3.5 (config-if)# access-list logging	46
3.9.3.6 (config-if)# access-list policy	46
3.9.3.7 (config-if)# access-list port-state	47
3.9.3.8 (config-if)# access-list rate-limiter	47
3.9.3.9 (config-if)# access-list shutdown	47
3.9.3.10 (config-if)# access-list {redirect}	47
3.9.4 (config)# aggregation	48
3.9.4.1 (config)# aggregation mode	48
3.9.4.2 (config-if)# aggregation group	48
3.9.5 (config)# banner	48
3.9.5.1 (config)# banner [motd] <banner>	48
3.9.5.2 (config)# banner exec <banner>	49
3.9.5.3 (config)# banner login <banner>	49

3.9.6 (config)# clock.....	49
3.9.6.1 (config)# clock summer-time <word16> date	49
3.9.6.2 (config)# clock summer-time <word16> recurring	50
3.9.6.3 (config)# clock timezone.....	50
3.9.7 (config)# default.....	51
3.9.7.1 (config)# default access-list rate-limiter	51
3.9.8 (config)# dot1x.....	51
3.9.8.1 (config)# dot1x system-auth-control	51
3.9.8.2 (config)# dot1x re-authentication	52
3.9.8.3 (config)# dot1x authentication timer re-authenticate	52
3.9.8.4 (config)# dot1x timeout tx-period	52
3.9.8.5 (config)# dot1x authentication timer inactivity	53
3.9.8.6 (config)# dot1x timeout quiet-period.....	53
3.9.8.7 (config)# dot1x feature.....	54
3.9.8.8 (config)# dot1x guest-vlan	54
3.9.8.9 (config)# dot1x guest-vlan supplicant	54
3.9.8.10 (config)# dot1x max-reauth-req	55
3.9.8.11 (config-if)# dot1x port-control.....	55
3.9.8.12 (config-if)# dot1x guest-vlan.....	56
3.9.8.13 (config-if)# dot1x radius-qos	56
3.9.8.14 (config-if)# dot1x radius-vlan	56
3.9.8.15 (config-if)# dot1x re-authenticate	57
3.9.9 (config-if)# duplex.....	57
3.9.10 (config)# enable	57
3.9.10.1 (config)# enable password	57
3.9.10.2 (config)# enable password level	58
3.9.10.3 (config)# enable secret	58
3.9.11 (config-if)# excessive-restart	58
3.9.12 (config)# fanmode { auto full low }.....	59
3.9.13 (config-if)# flowcontrol { on off }.....	59
3.9.14 (config-if)# frame-length-check	59
3.9.15 (config-if)# green-ethernet	60
3.9.15.1 (config-if)# green-ethernet energy-detect	60
3.9.15.2 (config-if)# green-ethernet short-reach	60
3.9.16 (config)# gvrp	60
3.9.16.1 (config)# gvrp.....	60
3.9.16.2 (config)# gvrp max-vlans	60
3.9.16.3 (config)# gvrp time	61
3.9.16.4 (config-if)# gvrp	61
3.9.17 (config)# hostname	62
3.9.18 (config)# interface.....	62
3.9.18.1 (config)# interface (<port_type> [<plist>])	62
3.9.18.2 (config)# interface vlan.....	63
3.9.19 (config)# ip	63
3.9.19.1 (config)# ip arp inspection	63
3.9.19.2 (config)# ip arp inspection entry interface	63
3.9.19.3 (config)# ip arp inspection translate.....	64
3.9.19.4 (config)# ip arp inspection vlan	64
3.9.19.5 (config)# ip arp inspection vlan <in_vlan_list> logging.....	64
3.9.19.6 (config)# ip dhcp excluded-address.....	65
3.9.19.7 (config)# ip dhcp pool.....	65
3.9.19.8 (config)# ip dhcp relay	66
3.9.19.9 (config)# ip dhcp relay information option.....	66
3.9.19.10 (config)# ip dhcp relay information policy {drop keep replace}.....	66
3.9.19.11 (config)# ip dhcp server	67
3.9.19.12 (config)# ip dhcp snooping	67
3.9.19.13 (config)# ip dns proxy	68
3.9.19.14 (config)# ip helper-address.....	68

3.9.19.15 (config)# ip http secure-certificate	68
3.9.19.16 (config)# ip http secure-server	68
3.9.19.17 (config)# ip http secure-redirect.....	69
3.9.19.18 (config)# ip igmp host-proxy.....	69
3.9.19.19 (config)# ip igmp snooping	69
3.9.19.20 (config)# ip igmp snooping vlan.....	70
3.9.19.21 (config)# ip igmp ssm-range	70
3.9.19.22 (config)# ip igmp unknown-flooding	70
3.9.19.23 (config)# ip name-server	71
3.9.19.24 (config)# ip route	71
3.9.19.25 (config)# ip routing	72
3.9.19.26 (config)# ip source binding interface	72
3.9.19.27 (config)# ip ssh.....	73
3.9.19.28 (config)# ip verify source	73
3.9.19.29 (config)# ip verify source translate	73
3.9.19.30 (config-if)# ip arp inspection check-vlan.....	73
3.9.19.31 (config-if)# ip arp inspection logging	74
3.9.19.32 (config-if)# ip arp inspection trust	74
3.9.19.33 (config-if)# ip dhcp snooping trust	74
3.9.19.34 (config-if)# ip igmp snooping filter	74
3.9.19.35 (config-if)# ip igmp snooping immediate-leave	75
3.9.19.36 (config-if)# ip igmp snooping max-groups	75
3.9.19.37 (config-if)# ip igmp snooping mrouter.....	75
3.9.19.38 (config-if)# ip verify source	76
3.9.19.39 (config-if)# ip verify source limit.....	76
3.9.19.40 (config-if-vlan)# ip address	76
3.9.19.41 (config-if-vlan)# ip dhcp server.....	77
3.9.19.42 (config-if-vlan)# ip igmp snooping	77
3.9.19.43 (config-if-vlan)# ip igmp snooping compatibility	77
3.9.19.44 (config-if-vlan)# ip igmp snooping last-member-query-interval.....	78
3.9.19.45 (config-if-vlan)# ip igmp snooping priority	78
3.9.19.46 (config-if-vlan)# ip igmp snooping querier	78
3.9.19.47 (config-if-vlan)# ip igmp snooping query-interval	78
3.9.19.48 (config-if-vlan)# ip igmp snooping query-max-response-time	79
3.9.19.49 (config-if-vlan)# ip igmp snooping robustness-variable	79
3.9.19.50 (config-if-vlan)# ip igmp snooping unsolicited-report-interval.....	79
3.9.19.51 (config-if-vlan)# ipv6 address	80
3.9.19.52 (config-if-vlan)# ipv6 address {autoconfig dhcp rapid-commit}.....	80
3.9.19.53 (config-if-vlan)# ipv6 mld snooping	80
3.9.19.54 (config-if-vlan)# ipv6 mld snooping compatibility	81
3.9.19.55 (config-if-vlan)# ipv6 mld snooping last-member-query-interval.....	81
3.9.19.56 (config-if-vlan)# ipv6 mld snooping priority <cos_priority>	81
3.9.19.57 (config-if-vlan)# ipv6 mld snooping querier election.....	82
3.9.19.58 (config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>.....	82
3.9.19.59 (config-if-vlan)# ipv6 mld snooping query-max-response-time <ipmc_qri>.....	82
3.9.19.60 (config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>.....	82
3.9.19.61 (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <ipmc_uri>.....	83
3.9.20 (config)# ipmc	83
3.9.20.1 (config)# ipmc profile	83
3.9.20.2 (config)# ipmc profile <profile_name>	83
3.9.20.3 (config)# ipmc range.....	84
3.9.20.4 (config-ipmc-profile)# default range	84
3.9.20.5 (config-ipmc-profile)# description	84
3.9.20.6 (config-ipmc-profile)# range.....	85
3.9.21 (config)# ipv6 mld host-proxy.....	85
3.9.21.1 (config)# ipv6 mld host-proxy.....	85
3.9.21.2 (config)# ipv6 mld host-proxy leave-proxy	86
3.9.21.3 (config)# ipv6 mld snooping	86

3.9.21.4 (config)# ipv6 mld snooping vlan	87
3.9.21.5 (config)# ipv6 mld ssm-range	87
3.9.21.6 (config)# ipv6 mld unknown-flooding	88
3.9.21.7 (config)# ipv6 route	88
3.9.21.8 (config-if)# ipv6 mld snooping filter	88
3.9.21.9 (config-if)# ipv6 mld snooping immediate-leave	89
3.9.21.10 (config-if)# ipv6 mld snooping max-groups	89
3.9.21.11 (config-if)# ipv6 mld snooping mrouter	89
3.9.22 (config)# lacp	90
3.9.22.1 (config)# lacp system-priority	90
3.9.22.2 (config-if)# lacp	90
3.9.22.3 (config-if)# lacp key	90
3.9.22.4 (config-if)# lacp port-priority <v_1_to_65535>	91
3.9.22.5 (config-if)# lacp role { active passive }	91
3.9.22.6 (config-if)# lacp timeout { fast slow }	91
3.9.23 (config)# line	92
3.9.23.1 (config)# line	92
3.9.23.2 (config-line)# do	92
3.9.23.3 (config-line)# editing	93
3.9.23.4 (config-line)# end	93
3.9.23.5 (config-line)# exec-banner	93
3.9.23.6 (config-line)# exec-timeout	94
3.9.23.7 (config-line)# exit	94
3.9.23.8 (config-line)# help	94
3.9.23.9 (config-line)# history size	95
3.9.23.10 (config-line)# length	95
3.9.23.11 (config-line)# location	96
3.9.23.12 (config-line)# motd-banner	96
3.9.23.13 (config-line)# privilege level	97
3.9.23.14 (config-line)# width	97
3.9.24 (config)# lldp	97
3.9.24.1 (config)# lldp holdtime	97
3.9.24.2 (config)# lldp reinit	98
3.9.24.3 (config)# lldp timer	98
3.9.24.4 (config)# lldp transmission-delay	99
3.9.24.5 (config)# lldp med datum	99
3.9.24.6 (config)# lldp med fast	100
3.9.24.7 (config)# lldp med location-tlv altitude	100
3.9.24.8 (config)# lldp med location-tlv civic-addr	101
3.9.24.9 (config)# lldp med location-tlv elin-addr	102
3.9.24.10 (config)# lldp med location-tlv latitude	102
3.9.24.11 (config)# lldp med location-tlv longitude	103
3.9.24.12 (config)# lldp med media-vlan-policy	103
3.9.24.13 (config-if)# lldp cdp-aware	104
3.9.24.14 (config-if)# lldp med media-vlan policy-list	104
3.9.24.15 (config-if)# lldp med transmit-tlv	104
3.9.24.16 (config-if)# lldp receive	105
3.9.24.17 (config-if)# lldp tlv-select	105
3.9.24.18 (config-if)# lldp transmit	105
3.9.25 (config)# logging	105
3.9.25.1 (config)# logging on	105
3.9.25.2 (config)# logging host	106
3.9.25.3 (config)# logging level	106
3.9.26 (config)# loop-protect	107
3.9.26.1 (config)# loop-protect	107
3.9.26.2 (config)# loop-protect shutdown-time	107
3.9.26.3 (config)# loop-protect transmit-time	108
3.9.26.4 (config-if)# loop-protect	108

3.9.26.5 (config-if)# loop-protect action	108
3.9.26.6 (config-if)# loop-protect tx-mode.....	108
3.9.27 (config)# mac	109
3.9.27.1 (config)# mac address-table aging-time	109
3.9.27.2 (config)# mac address-table static.....	109
3.9.27.3 (config-if)# mac address-table learning.....	110
3.9.28 (config-if)# media-type	110
3.9.29 (config-if)# mtu	111
3.9.30 (config)# monitor session	111
3.9.31 (config)# mvr.....	111
3.9.31.1 (config)# mvr	111
3.9.31.2 (config)# mvr name <mvr_name> channel.....	112
3.9.31.3 (config)# mvr name <mvr_name> frame priority	112
3.9.31.4 (config)# mvr name <mvr_name> frame tagged	113
3.9.31.5 (config)# mvr name <mvr_name> igmp-address.....	113
3.9.31.6 (config)# mvr name <mvr_name> last-member-query-interval.....	114
3.9.31.7 (config)# mvr name <mvr_name> mode	114
3.9.31.8 (config)# mvr vlan <v_vlan_list>[name <mvr_name>]	115
3.9.31.9 (config)# mvr vlan <v_vlan_list> channel	115
3.9.31.10 (config)# mvr vlan <v_vlan_list> frame priority.....	116
3.9.31.11 (config)# mvr vlan <v_vlan_list> frame tagged.....	116
3.9.31.12 (config)# mvr vlan <v_vlan_list> igmp-address	116
3.9.31.13 (config)# mvr vlan <v_vlan_list> last-member-query-interval.....	117
3.9.31.14 (config)# mvr vlan <v_vlan_list> mode	118
3.9.31.15 (config-if)# mvr immediate-leave	118
3.9.31.16 (config-if)# mvr name	118
3.9.31.17 (config-if)# mvr vlan	119
3.9.32 (config)# ntp.....	119
3.9.32.1 (config)# ntp	119
3.9.32.2 (config)# ntp server	120
3.9.33 (config)# port-security	120
3.9.33.1 (config)# port-security.....	120
3.9.33.2 (config)# port-security aging	121
3.9.33.3 (config)# port-security aging time	121
3.9.33.4 (config-if)# port-security.....	121
3.9.33.5 (config-if)# port-security maximum.....	122
3.9.33.6 (config-if)# port-security violation.....	122
3.9.34 (config)# privilege	123
3.9.35 (config-if)# pvlan	124
3.9.35.1 (config-if)# pvlan.....	124
3.9.35.2 (config-if)# pvlan isolation	124
3.9.36 (config)# qos	124
3.9.36.1 (config)# qos map cos-dscp	124
3.9.36.2 (config)# qos map dscp-classify	125
3.9.36.3 (config)# qos map dscp-cos	126
3.9.36.4 (config)# qos map dscp-egress-translation.....	127
3.9.36.5 (config)# qos map dscp-ingress-translation.....	127
3.9.36.6 (config)# qos qce refresh	128
3.9.36.7 (config)# qos qce update	128
3.9.36.8 (config)# qos storm.....	131
3.9.36.9 (config)# qos wred queue.....	131
3.9.36.10 (config-if)# qos cos	132
3.9.36.11 (config-if)# qos dei.....	132
3.9.36.12 (config-if)# qos dpl.....	132
3.9.36.13 (config-if)# qos dscp-classify.....	133
3.9.36.14 (config-if)# qos dscp-remark.....	133
3.9.36.15 (config-if)# qos dscp-translate	133
3.9.36.16 (config-if)# qos map cos-tag cos.....	134

3.9.36.17 (config-if)# qos map tag-cos pcp	134
3.9.36.18 (config-if)# qos pcp.....	135
3.9.36.19 (config-if)# qos policer.....	135
3.9.36.20 (config-if)# qos queue-policer queue	135
3.9.36.21 (config-if)# qos queue-shaper queue	136
3.9.36.22 (config-if)# qos shaper.....	136
3.9.36.23 (config-if)# qos tag-remark.....	136
3.9.36.24 (config-if)# qos trust dscp.....	137
3.9.36.25 (config-if)# qos trust tag	137
3.9.36.26 (config-if)# qos wred-group.....	137
3.9.36.27 (config-if)# qos wrr	137
3.9.37 (config)# radius-server	138
3.9.37.1 (config)# radius-server attribute 32	138
3.9.37.2 (config)# radius-server attribute 4	138
3.9.37.3 (config)# radius-server attribute 95	139
3.9.37.4 (config)# radius-server deadtime	139
3.9.37.5 (config)# radius-server host.....	139
3.9.37.6 (config)# radius-server key	140
3.9.37.7 (config)# radius-server retransmit.....	140
3.9.37.8 (config)# radius-server timeout.....	141
3.9.38 (config)# rmon	141
3.9.38.1 (config)# rmon alarm.....	141
3.9.38.2 (config)# rmon event	142
3.9.38.3 (config-if)# rmon collection history	143
3.9.38.4 (config-if)# rmon collection stats.....	143
3.9.39 (config)# sflow	143
3.9.39.1 (config)# sflow agent-ip.....	143
3.9.39.2 (config)# sflow collector-address	144
3.9.39.3 (config)# sflow collector-port	144
3.9.39.4 (config)# sflow max-datagram-size.....	144
3.9.39.5 (config)# sflow timeout	145
3.9.39.6 (config-if)# sflow.....	145
3.9.39.7 (config-if)# sflow sampling-rate.....	145
3.9.39.8 (config-if)# sflow max-sampling-size	146
3.9.39.9 (config-if)# sflow counter-poll-interval.....	146
3.9.40 (config-if)# shutdown.....	146
3.9.41 (config)# snmp-server.....	147
3.9.41.1 (config)# snmp-server.....	147
3.9.41.2 (config)# snmp-server access	147
3.9.41.3 (config)# snmp-server community v2c	148
3.9.41.4 (config)# snmp-server community v3.....	148
3.9.41.5 (config)# snmp-server contact.....	148
3.9.41.6 (config)# snmp-server engine-id local	149
3.9.41.7 (config)# snmp-server host.....	149
3.9.41.8 (config)# snmp-server location.....	150
3.9.41.9 (config)# snmp-server security-to-group model.....	150
3.9.41.10 (config)# snmp-server trap	150
3.9.41.11 (config)# snmp-server user.....	151
3.9.41.12 (config)# snmp-server version	151
3.9.41.13 (config)# snmp-server view	152
3.9.41.14 (config-if)# snmp-server host <conf_name> traps	152
3.9.41.15 (config-snmps-host)# host <v_ipv6_ucast>.....	153
3.9.41.16 (config-snmps-host)# host <v_ipv4_ucast>.....	153
3.9.41.17 (config-snmps-host)# version	154
3.9.41.18 (config-snmps-host)# informs retries	154
3.9.41.19 (config-snmps-host)# shutdown.....	155
3.9.41.20 (config-snmps-host)# traps.....	155
3.9.42 (config)# spanning-tree.....	156

3.9.42.1 (config)# spanning-tree aggregation	156
3.9.42.2 (config-stp-aggr)# spanning-tree	156
3.9.42.3 (config-stp-aggr)# spanning-tree auto-edge	156
3.9.42.4 (config-stp-aggr)# spanning-tree bpdu-guard	156
3.9.42.5 (config-stp-aggr)# spanning-tree edge	157
3.9.42.6 (config-stp-aggr)# spanning-tree link-type	157
3.9.42.7 (config-stp-aggr)# spanning-tree mst <instance> cost	157
3.9.42.8 (config-stp-aggr)# spanning-tree mst <instance> port-priority	158
3.9.42.9 (config-stp-aggr)# spanning-tree restricted-role	158
3.9.42.10 (config-stp-aggr)# spanning-tree restricted-tcn	158
3.9.42.11 (config)# spanning-tree edge bpdu-filter	158
3.9.42.12 (config)# spanning-tree edge bpdu-guard	159
3.9.42.13 (config)# spanning-tree mode	159
3.9.42.14 (config)# spanning-tree mst <instance> priority <prio>	160
3.9.42.15 (config)# spanning-tree mst <instance> vlan <v_vlan_list>	160
3.9.42.16 (config)# spanning-tree mst forward-time	161
3.9.42.17 (config)# spanning-tree mst max-age	161
3.9.42.18 (config)# spanning-tree mst max-hops	162
3.9.42.19 (config)# spanning-tree mst name	162
3.9.42.20 (config)# spanning-tree recovery interval	162
3.9.42.21 (config)# spanning-tree transmit hold-count	163
3.9.42.22 (config-if)# spanning-tree	163
3.9.42.23 (config-if)# spanning-tree auto-edge	163
3.9.42.24 (config-if)# spanning-tree bpdu-guard	164
3.9.42.25 (config-if)# spanning-tree edge	164
3.9.42.26 (config-if)# spanning-tree link-type	164
3.9.42.27 (config-if)# spanning-tree mst <instance> cost	165
3.9.42.28 (config-if)# spanning-tree mst <instance> port-priority	165
3.9.42.29 (config-if)# spanning-tree restricted-role	165
3.9.42.30 (config-if)# spanning-tree restricted-tcn	166
3.9.43 (config-if)# speed	166
3.9.44 (config-if)# switchport	166
3.9.44.1 (config-if)# switchport access vlan	166
3.9.44.2 (config-if)# switchport forbidden vlan	167
3.9.44.3 (config-if)# switchport hybrid acceptable-frame-type	167
3.9.44.4 (config-if)# switchport hybrid allowed vlan	167
3.9.44.5 (config-if)# switchport hybrid egress-tag	168
3.9.44.6 (config-if)# switchport hybrid ingress-filtering	168
3.9.44.7 (config-if)# switchport hybrid native vlan	168
3.9.44.8 (config-if)# switchport hybrid port-type	169
3.9.44.9 (config-if)# switchport mode	170
3.9.44.10 (config-if)# switchport trunk allowed vlan	170
3.9.44.11 (config-if)# switchport trunk native vlan	170
3.9.44.12 (config-if)# switchport trunk vlan tag native	171
3.9.44.13 (config-if)# switchport vlan ip-subnet id	171
3.9.44.14 (config-if)# switchport vlan mac	171
3.9.44.15 (config-if)# switchport vlan protocol group	172
3.9.44.16 (config-if)# switchport voice vlan discovery-protocol	172
3.9.44.17 (config-if)# switchport voice vlan mode	172
3.9.44.18 (config-if)# switchport voice vlan security	173
3.9.45 (config)# tacacs-server	173
3.9.45.1 (config)# tacacs-server timeout	173
3.9.45.2 (config)# tacacs-server deadtime	173
3.9.45.3 (config)# tacacs-server key	174
3.9.45.4 (config)# tacacs-server host	174
3.9.46 (config)# udd	174
3.9.46.1 (config)# udd	174
3.9.46.2 (config-if)# udd port	175

3.9.47 (config)# upnp.....	176
3.9.47.1 (config)# upnp	176
3.9.47.2 (config)# upnp advertising-duration.....	176
3.9.47.3 (config)# upnp ttl.....	176
3.9.48 (config)# username	177
3.9.48.1 (config)# username<username>privilege<priv>password encrypted	177
3.9.48.2 (config)# username<username>privilege<priv>password none	177
3.9.48.3 (config)# username<username>privilege<priv>password unencrypted	178
3.9.49 (config)# vlan	179
3.9.49.1 (config)# vlan	179
3.9.49.2 (config)# vlan ethertype s-custom-port.....	179
3.9.49.3 (config)# vlan protocol	179
3.9.50 (config)# voice vlan	180
3.9.50.1 (config)# voice vlan.....	180
3.9.50.2 (config)# voice vlan aging-time.....	181
3.9.50.3 (config)# voice vlan class	181
3.9.50.4 (config)# voice vlan oui <oui> [description <description>]	181
3.9.50.5 (config)# voice vlan vid	182
3.9.51 (config)# web privilege group.....	182
CHAPTER 4. WEB OPERATION & CONFIGURATION	183
4.1 WEB MANAGEMENT INTERFACE CONNECTION & LOGIN	183
4.2 ICONS & BUTTONS.....	184
4.2.1 Port Status	184
4.2.2 Refresh	184
4.2.3 Help System	184
4.2.4 Logout.....	184
4.3 CONFIGURATION	185
4.3.1 System.....	185
4.3.1.1 System Information Configuration	185
4.3.1.2 Fan	186
4.3.1.3 System IP	186
4.3.1.4 System NTP.....	188
4.3.1.5 System Time	189
4.3.1.6 System Log Configuration.....	190
4.3.2 Power Saving.....	191
4.3.2.1 Configuration.....	191
4.3.3 Ports.....	192
4.3.4 DHCP	194
4.3.4.1 Server	194
4.3.4.1.1 Mode.....	194
4.3.4.1.2 Excluded IP	195
4.3.4.1.3 Pool	195
4.3.4.2 DHCP Snooping.....	197
4.3.4.3 Relay Configuration	199
4.3.5 Security	199
4.3.5.1 Switch	200
4.3.5.1.1 Users	200
4.3.5.1.2 Privilege Levels	201
4.3.5.1.3 Auth Method.....	202
4.3.5.1.4 SSH	203
4.3.5.1.5 HTTPS	204
4.3.5.1.6 Access Management Configuration	204
4.3.5.1.7 SNMP	205
4.3.5.1.7.1 SNMP System Configuration.....	205
4.3.5.1.7.2 SNMP Trap Configuration	206
4.3.5.1.7.3 SNMPv3 Community Configuration	209
4.3.5.1.7.4 SNMPv3 User Configuration	210

4.3.5.1.7.5 SNMPv3 Group Configuration	211
4.3.5.1.7.6 SNMPv3 View Configuration	211
4.3.5.1.7.7 SNMPv3 Access Configuration	212
4.3.5.1.8 RMON	213
4.3.5.1.8.1 RMON Statistics Configuration	213
4.3.5.1.8.2 RMON History Configuration	213
4.3.5.1.8.3 RMON Alarm Configuration	213
4.3.5.1.8.4 RMON Event Configuration	215
4.3.5.2 Network	216
4.3.5.2.1 Limit Control	216
4.3.5.2.2 NAS	217
4.3.5.2.3 ACL	220
4.3.5.2.3.1 Ports	220
4.3.5.2.3.2 Rate Limiters	221
4.3.5.2.3.3 Access Control List	222
4.3.5.2.4 IP Source Guard	226
4.3.5.2.4.1 Configuration	226
4.3.5.2.4.2 Static Table	227
4.3.5.2.5 ARP inspection	227
4.3.5.2.5.1 Port Configuration	227
4.3.5.2.5.2 VLAN Configuration	228
4.3.5.2.5.3 Static Table	229
4.3.5.2.5.4 Dynamic Table Configuration	229
4.3.5.3 AAA	230
4.3.5.3.1 RADIUS Configuration	230
4.3.5.3.2 TACACS+	231
4.3.6 Aggregation	232
4.3.6.1 Static	232
4.3.6.2 LACP	233
4.3.7 Loop Protection	234
4.3.8 Spanning Tree	235
4.3.8.1 Bridge Settings	236
4.3.8.2 MSTI Mapping	237
4.3.8.3 MSTI Priorities	238
4.3.8.4 CIST Ports	238
4.3.8.5 MSTI Ports	239
4.3.9 IPMC Profile	240
4.3.9.1 Profile Table	240
4.3.9.2 Address Entry	242
4.3.10 MVR	242
4.3.11 IPMC	244
4.3.11.1 IGMP Snooping	244
4.3.11.1.1 Basic Configuration	245
4.3.11.1.2 VLAN Configuration	246
4.3.11.1.3 Port Filtering Profile	247
4.3.11.2 MLD Snooping	247
4.3.11.2.1 Basic Configuration	248
4.3.11.2.2 VLAN Configuration	249
4.3.11.2.3 Port Filtering Profile	250
4.3.12 LLDP	250
4.3.12.1 LLDP Configuration	251
4.3.12.2 LLDP-MED	253
4.3.13 MAC Table	256
4.3.14 VLANs	257
4.3.15 Private VLANs	260
4.3.15.1 PVLAN Membership	260
4.3.15.2 Port Isolation	261
4.3.16 VCL	261

4.3.16.1 MAC-based VLAN	261
4.3.16.2 Protocol-based VLAN	261
4.3.16.2.1 Protocol to Group	262
4.3.16.2.2 Group to VLAN	263
4.3.16.3 IP Subnet-based VLAN	263
4.3.17 Voice VLAN	264
4.3.17.1 Configuration	264
4.3.17.2 OUI	265
4.3.18 QoS	266
4.3.18.1 Port Classification	266
4.3.18.2 Port Policing	267
4.3.18.3 Queue Policing	268
4.3.18.4 Port Scheduler	269
4.3.18.5 Port Shaping	271
4.3.18.6 Port Tag Remarking	271
4.3.18.7 Port DSCP	273
4.3.18.8 DSCP-Based QoS Ingress Classification	274
4.3.18.9 DSCP Translation	275
4.3.18.10 DSCP Classification	275
4.3.18.11 QoS Control List	275
4.3.18.12 Storm Policing	279
4.3.18.13 WRED	280
4.3.19 Mirroring	280
4.3.20 UPnP	282
4.3.21 GVRP	282
4.3.21.1 Global Config	283
4.3.21.2 Port Config	284
4.3.22 sFlow	285
4.3.22.1 Configuration	285
4.3.23 UDLD	286
4.4 MONITOR	288
4.4.1 System	288
4.4.1.1 System Information	288
4.4.1.2 Power & Fan	288
4.4.1.3 System CPU Load	289
4.4.1.4 System IP Status	289
4.4.1.5 System Log Information	290
4.4.1.6 System Detailed Log	290
4.4.2 Ports	290
4.4.2.1 State	290
4.4.2.2 SFP	291
4.4.2.3 Traffic Overview	291
4.4.2.4 QoS Statistics	292
4.4.2.5 QCL Status	292
4.4.2.6 Ports Detailed Statistics	293
4.4.3 DHCP	295
4.4.3.1 Server	295
4.4.3.1.1 Statistics	295
4.4.3.1.2 Binding	296
4.4.3.1.3 Declined IP	296
4.4.3.2 Snooping Table	296
4.4.3.2.1 Relay Statistics	297
4.4.3.2.2 Detailed Statistics	298
4.4.4 Security	299
4.4.4.1 Access Management Statistics	299
4.4.4.2 Network	300
4.4.4.2.1 Port Security	300
4.4.4.2.1.1 Switch	300

4.4.4.2.1.2 Port Status	301
4.4.4.2.2 NAS.....	301
4.4.4.2.2.1 Switch	301
4.4.4.2.2.2 Port.....	302
4.4.4.2.3 ACL Status	302
4.4.4.2.4 Dynamic ARP Inspection Table.....	303
4.4.4.2.5 Dynamic IP Source Guard Table	304
4.4.4.3 AAA.....	304
4.4.4.3.1 RADIUS Overview	304
4.4.4.3.2 RADIUS Details	305
4.4.4.4 Switch	307
4.4.4.4.1 RMON.....	307
4.4.4.4.1.1 RMON Statistics Overview	307
4.4.4.4.1.2 RMON History Overview.....	308
4.4.4.4.1.3 RMON Alarm Overview.....	309
4.4.4.4.1.4 RMON Event Overview	309
4.4.5 Aggregation.....	310
4.4.5.1 Static.....	310
4.4.6 LACP	310
4.4.6.1 System Status	310
4.4.6.2 Port Status	311
4.4.6.3 Port Statistics.....	312
4.4.7 Loop Protection	312
4.4.8 Spanning Tree	313
4.4.8.1 Bridge Status	313
4.4.8.2 Port Status	315
4.4.8.3 Port Statistics.....	316
4.4.9 MVR	316
4.4.9.1 MVR Statistics.....	316
4.4.9.2 MVR Channel Groups	317
4.4.9.3 MVR SFM Information	317
4.4.10 IPMC.....	318
4.4.10.1 IGMP Snooping.....	318
4.4.10.1.1 Status	318
4.4.10.1.2 Groups Information.....	319
4.4.10.1.3 IPv4 SFM Information.....	319
4.4.10.2 MLD Snooping	320
4.4.10.2.1 Status	320
4.4.10.2.2 Groups Information.....	321
4.4.10.2.3 IPv6 SFM Information.....	321
4.4.11 LLDP	322
4.4.11.1 Neighbors	322
4.4.11.2 LLDP-MED Neighbors.....	322
4.4.11.3 Port Statistics.....	323
4.4.12 MAC Table.....	324
4.4.13 VLANs.....	324
4.4.13.1 Membership	324
4.4.13.2 Ports	325
4.4.14 sFlow	326
4.4.15 UDLD	327
4.5 DIAGNOSTICS	328
4.5.1 Ping	328
4.5.3 Ping6	328
4.27.3 VeriPHY	329
4.6 MAINTENANCE	330
4.6.1 Restart Device.....	330
4.6.2 Factory Defaults.....	330
4.6.3 Software.....	330

4.6.3.1 Upload	330
4.6.3.2 Image Select	331
4.6.4 Configuration	331
4.6.4.1 Save	331
4.6.4.2 Download	331
4.6.4.3 Upload	332
4.6.4.4 Activate	332
4.6.4.5 Delete	332

CHAPTER 1. INTRODUCTION

1.1 Product Description

CGR-3291-NA2A is a layer 2+ managed Ethernet switches that provides stable and reliable Ethernet transmission for Carrier Ethernet access switch solution. CGR-3291-NA2A is designed in standard 1U 19-inch size and can be mountable in standard 19-inch rack. To offer the best flexibility and scalability for network deployment, CGR-3291-NA2A is equipped with 24 SFP-based 100/1000Mbps dual speed optical ports, 4 10/100/1000Mbps RJ-45 ports and 4 SFP+ 1/10Gbps dual speed uplink ports.

CGR-3291-NA2A series optionally incorporates redundant power modules. The supply derives its power from either an AC power source and/or DC power source. When two modules are installed, they provide for power redundancy. Fans are located on the rear panel of the device. The immediate fan condition can be observed via FAN LED on the front panel or via Web management.

1.2 Panels

The front of the CGR-3291-NA2A contains two power slots. Built-in power module or modules from factory are varied based on the user's order. You can have one AC power, one DC power, one AC and one DC power, two AC power supplies or two DC power supplies. Next to power supplies, 24 SFP-based slots, 4 RJ-45 ports, 4 SFP+ uplink ports, one MGMT (management) port and one console port are provided. SFP-based slots are numbered 1 through 24, from left to right as viewed from the front. The device can be configured via the MGMT or console port. Right next to the power module on the left is the protective earth grounding terminal. It is highly recommended that a stable ground be attached to this device so that any surges on power via LAN ports can be properly and safely shunted to ground.

Power Modules (options available:

AC, DC, 2 AC, 2 DC, AC+DC)

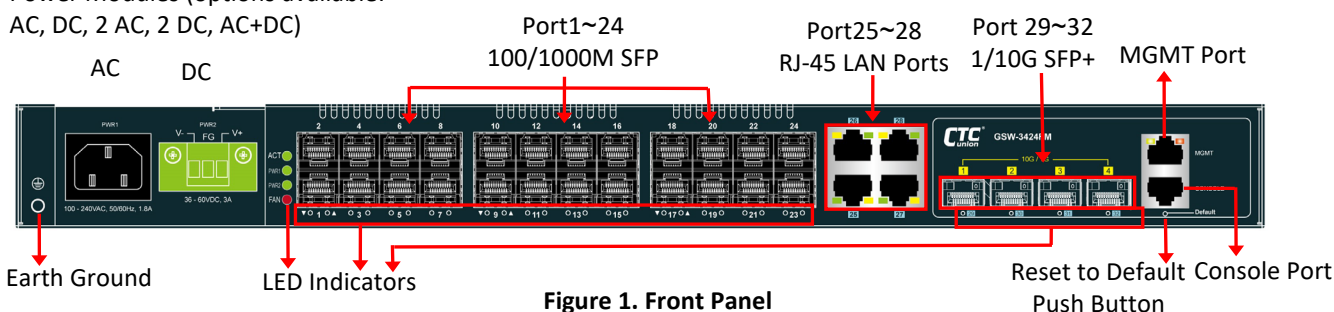


Figure 1. Front Panel

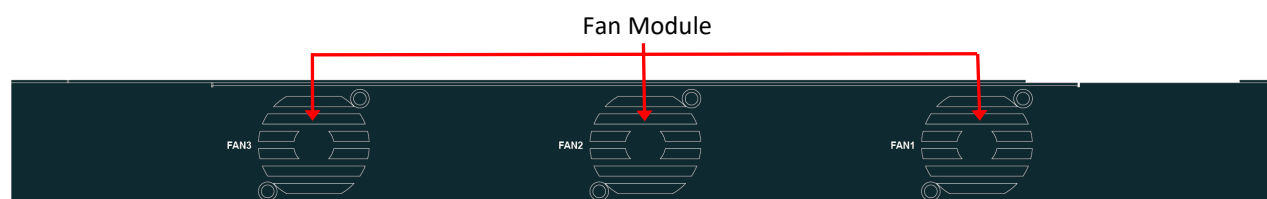


Figure 2. Rear Panel

CHAPTER 2. INSTALLATION

The CGR-3291-NA2A is designed to be placed on the flat desktop or to be mounted in a standardized 19-inch rack for rack-mount placement. The switch you purchase should come with rack-mounting brackets from the factory and these brackets are used for rack-mounting installation.

Besides, CGR-3291-NA2A is equipped with built-in power and fan modules. Types of power modules available are AC, DC, AC+DC, two AC and two DC power modules. Fans which are not removable are located on the rear panel of the device. If you need to repair fan modules, please contact your sales representatives.

In this section, we will provide necessary information about fiber connections, console connection, power connection and wall-mounting installation. Definitions of LED indicators are also provided at the end of this section.

2.1 Fiber or RJ-45 Connections

The CGR-3291-NA2A utilizes SFP modules for fiber transmissions. Each of the fiber ports has an associated status LED to indicate the presence or absence of fiber link and will also flash when there is Ethernet activity on the port. For port 1 to port 24, each of SFP cages may insert any standard SFP module and be configured for 100M or 1000M operation. For port 25 to port 28, they use 10/100/1000M RJ-45 for service connection. For port 29 to port 32, each of SFP cages may insert any SFP+ module that supports 1/10G Ethernet connectivity. Having SFP+ option for uplink connectivity offers customers a wide variety of applications for data center, enterprise wiring closet and service provider transport.

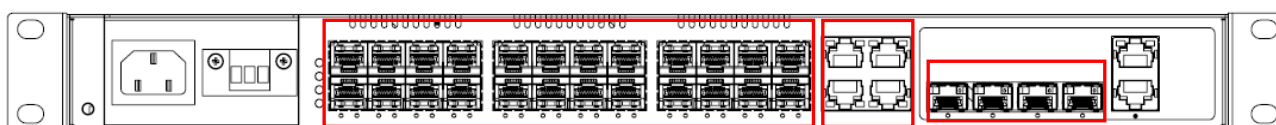


Figure 3. Fiber Connections

2.2 MGMT Port Connection

The CGR-3291-NA2A has a MGMT (Management) port for in-band management via TCP/IP connectivity. The MGMT port allows you to access Command Line Interface (CLI) using Telnet or Web management over TCP/IP using standard web browsers.

When you use the switch for the first time or restore the switch to the factory defaults, you can use RJ-45 cable to directly connect MGMT port to your management PC. Then, run a Telnet or SSH facility or web browser to communicate with the device over a TCP/IP network using the default IP address 10.1.1.1. For Telnet connection, up to 16 active Telnet sessions can access the Switch concurrently. After you successfully login to the switch, you can change the IP address to the desired one (See Chapter 3 & 4 for setting up new IP address).

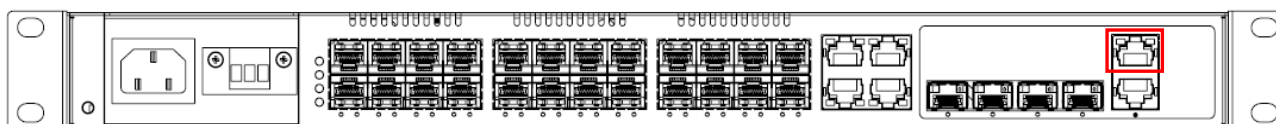


Figure 4. MGMT Port Connection

2.3 Console Port Connection

The CGR-3291-NA2A has an asynchronous terminal console port for local management via a serial terminal. The terminal provides management via a CLI (Command Line Interface) which will be familiar to many networking engineers. For most users, the CLI can be used to initially configure TCP/IP access so that further configuration can be completed via the GUI (Graphical User Interface) and any web browser.

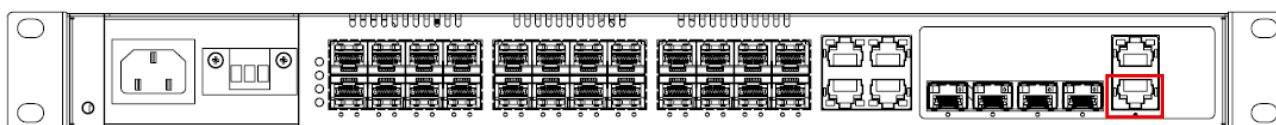
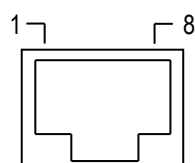


Figure 5. Console Port Connection

2.3.1 RJ-45 Pin Assignment

This RJ-45 connector provides an RS-232 DCE (data communication equipment) asynchronous serial connection for local management.



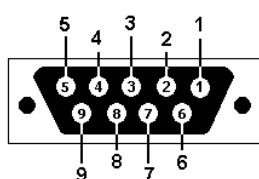
CONSOLE

Pin	Ref.	Definition	Direction
3	RxD	Receive Data	Out towards DTE
6	TxD	Transmit Data	In from DTE
4	SG	Signal Ground	N/A

2.3.2 Accessory Cable

This DB9F to RJ-45 cable provides a connection for the RS-232. This cable is used between the CGR-3291-NA2A and the serial port of terminal.

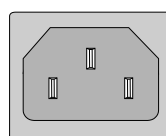
to PC COM Port



Pins				
DB9	RJ-45	Ref.	Definition	Direction
2	3	RxD	Receive Data	Out the device towards DTE
3	6	TxD	Transmit Data	In to the device from DTE
5	4	SG	Signal Ground	na

2.4 Electrical Installation

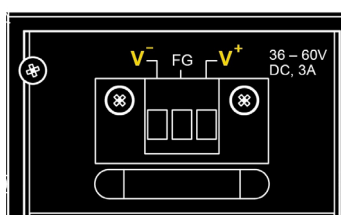
AC power module is supplied to the CGR-3291-NA2A through a standard IEC C14 3-prong receptacle, located on the front of the module. Any national power cord with IEC C13 line plug may be used to connect AC power to the power module.



Left: Live line
Right: Neutral line
Middle: Ground

Figure 6. IEC (AC) Power Connector Pin Assignment

CGR-3291-NA2A switches also provide DC module for power connection. The user must connect the device only to DC input source that has an input supply voltage from -36 to -60 VDC. If the power you use is not in this range, the device might not operate properly and there is great possibility that the device might be damaged.



Left: -V
Right: +V
Middle: Frame Ground

Figure 7. Terminal Block (DC) Power Connector Pin Assignment

2.5 Rack Mounting

When installing the rack mount brackets, be sure to correctly align the orientation pin. Use the screws provided in the rack-mounting kit to securely fasten the brackets.

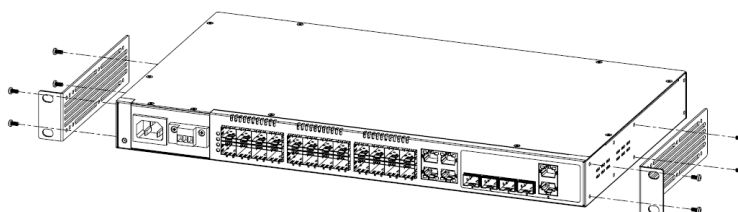


Figure 8. Attaching Rack-Mounting Brackets

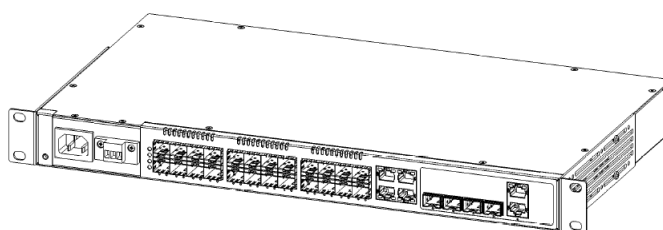


Figure 9. The Switch with Rack-Mounting Brackets

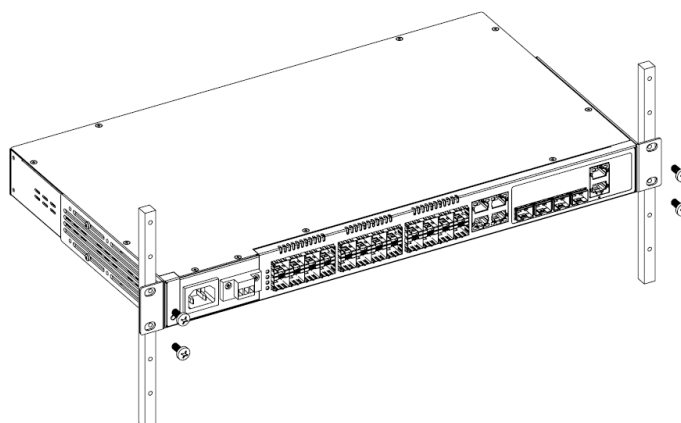


Figure 10. Mounting in Rack

2.6 LED Indicators & Reset to Default Button

LED	Color	Status	Meaning
ACT	Green	On	The switch is active.
	Red	On	Alert
	Off		The switch does not receive power.
PWR 1	Green	On	Power 1 module is working.
		Off	Power 1 module is off.
PWR 2	Green	On	Power 2 module is working.
		Off	Power 2 module is off.
FAN	Green	On	Fan is working normally.
	Red	On	Fan is working abnormally. This indicates Fan alarm status.
	Off		Fan module is off.
1~24 SFP	Green	On	Port link is up and works in 100Mbps.
		Blinking	Traffic is present.
		Off	Port link is down or has no link.
	Amber	On	Port link is up and works in 1000Mbps.
		Blinking	Traffic is present.
		Off	Port link is down or has no link.
25~28 RJ-45	Green	On	Port link is up and works in 100Mbps.
	Amber	On	Port link is up and works in 1000Mbps.
	Green	Blinking	Traffic is present.
	Green/Amber	Off	Port link is down or has no link.
29~32 SFP+	Orange	On	Port link is up and works in 1Gbps.
		Blinking	Traffic is present.
		Off	Port link is down or has no link.
	Blue	On	Port link is up and works in 10Gbps.
		Blinking	Traffic is present.
		Off	Port link is down or has no link.
Reset to default button			Press and hold the button for 7 seconds and then release to reset the device to factory default settings.

CHAPTER 3. INTRODUCTION TO CLI

3.1 Introduction

CGR-3291-NA2A, L2+ Managed Ethernet switch, provides a number of configuration/management methods. The first and very basic is serial console access. This method is also called out-of-band management and is only available when a terminal or administrator PC can be physically connected to the local CGR-3291-NA2A Series switch at the CONSOLE port using RJ45 to RS-232 console cable. Accessing the switch via CONSOLE port allows the user to use CLI (Command Line Interface) to manage and configure the device. The out-of-band management is relatively useful when you lose the network connection to the device.

On the other hand, in-band management enables you to manage the device remotely using the device's IP address. Using in-band management enables you to use Telnet console (CLI) or web browser (GUI) to access the device. If you plan on using in-band management, you need to configure the device's IP address first before it can be accessed via a LAN port.

The out-of-band management via console access, using a command line (CLI), is familiar to most network engineers. For engineers that are not comfortable using CLI, this device can also be managed using any standard Web Browser in a more user friendly 'point-and-click' method. Therefore, in most configuration scenarios, the console will only be used to initially configure the IP address, so that the device may be accessed via the other methods which require working TCP/IP.

After the device has been properly configured for the application and placed into service, a third method of configuration/management can be employed using Simple Network Management Protocol (SNMP). The operator will use SNMP management software to manage and monitor the CGR-3291-NA2A switches on a network. This requires some configuration of the device to allow SNMP management. In addition, the network management platform will need to import and compile the proprietary MIB (management information base) file so that the manager knows "how" to manage the CGR-3291-NA2A.

3.2 Access Connection

3.2.1 Telnet Operation

To use Command Line Interface (CLI), you can choose to access the device through a Telnet/ssh connection via TCP/IP network over Ethernet using MGMT port. For initial operation, use the default TCP/IP settings (10.1.1.1) to login to the device. This device supports up to 16 simultaneous Telnet sessions. Each session will disconnect automatically after a period of idle time specified by exec-timeout command.

Default TCP/IP settings:

IP Address: 10.1.1.1
Subnet Mask: 255.255.255.0
Username: admin
Password: no password (Press "Enter" Key)

3.2.2 CONSOLE Operation

Use the provided accessory cable to connect the "CONSOLE" port (RJ-45) to the PC terminal communications port (DB9). Run any terminal emulation program (HyperTerminal, PuTTY, TeraTerm Pro, etc.) and configure the communication parameters as follows:

Speed: 115,200
Data: 8 bits
Parity: None
Stop bits: 1
Flow control: None

From a cold start, the following screen will be displayed. At the "Username" prompt, enter 'admin' with **no password**.

```
Press ENTER to get started
Username: admin
Password:
```

3.3 CLI Modes

The Command Line Interface (CLI) is mainly divided into four basic modes; these are User mode, EXEC mode, Config mode and Config Interface mode. After entering the username and password, you start from the EXEC mode (prompted with "#"). The commands available in User mode and EXEC mode are limited. For more advanced configurations, you must enter Config mode or Config Interface mode. In each mode, a question mark (?) at the system prompt can be issued to obtain a list of commands available for each command mode. The following table provides a brief overview of modes available in this device.

Mode	Prompt	Enter Method	Exit Method
User mode	>	enable	disable
EXEC mode	#	Enter authorized username and password	Exit, logout
Global Config Mode	(config)#	Enter "configure terminal" after "#"	End, exit, do logout
Config Interface Mode	(config-if)#	Specify interface, interface type and number after (config)#	End, exit, do logout

3.4 Quick Keys

There are several useful quick keys you can use when editing command lines.

Keyboard	Action
?	Issue "?" to get a list of commands available in the current mode.
Up arrow key	To view the previous entered commands.
Down arrow key	To view the previous entered commands.
Tab key	To complete an unfinished command.

3.5 Command Syntax

Commands introduced in this user manual are written using the coherent symbols and easy-to-understand syntax and style. Although users can issue Help command to complete a desired command in CLI, it is useful to understand frequently-used symbols and syntax conventions. The following table lists the syntax conventions used in this user manual together with an example.

Example: (config-if-vlan)# ip address { { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }

Symbol	Function	Example	Explanation
< > (Angle bracket)	Enter a value, alphanumeric strings or keywords.	<address> <netmask>	Enter IP address and subnet mask.
[] (Square bracket)	This is an optional parameter.	[fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]]	Fallback parameter is an optional item.
{ } (Curly bracket)	A curly bracket has the following two functions: 1. If there are more than two options available, a curly bracket can be used to separate them. 2. The outer curly bracket means that this is a must parameter. At least one value should be specified.	{ { <address> <netmask> } { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }	At least specify one option to complete the command.
(Vertical bar)	Use a vertical bar to separate options.	{ { <address> <netmask> } { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }	Enter IP address or use DHCP to assign IP address automatically.

3.6 Basic Configurations

This section introduces users how to change the default IP address to the desired one and save the current running configurations to startup configurations. For detailed introductions to commands, please see section 3.7, 3.8, 3.9.

3.6.1 Configuring IPv4 Address

IP address: 192.168.0. 101
Subnet mask: 255.255.255.0

<pre># config terminal (config)# interface vlan 1 (config-if-vlan)# ip address 192.168.0.101 255.255.255.0 (config-if-vlan)# exit (config)# exit # show ip interface brief Vlan Address Method Status ----- 1 192.168.0.101/24 Manual DOWN</pre>		
---	--	--

3.6.2 Enter Config Interface Mode

For firmware 1.007 or newer, the Interface and Port mapping table is as follows:

** If your firmware version is below 1.007, please contact your sales representatives for firmware updates.

Panel Mylar Port No. Printing	Interface (CLI)	Port No. (WEB)
1	GigabitEthernet 1/1	1
2	GigabitEthernet 1/2	2
3	GigabitEthernet 1/3	3
4	GigabitEthernet 1/4	4
5	GigabitEthernet 1/5	5
6	GigabitEthernet 1/6	6
7	GigabitEthernet 1/7	7
8	GigabitEthernet 1/8	8
9	GigabitEthernet 1/9	9
10	GigabitEthernet 1/10	10
11	GigabitEthernet 1/11	11
12	GigabitEthernet 1/12	12
13	GigabitEthernet 1/13	13
14	GigabitEthernet 1/14	14
15	GigabitEthernet 1/15	15
16	GigabitEthernet 1/16	16
17	GigabitEthernet 1/17	17
18	GigabitEthernet 1/18	18
19	GigabitEthernet 1/19	19
20	GigabitEthernet 1/20	20
21	GigabitEthernet 1/21	21
22	GigabitEthernet 1/22	22
23	GigabitEthernet 1/23	23
24	GigabitEthernet 1/24	24
25	GigabitEthernet 1/25	25
26	GigabitEthernet 1/26	26
27	GigabitEthernet 1/27	27
28	GigabitEthernet 1/28	28
1 29	10GigabitEthernet 1/1	29
2 30	10GigabitEthernet 1/2	30
3 31	10GigabitEthernet 1/3	31
4 32	10GigabitEthernet 1/4	32
MGMT	GigabitEthernet 1/29	33

- If you want to enter Port 3's Config Interface mode.

```
# config terminal
(config)# interface GigabitEthernet 1/3
(config-if)#
```

Note: 1/3 means Ethernet Interface 1, Port 3.

- If you want to enter Port 29's Config Interface mode.

```
# config terminal
(config)# interface 10GigabitEthernet 1/1
(config-if)#
```

Note: 10Gigabit Ethernet Interface 1/1 equals Port 29.

- If you want to enter Port 1~3's Config Interface mode.

```
# config terminal
(config)# interface GigabitEthernet 1/1-3
(config-if)#
```

Note: 1/1-3 means Ethernet Interface 1, Port 1 to Port 3.

- If you want to enter Port 1~3 & Port 5's Config Interface mode.

```
# config terminal
(config)# interface GigabitEthernet 1/1-3,5
(config-if)#
```

Note: 1/1-3,5 means Ethernet Interface 1, Port 1 to Port 3 and Port 5.

3.6.3 Save Configurations

```
# copy running-config startup-config
Building configuration...
% Saving 1469 bytes to flash:startup-config
#
```

3.6.4 Restart the Device

```
# reload cold
% Cold reload in progress, please stand by.
#

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

RedBoot> fi lo -d managed
Image loaded from 0x80040000-0x80ae54cc
```

```
RedBoot> go

Press ENTER to get started
```

3.6.5 Load Factory Defaults

- Load factory default settings

```
# reload defaults
% Reloading defaults. Please stand by.
```

- Load factory defaults but keep IP settings

```
# reload defaults keep-ip
% Reloading defaults, attempting to keep VLAN 1 IP address. Please stand by.
```

3.6.6 Show System and Software Information

```
# show version

MEMORY          : Total=77679 KBytes, Free=51457 KBytes, Max=51417 KBytes
Flash           : 0x40000000-0x41fdffff, 510 x 0x10000 blocks
MAC Address     : 00-02-ab-00-00-01

System Contact  :
System Name     :
System Location : 2020-05-28T14:28:51+08:00
System Time     : 00:28:39
System Uptime   :

Active Image
-----
Image           : CGR-3291-NA2A.dat (primary)
Version         : "V1.007"
Date            : 2019-07-12T11:53:10+08:00

Alternative Image
-----
Image           : CGR-3291-NA2A.dat (backup)
Version         : "V1.005"
Date            : 2019-04-09T16:18:27+08:00
-----
```

3.6.7 Show Running Configurations

```
# show running-config
Building configuration...
username admin privilege 15 password none
!
vlan 1
!
!
!
no smtp server
spanning-tree mst name 00-02-ab-00-00-01 revision 0
!
```

```
interface GigabitEthernet 1/1
no spanning-tree
!
interface GigabitEthernet 1/2
no spanning-tree
!
interface GigabitEthernet 1/3
no spanning-tree
!
interface GigabitEthernet 1/4
no spanning-tree
!
-- more --, next page: Space, continue: g, quit: ^C
```

3.6.8 Show History Commands

```
# show history
config t
exit
config t
ip arp ex
exit
```

```
> show history
config t
interface GigabitEthernet 1/3
exit
interface GigabitEthernet 1/1-5
exit
interface GigabitEthernet 1/1-3,5,7
flowcontrol on
exit
show interface * status
disable
show clock detail
show dot1x
show history
```

3.6.9 Help

Help command can be issued in User, Exec, and Global Config mode to get a hint message describing how to use “show” command to get help from CLI.

```
# help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
command argument (e.g. 'show ?') and describes each possible
argument.
2. Partial help is provided when an abbreviated argument is entered
and you want to know what arguments match the input
(e.g. 'show pr?').
```

3.6.10 Logout

To close an active terminal session, issue the “logout” command in User or EXEC mode.

```
(config)# exit
# logout

Press ENTER to get started
```

```
# disable
> logout

Press ENTER to get started
```

3.7 Commands in User Mode

When you successfully login in Command Line Interface, you are in EXEC Mode (prompted with “#”). To enter User mode, issue “disable” command after # prompt. Then you will be directed to User mode with “>” prompt.

```
Username: admin
Password:
#
# disable
>
```

In User mode, only limited commands are available. These commands are used for clearing statistics, entering Exec mode and pinging the specified destination. To configure a function, you should enter Config mode or Config Interface mode.

3.7.1 > clear ip arp

Syntax: > clear ip arp

Explanation: Clear ARP cache.

3.7.2 > clear lldp statistics

Syntax: > clear lldp statistics

Explanation: Clear LLDP statistics.

3.7.3 > clear statistics

Syntax: > clear statistics {[interface] (<port_type> [<v_port_type_list>])}

<port_type>: Specify the interface type.

[<v_port_type_list>: Specify the ports that you want to clear.

Explanation: Clear statistics of the specified interfaces.

3.7.4 > *enable*

Syntax: > enable [<new_priv>]

[<new_priv: 0-15>]: Choose a privilege level.

Explanation: Enter the EXEC mode.

3.7.5 > *exit*

Syntax: > exit

Explanation: Return to the previous mode. Issuing this command in User mode will logout the Command Line Interface.

3.7.6 > *help*

Syntax: > help

Explanation: Provide help messages.

3.7.7 > *logout*

Syntax: > logout

Explanation: Logout the Command Line Interface.

3.7.8 > *ping ip*

Syntax: > ping ip <v_ip_addr> [repeat <count>] [size <size>] [interval <seconds>]

<v_ip_addr>: Specify IPv4 address that you want to ping.

[repeat <count>]: The number of packets that are sent to the destination IP or host.

[size <size>]: The size of the packet.

[interval <seconds>]: Timeout interval. The ping test is successful only when it receives echo reply from the destination IP or host within the time specified here.

Explanation: To carry out ping tests on the specified destination IPv4 address or host.

3.7.9 > ping ipv6

Syntax: > ping ipv6 <v_ipv6_addr> [repeat <count>] [size <size>] [interval <seconds>] [interface vlan <v_vlan_id>]

<v_ipv6_addr>: Specify IPv6 address that you want to ping.

[repeat <count>]: The number of packets that are sent to the destination IP or host.

[size <size>]: The size of the ping packet.

[interval <seconds>]: Timeout interval. The ping test is successful only when it receives echo reply from the destination IP or host within the time specified here.

[interface vlan <v_vlan_id>]:

Explanation: To carry out ping tests on the specified destination IPv6 address or host.

3.7.10 show commands

In User mode, “show” commands can be issued to display current status or settings of a certain command. They will be introduced in Section 3.9 “Commands in Config Mode”.

3.8 Commands in EXEC Mode

3.8.1 # clear access management statistics

Syntax: # clear access management statistics

Explanation: Clear access (HTTP, HTTPs, SNMP, Telnet, SSH) management statistics.

3.8.2 # clear access-list ace statistics

Syntax: # clear access-list ace statistics

Explanation: Clear access list entry statistics.

3.8.3 # clear dot1x statistics

Syntax: # clear dot1x statistics [interface (<port_type> [<v_port_type_list>])]

Parameter:

[interface (<port_type> [<v_port_type_list>])]: Specify the interface that you want to clear.

Explanation: Clear (the specified interfaces') dot1x statistics.

3.8.4 # clear ip arp

Syntax: # clear ip arp

Explanation: Clear ARP cache.

3.8.5 # clear ip dhcp detailed statistics

Syntax: # clear ip dhcp detailed statistics { server | client | snooping | relay | helper | all } [interface (<port_type> [<in_port_list>])]

Explanation: ClearIP DHCP statistics.

Parameter:

{ server | client | snooping | relay | helper | all }: Specify the type of information that you want to clear.

[interface (<port_type> [<in_port_list>])]: Specify the interface type and port number.

3.8.6 # clear ip dhcp relay statistics

Syntax: # clear ip dhcp relay statistics

Explanation: Clear IP DHCP Relay statistics.

3.8.7 # clear ip dhcp server binding <ip>

Syntax: # clear ip dhcp server binding <ip>

Explanation: Clear IP DHCP server IP binding information.

3.8.8 # clear ip dhcp server binding { automatic | manual | expired }

Syntax: # clear ip dhcp server binding { automatic | manual | expired }

Explanation: Clear IP DHCP server binding information.

3.8.9 # clear ip dhcp server statistics

Syntax: # clear ip dhcp server statistics

Explanation: Clear IP DHCP server binding statistics.

3.8.10 # clear ip dhcp snooping statistics

Syntax: # clear ip dhcp snooping statistics [interface (<port_type> [<in_port_list>])]

Explanation: Clear IP DHCP Snooping statistics.

3.8.11 # clear ip igmp snooping

Syntax: # clear ip igmp snooping [vlan <v_vlan_list>] statistics

Explanation: Clear IP IGMP Snooping statistics.

3.8.12 # clear ip statistics

Syntax: # clear ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Explanation: Clear IPv4 statistics for system, interface and ICMP.

3.8.13 # clear ipv6 mld snooping

Syntax: # clear ipv6 mld snooping [vlan <v_vlan_list>] statistics

Explanation: Clear statistics for IPv6 MLD Snooping.

3.8.14 # clear ipv6 neighbors

Syntax: # clear ipv6 neighbors

Explanation: Clear the table for IPv6 neighbors.

3.8.15 # clear ipv6 statistics

Syntax: # clear ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Explanation: Clear IPv6 statistics for system, interface and ICMP.

3.8.16 # clear lacp statistics

Syntax: # clear lacp statistics

Explanation: Clear LACP statistics.

3.8.17 # clear lldp statistics

Syntax: # clear lldp statistics

Explanation: Clear LLDP statistics.

3.8.18 # clear logging

Syntax: # clear logging [info] [warning] [error] [switch <switch_list>]

Explanation: Clear specific syslog events.

3.8.19 # clear mac address-table

Syntax: # clear mac address-table

Explanation: Clear MAC address table.

3.8.20 # clear mvr

Syntax: # clear mvr [vlan <v_vlan_list> | name <mvr_name>] statistics

Explanation: Clear MVR statistics.

3.8.21 # clear spanning-tree

Syntax: # clear spanning-tree { { statistics [interface (<port_type> [<v_port_type_list>])] } | { detected-protocols [interface (<port_type> [<v_port_type_list_1>])] } }

Explanation: Clear specific interfaces' Spanning Tree statistics.

3.8.22 # clear statistics

Syntax: # clear statistics [interface] (<port_type> [<v_port_type_list>])

Explanation: Clear Fast Ethernet and/or Gigabit Ethernet interfaces' statistics.

3.8.23 # config terminal

Syntax: # config terminal

Explanation: Enter the Global Config mode.

```
# config t
(config)#
```

3.8.24 # copy

Syntax: # copy { startup-config | running-config | <source_path> } { startup-config | running-config | <destination_path> } [syntax-check]

{ startup-config | running-config | <source_path> }: Specify the file type that you want to copy from. This can be "startup-config", "running-config" or a specific source file in flash or TFTP server.

{ startup-config | running-config | <destination_path> }: Specify the file type that you want to copy to. This can be "startup-config", "running-config" or a specific destination file in flash or TFTP server.

Explanation: Save running configurations to startup configurations.

```
# copy running-config startup-config
Building configuration...
% Saving 1596 bytes to flash:startup-config
#
```

Explanation: Save startup configurations to running configurations.

```
# copy startup-config running-config
Building configuration...
% Saving 1596 bytes to flash:startup-config
#
```

Explanation: Save running configurations to Flash 201

```
# copy running-config Flash:201
Building configuration...
% Saving 1487 bytes to flash:201
# dir
Directory of flash:
   r- 1970-01-01 00:00:00      284 default-config
   rw 2015-01-01 01:56:32    1487 startup-config
   rw 2015-01-01 01:56:49    1487 201
3 files, 3258 bytes total.
```

3.8.25 # delete

Syntax: # delete <path>

Explanation: Delete a file saved in Flash.

Parameters:

<Path : word>: Name of the file in Flash to be deleted.

Example: Delete a file named 201 in Flash.

```
# dir
Directory of flash:
   r- 1970-01-01 00:00:00      284 default-config
   rw 2015-01-01 01:56:32    1487 startup-config
   rw 2015-01-01 01:56:49    1487 201
3 files, 3258 bytes total.
# delete flash:201
# dir
Directory of flash:
   r- 1970-01-01 00:00:00      284 default-config
   rw 2015-01-01 01:56:32    1487 startup-config
2 files, 1771 bytes total.
```

3.8.26 # dir

Explanation: Display files in flash.

Example:

```
# dir
Directory of flash:
  r- 1970-01-01 00:00:00      284 default-config
  rw 2015-01-01 01:56:32    1487 startup-config
  rw 2015-01-01 01:56:49    1487 201
3 files, 3258 bytes total.
```

3.8.27 # disable & # enable

Explanation: Return to user mode or enter exec mode.

```
# disable
>
>
> enable
#
#
# enable 0
>
```

3.8.28 # dot1x

Syntax: # dot1x initialize [interface (<port_type> [<plist>])

[interface (<port_type> [<plist>])]: Specify the type of interface that you intend to use. "*" means all interfaces.

<plist>: Specify the ports that apply to this command.

Explanation: To initialize dot1x function in an interface immediately.

3.8.29 # firmware swap

Syntax: # firmware swap

Explanation: Use the other standby firmware image file uploaded to flash.

3.8.30 # *firmware upgrade*

Syntax: # firmware upgrade <TFTPServer_path_file : word>

<TFTPServer_path_file : word>: Specify the TFTP server IP address and firmware filename.

Explanation: Upgrade the firmware image.

3.8.31 # *ip dhcp retry interface vlan*

Syntax: # ip dhcp retry interface vlan <vlan_id>

<vlan_id>: Specify the valid VLAN ID for DHCP query.

Explanation: Restart the DHCP query process.

3.8.32 # *ipv6 dhcp-client restart*

Syntax: # ipv6 dhcp-client restart [interface vlan <v_vlan_list>]

<v_vlan_list>: Specify the VLANs associated with the IP interface.

Explanation: Restart the IPv6 client service.

3.8.33 # *more*

Syntax: # more <path>

<path>: Specify the filename.

Explanation: Display file in Flash or in TFTP server.

3.8.34 # *ping ip*

Syntax: # ping ip <v_ip_addr> [repeat <count>] [size <size>] [interval <seconds>]

Explanation: Ping the specified IP.

Parameters:

<addr>: Specify the IPv4 address or IPv6 address for ping test.

3.8.35 # ping ipv6

Syntax: #ping ipv6 <v_ipv6_addr> [repeat <count>] [size <size>] [interval <seconds>] [interface vlan <v_vlan_id>]

< v_ipv6_addr >: Specify the IPv4 address or IPv6 address for ping test.

Explanation: Ping the specified IPv6 address.

Parameters:

[repeat <count>]: The number of echo packets will be sent.

[size <size>]: The size or length of echo packets.

[interval <seconds>]: The time interval between each ping request.

[interface vlan <v_vlan_id>]: Specify the VLAN ID.

3.8.36 # reload cold

Syntax: # reload cold

Explanation: Perform a cold reload on the system.

3.8.37 # reload defaults

Syntax: # reload defaults [keep-ip]

Explanation: Restore the device to factory default settings.

Parameters:

[keep-ip]: Keep VLAN 1 IP setting.

3.8.38 # send

Syntax: # send { * | <session_list> | console 0 | vty <vty_list> } <message>

Explanation: Send messages to other tty lines.

Parameters:

{ * | <session_list> | console 0 | vty <vty_list> }: Choose one of the options.

* : Specify "*" to denote all tty users.

<session_list>: Specify a session number between 0 and 16.

console 0: This means primary terminal line.

<vty_list>: Send a message to a virtual terminal.

<message>: Enter a message in 128 characters that you want to send.

3.8.39 # terminal editing

Syntax: # terminal editing

Explanation: Enable command line editing.

Show: > show terminal
show terminal

Negation: # no terminal editing

3.8.40 # terminal exec-timeout

Syntax: # terminal exec-timeout <0-1440> [<0-3600>]

Parameters:

<0-1440>: Specify the timeout value in minutes.

[<0-3600>]: Specify the timeout value in seconds.

Explanation: Set up terminal timeout value.

Show: > show terminal
show terminal

Negation: # no terminal exec-timeout

3.8.41 # terminal history size

Syntax: # terminal history size <0-32>

Parameters:

<0-32>: Specify the current history size. "0" means to disable.

Explanation: Set up terminal history size.

Show: > show terminal
show terminal

Negation: # no terminal history size

3.8.42 # terminal length

Syntax: # terminal length <0 or 3-512>

Parameters:

<0 or 3-512>: Specify the lines displayed on the screen. "0" means no pausing.

Explanation: Set up terminal length.

Show: > show terminal
show terminal

Negation: # no terminal length

3.8.43 # terminal width

Syntax: # terminal width <0 or 40-512>

Parameters:

<0 or 40-512>: Specify the width displayed on the screen. "0" means unlimited width.

Explanation: Set up terminal display width.

Show: > show terminal
show terminal

Negation: # no terminal width

3.8.44 # no port-security shutdown

Syntax: # no port-security shutdown [interface (<port_type>[<v_port_type_list>])]

Explanation: Reopen ports that are shutdown or disabled by Port Security function.

Parameters:

[interface (<port_type>[<v_port_type_list>])]: Specify the port type and port numbers that you want to reopen.

3.8.45 # veriphy

Syntax: # veriphy [{ interface (<port_type> [<v_port_type_list>]) }]

Explanation: Run VeriPHY™ Cable Diagnostics for 10/100 and 1G copper port.

Parameters:

[interface (<port_type>[<v_port_type_list>])]: Specify the port type and port numbers that you want to run VeriPHY cable diagnostics.

3.8.46 show commands

In Exec mode, “show” commands can be issued to display current status or settings of a certain command. They will be introduced in Section 3.9 “Commands in Config Mode”.

3.9 Commands in Config Mode

3.9.1 aaa

3.9.1.1 (config)# aaa accounting

Syntax: (config)# aaa accounting { console | telnet | ssh } tacacs { [commands <priv_lvl>] [exec] }

Explanation: Configure the command and exec (login) authentication method for the client.

Parameters:

{ console | telnet | ssh }: Specify one of the authentication clients.

{ [commands <priv_lvl>] [exec] }: Use the remote TACACS server for accounting. Enable the accounting of all commands with a privilege level. Valid level values are 0 to 15. Specify "exec" to enable exec (login) accounting.

Negation: (config)# no aaa accounting { console | telnet | ssh }

Show: # show aaa

3.9.1.2 (config)# aaa authentication login

Syntax: (config)# aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }

Explanation: Configure the authentication method for the client.

Parameters:

{ console | telnet | ssh | http }: Specify one of the authentication clients.

{ { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }: Specify one of the authentication methods for the specified client. At least one method needs to be specified. Users can specify three methods at most.

local: Use the local user database on the switch for authentication.

radius: Use remote RADIUS server(s) for authentication.

tacacs: Use remote TACACS+ server(s) for authentication.

NOTE: Methods that involve remote servers will time out if the remote servers are offline. In this case the next method is tried. Each method is tried and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

Example: Set the Console client to use remote RADIUS server(s) for authentication.

```
# config t
(config)# aaa authentication login console radius
```

Negation: (config)# no aaa authentication login { console | telnet | ssh | http }

Show: # show aaa

3.9.1.3 (config)# aaa authorization

Syntax: (config)# aaa authorization { console | telnet | ssh } tacacs commands <priv_lvl> [config-commands]

Explanation: Use this command to limit the CLI commands available to a user.

Parameters:

{ console | telnet | ssh }: Specify one of the authentication clients that applies to this rule.

<priv_lvl> : Use the remote TACACS server for authorization. Authorize all commands with a privilege level. Valid level values are 0 to 15.

[config-commands]: Specify "config-commands" to authorize configuration commands.

Negation: (config)# no aaa authorization { console | telnet | ssh }

Show: # show aaa

3.9.2 (config)# access management

Syntax: (config)# access management <access_id> <access_vid> <start_addr> [to <end_addr>] { [web] [snmp] [telnet] | all }

Explanation: Create an access management rule.

Parameters:

<access_id: 1-16>: Specify an ID for this access management entry.

<access_vid>: Indicates the VLAN ID for the access management entry.

<start_addr> [to <end_addr>]: Indicate the starting and ending IP address for the access management entry.

{ [web] [snmp] [telnet] | all }: Specify matched hosts can access the switch from which interface.

Example: Allow IP 192.168.0.1 to 192.168.0.10 to access the device via Web, SNMP and Telnet.

```
# config t
(config)# access management 1 1 192.168.0.1 to 192.168.0.10 all
```

Negation: (config)# no access management
(config)# no access management <access_id>

Show: # show access management [statistics | <access_id_list>]

Clear: # clear access management statistics

3.9.3 (config)# access-list

3.9.3.1 (config)# access-list ace

Syntax: (config)# access-list ace <Aceld : 1-256> [action {deny | filter | permit}} [dmac-type {any| broadcast | multicast | unicast }] [frame-type {any| arp|etype|ipv4|ipv4-icmp|ipv4-tcp|ipv4-udp|ipv6|ipv6-icmp|ipv6-tcp|ipv6-udp}] [ingress {any | interface <PORT_TYPE> }] [logging] [next { <Aceld : 1-256>|last}}] [policy <PolicyId : 0-255>] [rate-limiter {<RateLimiterId : 1-16>|disable}}] [redirect {disable| interface <PORT_TYPE>}}] [shutdown] [tag {any|tagged|untagged}}] [tag-priority {0-1| 0-3| 2-3| 4-5| 4-7| 6-7| <TagPriority : 0-7>|any}}] [vid { <Vid : 1-4095>|any}}]

Explanation: Configure an access control list.

Parameters:

<Aceld : 1-256>: Specify access control list ID that applies to this rule.

[action {deny | filter | permit}}]: Specify the action that applies to this rule.

[dmac-type {any| broadcast | multicast | unicast }]: Specify destination MAC type that applies to this rule.

[frame-type {any| arp|etype|ipv4|ipv4-icmp|ipv4-tcp|ipv4-udp|ipv6|ipv6-icmp|ipv6-tcp|ipv6-udp}]: Specify the frame type that applies to this rule.

[ingress {any | interface <PORT_TYPE> }]: Specify the ingress port.

[logging]: Enable logging function.

[mirror]: Enable the function of mirroring frames to destination mirror port.

[next { <Aceld : 1-256>|last}}]: Insert the current ACE ID before the next ACE ID or put the ACE ID to the last one.

[policy <PolicyId : 0-255>]: Specify the policy ID.

[rate-limiter {<RateLimiterId : 1-16>|disable}}]: Specify the rate limit ID or disable this function.

[redirect {disable| interface <PORT_TYPE>}}]: Redirect frames to a specific port or disable this function.

[shutdown]: Enable shutdown function.

[tag {any|tagged|untagged}}]: Specify whether frames should be tagged or untagged.

[tag-priority {0-1| 0-3| 2-3| 4-5| 4-7| 6-7| <TagPriority : 0-7>|any}}]: Specify the priority value.

[vid { <Vid : 1-4095>|any}}]: Specify the VLAN ID.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [<ace_list>]]

Negation: (config)# no access-list ace <ace_list>

Clear: # clear access-list ace statistics

3.9.3.2 (config)# access-list ace update

Syntax: (config)# access-list ace update <AcelId : 1-256> [action {deny | filter | permit}} [dmac-type {any| broadcast | multicast | unicast }] [frame-type {any| arp| etype| ipv4| ipv4-icmp| ipv4-tcp| ipv4-udp| ipv6| ipv6-icmp| ipv6-tcp| ipv6-udp}] [ingress {any | interface <PORT_TYPE> }] [logging] [next { <AcelId : 1-256>|last}}] [policy <PolicyId : 0-255>] [rate-limiter {<RateLimiterId : 1-16>|disable}}] [redirect {disable| interface <PORT_TYPE>}}] [shutdown] [tag {any| tagged| untagged}}] [tag-priority {0-1| 0-3| 2-3| 4-5| 4-7| 6-7| <TagPriority : 0-7>|any}}] [vid { <Vid : 1-4095>|any}}]

Explanation: Update an access control list.

Parameters:

<AcelId : 1-256>: Specify access control list ID that applies to this rule.

[action {deny | filter | permit}}]: Specify the action that applies to this rule.

[dmac-type {any| broadcast | multicast | unicast }]: Specify destination MAC type that applies to this rule.

[frame-type {any| arp| etype| ipv4| ipv4-icmp| ipv4-tcp| ipv4-udp| ipv6| ipv6-icmp| ipv6-tcp| ipv6-udp}]: Specify the frame type that applies to this rule.

[ingress {any | interface <PORT_TYPE> }]: Specify the ingress port.

[logging]: Enable logging function.

[mirror]: Enable the function of mirroring frames to destination mirror port.

[next { <AcelId : 1-256>|last}}]: Insert the current ACE ID before the next ACE ID or put the ACE ID to the last one.

[policy <PolicyId : 0-255>]: Specify the policy ID.

[rate-limiter {<RateLimiterId : 1-16>|disable}}]: Specify the rate limit ID or disable this function.

[redirect {disable| interface <PORT_TYPE>}}]: Redirect frames to a specific port or disable this function.

[shutdown]: Enable shutdown function.

[tag {any| tagged| untagged}}]: Specify whether frames should be tagged or untagged.

[tag-priority {0-1| 0-3| 2-3| 4-5| 4-7| 6-7| <TagPriority : 0-7>|any}}]: Specify the priority value.

[vid { <Vid : 1-4095>|any}}]: Specify the VLAN ID.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [<ace_list>]]

Negation: (config)# no access-list ace <ace_list>

3.9.3.3 (config)# access-list rate-limiter

Syntax: (config)# access-list rate-limiter [<rate_limiter_list>] { pps <pps_rate> | 100pps <pps100_rate> | kpps <kpps_rate> | 100kpps <kpps100_rate> }

Explanation: Configure rate limiter that applies to each rate limit ID.

Parameters:

[<rate_limiter_list>]: Specify the “rate limit ID”, “100kpps” or “pps” . The allowed rate limit ID range is from 1~16.

{ pps <pps_rate> | 100pps <pps100_rate> | kpps <kpps_rate> | 100kpps <kpps100_rate> }: Specify the rate limit rate.

Show: # show access-list rate-limiter [<RateLimiterList : 1~16>]

3.9.3.4 (config-if)# access-list action

Syntax: (config-if)# access-list action { permit|deny}

Explanation: Configure a specific port’s action option.

Parameters:

{ permit|deny}: Permit or deny frames on a specific port.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]]

3.9.3.5 (config-if)# access-list logging

Syntax: (config-if)# access-list logging

Explanation: Enable a specific port’s logging function.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]]

Negation: (config-if)# no access-list logging

3.9.3.6 (config-if)# access-list policy

Syntax: (config-if)# access-list policy <policy_id>

Parameters:

<policy_id:0-255>: Specify a policy ID that applies to this specific port.

Explanation: Apply a policy ID to a specific port.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]]

Negation: (config-if)# no access-list policy

3.9.3.7 (config-if)# access-list port-state

Syntax: (config-if)# access-list port-state

Explanation: Enable a specific port's port state.

Negation: (config-if)# no access-list port-state

3.9.3.8 (config-if)# access-list rate-limiter

Syntax: (config-if)# access-list rate-limiter <rate_limiter_id>

Parameters:

<rate_limiter_id:1-16>: Specify a rate limiter ID to a specific port.

Explanation: Apply a rate limiter ID to a specific port.

Negation: (config-if)# no access-list rate-limiter

3.9.3.9 (config-if)# access-list shutdown

Syntax: (config-if)# access-list shutdown

Explanation: Shutdown this port when specified rules are matched.

Negation: (config-if)# no access-list shutdown

3.9.3.10 (config-if)# access-list {redirect}

Syntax: (config-if)# access-list { redirect } interface { <port_type> <port_type_id> | (<port_type> [<port_type_list>]) }

Parameters:

{ redirect | port-copy }: Redirect this port's frames to the specified port.

interface { <port_type> <port_type_id> | (<port_type> [<port_type_list>]) }: Specify the redirect or copy port type and port list.

Explanation: Redirect this port's frames to the specified port.

Negation: (config-if)# no access-list redirect

3.9.4 (config)# aggregation

3.9.4.1 (config)# aggregation mode

Syntax: (config)# aggregation mode { [smac] [dmac] [ip] [port] }

Explanation: Configure aggregation mode.

Parameters:

[smac]: All traffic from the same Source MAC address is output on the same link in a trunk.

[dmac]: All traffic with the same Destination MAC address is output on the same link in a trunk.

[ip]: All traffic with the same source and destination IP address is output on the same link in a trunk.

[port]: All traffic with the same source and destination TCP/UDP port number is output on the same link in a trunk.

Negation: (config)# no aggregation mode

Show: # show aggregation [mode]

3.9.4.2 (config-if)# aggregation group

Syntax: (config-if)# aggregation group <unit>

Explanation: Add this specific interface to the specified aggregation group.

Parameters:

<unit>: Specify the aggregation group ID.

Negation: (config-if)# no aggregation group

Show: # show aggregation [mode]

3.9.5 (config)# banner

3.9.5.1 (config)# banner [motd] <banner>

Syntax: (config)# banner [motd] <banner>

Parameters:

[motd]: Type in the message of the day.

Explanation: Configure the message of the day.

Negation: (config)# no banner [motd]

3.9.5.2 (config)# banner exec <banner>

Syntax: (config)# banner exec <banner>

Explanation: Display the configured message when successfully entering Exec mode.

Negation: (config)# no banner exec

3.9.5.3 (config)# banner login <banner>

Syntax: (config)# banner login <banner>

Explanation: Display the configured message when prompted for login ID and password.

Negation: (config)# no banner login

3.9.6 (config)# clock

3.9.6.1 (config)# clock summer-time <word16> date

Syntax: clock summer-time <word16> date [<start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [<offset_var>]]

Explanation: Configure daylight saving time. This is used to set the clock forward or backward according to the configurations set for a defined Daylight Saving Time duration. “Recurring” command is used to repeat the configuration every year.

Parameters:

summer-time <word16>: Specify a description for this day-light setting.

date [<start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [<offset_var>]]

<start_month_var:1-12>: Specify the starting month.

<start_date_var: 1-31>: Specify the starting day.

<start_year_var:2000-2097>: Specify the starting year.

<start_hour_var: hh:mm>: Specify the time to start.

<end_month_var:1-12>: Specify the ending month.

<end_date_var: 1-31>: Specify the ending day.

<end_year_var:2000-2097>: Specify the ending year.

<end_hour_var: hh:mm>: Specify the time to start.

[<offset_var: 1-1440>]: Specify the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

Negation: (config)# no clock summer-time

Show: > show clock
 > show clock detail
 # show clock
 # show clock detail

3.9.6.2 (config)# clock summer-time <word16> recurring

Syntax: (config)# clock summer-time <word16> recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]]

Explanation: Configure daylight saving time. This is used to set the clock forward or backward according to the configurations set for a defined Daylight Saving Time duration. “Recurring” command is used to repeat the configuration every year.

Parameters:

summer-time <word16>: Specify a description for this day-light setting.

recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]]

<start_week_var:1-5>: Specify the starting week.

<start_day_var: 1-31>: Specify the starting day.

<start_month_var:1-12>: Specify the starting month.

<start_hour_var: hh:mm>: Specify the time to start.

<end_week_var:1-5>: Specify the ending week.

<end_day_var: 1-31>: Specify the ending day.

<end_month_var: 1-12>: Specify the ending month.

<end_hour_var: hh:mm>: Specify the time to end.

[<offset_var: 1-1440>]: Specify the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

Negation: (config)# no clock summer-time

Show: # show clock
 # show clock detail

3.9.6.3 (config)# clock timezone

Syntax: (config)# clock timezone <word> <-23-23> [<0-59>]

Explanation: Configure a timezone used in the switch.

Parameters:

<word16>: Specify the name of the timezone.

<-23-23>: Hours offset from UTC.

[<0-59>]: Minutes offset from UTC.

Negation: (config)# no clock timezone

Show: # show clock
show clock detail

3.9.7 (config)# default

3.9.7.1 (config)# default access-list rate-limiter

Syntax: (config)# default access-list rate-limiter [<rate_limiter_list>]

Explanation: To default the specified rate-limiter ID.

Parameters:

[<rate_limiter_list: 1-16>]: Specify a rate limiter ID.

Example: To default rate-limiter 1.

```
# config t
(config)# default access-list rate-limiter 1
```

3.9.8 (config)# dot1x

3.9.8.1 (config)# dot1x system-auth-control

Syntax: (config)# dot1x system-auth-control

Explanation: To enable 802.1x service.

Parameters: None.

Example: Enable 802.1x service.

```
# config t
(config)# dot1x system-auth-control
```

Negation: (config)# no dot1x system-auth-control

Show: > show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]
show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]

3.9.8.2 (config)# dot1x re-authentication

Syntax: (config)# dot1x re-authentication

Explanation: Set clients to be re-authenticated after an interval set in "Re-authenticate" field. Re-authentication can be used to detect if a new device is attached to a switch port.

Example: Enable re-authentication function.

```
# config t
(config)# dot1x re-authentication
```

Negation: (config)# no dot1x re-authentication

Show: > show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]
show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]

3.9.8.3 (config)# dot1x authentication timer re-authenticate

Syntax: (config)# dot1x authentication timer re-authenticate <1-3600>

Explanation: Specify the time interval for a connected device to be re-authenticated. By default, the re-authenticated period is set to 3600 seconds. The allowed range is 1 - 3600 seconds.

Parameters:

<1-3600>: Specify a re-authentication value between 1 and 3600.

Example: Set re-authentication timer to 100.

```
# config t
(config)# dot1x authentication timer re-authenticate 100
```

Negation: (config)# no dot1x authentication timer re-authenticate

3.9.8.4 (config)# dot1x timeout tx-period

Syntax: (config)# dot1x timeout tx-period <v_1_to_65535>

Explanation: Specify the time that the switch waits for a supplicant response during an authentication session before transmitting a Request Identify EAPOL packet. By default, it is set to 30 seconds.

Parameters:

<v_1_to_65535>: Specify a timeout value between 1 and 65535 (seconds).

Example: Set EAPOL timeout to 30 seconds.

```
# config t
(config)# dot1x timeout tx-period 30
```

Negation: (config)# no dot1x timeout tx-period

3.9.8.5 (config)#dot1x authentication timer inactivity

Syntax: (config)# dot1x authentication timer inactivity <10-1000000>

Explanation: Specify the period that is used to age out a client's allowed access to the switch via 802.1X and MAC-based authentication. The default period is 300 seconds. The allowed range is 10 - 1000000 seconds.

Parameters:

<10-1000000>: Specify a value between 10 and 1000000 (seconds).

Example: Set the aging time to 300 seconds.

```
# config t
(config)# dot1x authentication timer inactivity 300
```

Negation: (config)# no dot1x authentication timer inactivity

3.9.8.6 (config)# dot1x timeout quiet-period

Syntax: (config)# dot1x timeout quiet-period <v_10_to_1000000>

Explanation: The time after an EAP Failure indication or RADIUS timeout that a client is not allowed access. This setting applies to ports running Single 802.1X, Multi 802.1X, or MAC-based authentication. By default, hold time is set to 10 seconds. The allowed range is 10 - 1000000 seconds.

Parameters:

<10-1000000>: Specify a value between 10 and 1000000 (seconds).

Example: Set hold time to 30 seconds.

```
# config t
(config)# dot1x timeout quiet-period 30
```

Negation: (config)# no dot1x timeout quiet-period

3.9.8.7 (config)# dot1x feature

Syntax: (config)# dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }

Explanation: Enable the specified feature.

Parameters:

{ [guest-vlan] [radius-qos] [radius-vlan] }:

[guest-vlan]: Enable guest VLAN. A Guest VLAN is a special VLAN typically with limited network access. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

[radius-qos]: Enable RADIUS assigned QoS.

[radius-vlan]: Enable RADIUS VLAN. RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature.

Example: Enable guest VLAN service.

```
# config t
(config)# dot1x feature guest-vlan
```

Negation: (config)# no dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }

3.9.8.8 (config)# dot1x guest-vlan

Syntax: (config)# dot1x guest-vlan <value>

Explanation: Configure a guest VLAN ID.

Parameters:

<value:1-4095>: Specify the guest VLAN ID. The allowed VLAN ID range is from 1 to 4095.

Negation: (config)# no dot1x guest-vlan

3.9.8.9 (config)# dot1x guest-vlan supplicant

Syntax: (config)# dot1x guest-vlan supplicant

Explanation: Enable Guest VLAN supplicant function. The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. When enabled, the switch does not maintain the EAPOL packet history and allows clients that fail authentication to access the guest VLAN, regardless of whether EAPOL packets had been detected on the interface. Clients that fail authentication can access the guest VLAN.

Negation: (config)# no dot1x guest-vlan supplicant

3.9.8.10 (config)# dot1x max-reauth-req

Syntax: (config)# dot1x max-reauth-req <value>

Explanation: The maximum number of times the switch transmits an EAPOL Request Identity frame without receiving a response before adding a port to the Guest VLAN. The value can only be changed when the Guest VLAN option is globally enabled. The range is 1 – 255.

Parameters:

<value:1-255>: Specify a value between 1 and 255.

Negation: (config)# no dot1x max-reauth-req

3.9.8.11 (config-if)# dot1x port-control

Syntax: (config-if)# dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-based }

Parameters:

{ force-authorized | force-unauthorized | auto | single | multi | mac-based }: Specify one of the authentication modes on the selected interfaces. This setting works only when NAS is globally enabled. The following modes are available:

force-authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

force unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

auto (Port-Based 802.1X): This mode requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.

single (802.1X): In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the "Port Security" module is used to secure a supplicant's MAC address once successfully authenticated.

multi (802.1X): In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the "Port Security" module.

mac-based: Unlike port-based 802.1X, MAC-based authentication do not transmit or receive EAPOL frames. In MAC-based authentication, the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator

between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

Example: Set Gigabit Ethernet port 1-10's admin state to "auto"

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x port-control auto
```

Negation: (config-if)# no dot1x port-control

3.9.8.12 (config-if)# dot1x guest-vlan

Syntax: (config-if)# dot1x guest-vlan

Explanation: Enable the guest VLAN on the selected interfaces.

Parameters: None.

Example: Enable guest VLAN on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x guest-vlan
```

Negation: (config-if)# no dot1x guest-vlan

3.9.8.13 (config-if)# dot1x radius-qos

Syntax: (config-if)# dot1x radius-qos

Explanation: Enable RADIUS Assigned QoS on the selected interfaces.

Parameters: None.

Example: Enable RADIUS Assigned QoS on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x radius-qos
```

Negation: (config-if)# no dot1x radius-qos

3.9.8.14 (config-if)# dot1x radius-vlan

Syntax: (config-if)# dot1x radius-vlan

Explanation: Enable RADIUS Assigned VLAN on the selected interfaces.

Parameters: None.

Example: Enable RADIUS Assigned VLAN on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x radius-vlan
```

Negation: (config-if)# no dot1x radius-vlan

3.9.8.15 (config-if)# dot1x re-authenticate

Syntax: (config-if)# dot1x re-authenticate

Explanation: Schedules reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. This command only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Show: > show dot1x statistics { eapol | radius | all } [interface (<port_type> [<v_port_type_list>])]
show dot1x statistics { eapol | radius | all } [interface (<port_type> [<v_port_type_list>])]

3.9.9 (config-if)# duplex

Syntax: (config-if)# duplex { half | full | auto [half | full] }

Explanation: Configure port's duplex mode.

Parameters:

{ half | full | auto [half | full] }: Specify the duplex mode for this specific interface.

Example: Set port 1's duplex mode to auto.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# duplex auto
```

Negation: (config-if)# no duplex

Show: > show interface (<port_type> [<v_port_type_list>]) status
show interface (<port_type> [<v_port_type_list>]) status

3.9.10 (config)# enable

3.9.10.1 (config)# enable password

Syntax: (config)# enable password <password>

Explanation: Configure password for Enable mode.

Parameters:

password <password>: Specify the enable mode password.

3.9.10.2 (config)# enable password level

Syntax: (config)# enable password [level <priv: 1-15>] <password>

Explanation: Configure enable password and privilege level.

Parameters:

[level <priv: 1-15>]: Specify the privilege level for this password.

<password>: Specify a password for Enable mode.

Negation: (config)# no enable password [level <priv>]

3.9.10.3 (config)# enable secret

Syntax: (config)# enable secret { 0 | 5 } [level <priv: 1-15>] <password>

Parameters:

{ 0 | 5 } : Specify “0” to denote unencrypted secret (cleartext). Specify “5” to denote encrypted secret (MD5).

[level <priv: 1-15>]: Specify the privilege level for this password.

<password>: Specify the enable mode password.

Explanation: Configure enable secret password and privilege level.

Negation: (config)# no enable secret { [0 | 5] } [level <priv>]

3.9.11 (config-if)# excessive-restart

Syntax: (config-if)# excessive-restart

Explanation: Restart backoff algorithm after 16 collisions (No excessive-restart means discard frames after 16 collisions.)

Negation: (config-if)# no excessive-restart

Show: > show interface (<port_type> [<v_port_type_list>]) status
show interface (<port_type> [<v_port_type_list>]) status

3.9.12 (config)# fanmode { auto | full | low }

Syntax: (config)# fanmode { auto | full | low }

Explanation: Adjust the fan speed of the device.

Parameters:

auto: The fan speed is adjusted automatically depending on the current temperature of the device.

full: The fan operates in full speed. Check current revolutions of per minutes (RPM) in **Monitor > System > Power & Fan** section.

low: This mode slows down the fan speed. Check current revolutions of per minutes (RPM) in **Monitor > System > Power & Fan** section.

3.9.13 (config-if)# flowcontrol { on | off }

Syntax: (config-if)# flowcontrol { on | off }

Explanation: Enable or disable flow control for this specific interface.

Parameters:

{ on | off }: Enable or disable flow control.

Negation: (config-if)# no flowcontrol

Show: > show interface (<port_type> [<v_port_type_list>]) status
show interface (<port_type> [<v_port_type_list>]) status

3.9.14 (config-if)# frame-length-check

Syntax: (config-if)# frame-length-check

Explanation: Enable Frame Length Check function. This configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch.

Negation: (config-if)# no frame-length-check

Show: # show running-config

3.9.15 (config-if)# green-ethernet

3.9.15.1 (config-if)# green-ethernet energy-detect

Syntax: (config-if)# green-ethernet energy-detect

Explanation: Enable power saving function for this specific interface when there is no link partner.

Negation: (config-if)# no green-ethernet energy-detect

Show: # show green-ethernet energy-detect [interface (<port_type> [<port_list>])]

3.9.15.2 (config-if)# green-ethernet short-reach

Syntax: (config-if)# green-ethernet short-reach

Explanation: Enable power saving for ports which is connect to link partner with short cable.

Negation: (config-if)# no green-ethernet short-reach

Show: # show green-ethernet short-reach [interface (<port_type> [<port_list>])]

3.9.16 (config)# gvrp

3.9.16.1 (config)# gvrp

Syntax: (config)# gvrp

Explanation: Globally enable GVRP function.

Parameters: None.

Example: Globally enable GVRP function.

```
# config t
(config)# gvrp
(config)#
```

Negation: (config)# no gvrp

3.9.16.2 (config)# gvrp max-vlans

Syntax: (config)# gvrp max-vlans <maxvlans>

Explanation: Set up the maximum number of VLANs can be learned via GVRP.

Parameters:

<maxvlans>: Specify the number of VLANs learned via GVRP.

Example: Set the maximum number of VLANs can be learned via GVRP to 20.

```
# config t
(config)# gvrp
(config)# gvrp max-vlans 20
```

Negation: (config)# no gvrp max-vlans <maxvlans>

3.9.16.3 (config)# gvrp time

Syntax: (config)# gvrp time { [join-time <jointime>] [leave-time <leavetime>] [leave-all-time <leavealltime>] }

Explanation: Set up the maximum number of VLANs can be learned via GVRP.

Parameters:

[join-time <jointime>]: Specify the amount of time in units of centi-seconds that PDUs are transmitted. The default value is 20 centi-seconds. The valid value is 1~20.

[leave-time <leavetime>]: Specify the amount of time in units of centi-seconds that the device waits before deleting the associated entry. The leave time is activated by a "Leave All-time" message sent/received and cancelled by the Join message. The default value is 60 centi-seconds.

NOTE: The "LeaveAll-time" parameter must be greater than the "Leave-time" parameter.

[leave-all-time <leavealltime>]: Specify the amount of time that "LeaveAll" PDUs are created. A LeaveAll PDU indicates that all registrations are shortly de-registered. Participants will need to rejoin in order to maintain registration. The valid value is 1000 to 5000 centi-seconds. The factory default 1000 centi-seconds.

NOTE: The "LeaveAll-time" parameter must be greater than the "Leave-time" parameter.

Negation: (config)# no gvrp time { [join-time <jointime>] [leave-time <leavetime>] [leave-all-time <leavealltime>] }

3.9.16.4 (config-if)# gvrp

Syntax: (config-if)# gvrp

Explanation: Enable GVRP function on the specified interfaces.

Parameters: None.

Example: Enable GVRP function on port 1~5.

```
# config t
(config)# interface GigabitEthernet 1/1-5
(config-if)# gvrp
(config-if)#
```

Negation: (config-if)# no gvrp

3.9.17 (config)# hostname

Syntax: (config)# hostname <WORD>

Explanation: Specify a descriptive name for this switch.

Parameters:

<WORD32>: Specify a descriptive name for this device. Indicate the hostname for this device. Alphabets (A-Z; a-z), digits (0-9) and minus sign (-) can be used. However, space characters are not allowed. The first character must be an alphabet character. The first and last character must not be a minus sign. The allowed string length is 0 – 255.

Example: Set the hostname to AccessSW.

```
# config t
(config)# hostname AccessSW
AccessSW(Config)#
```

Negation: (config)# no hostname

Show: > show version
show version

3.9.18 (config)# interface

3.9.18.1 (config)# interface (<port_type> [<plist>])

Syntax: (config)# interface (<port_type> [<plist>])

Explanation: Enter Config Interface mode for this specific interface.

Parameters:

<port_type> [<plist>]: Specify the port type and port number.

Example: Enter Config Interface mode for Gigabit Ethernet port 1.

```
# config t
(config)#
(config)# interface GigabitEthernet 1/1
(config-if)#
```

Show: > show interface (<port_type> [<in_port_list>]) switchport [access | trunk | hybrid]
> show interface (<port_type> [<v_port_type_list>]) capabilities
> show interface (<port_type> [<v_port_type_list>]) statistics [{ packets | bytes | errors | discards | filtered |
{ priority [<priority_v_0_to_7>] } }] [{ up | down }]
> show interface (<port_type> [<v_port_type_list>]) status
> show interface (<port_type> [<v_port_type_list>]) veriphy
> show interface vlan [<vlist>]

```
# show interface ( <port_type> [ <in_port_list> ] ) switchport [ access | trunk | hybrid ]
# show interface ( <port_type> [ <v_port_type_list> ] ) capabilities
```



```
# show interface ( <port_type> [ <v_port_type_list> ] ) statistics [ { packets | bytes | errors | discards | filtered |
{ priority [ <priority_v_0_to_7> ] } } ] [ { up | down } ]
# show interface ( <port_type> [ <v_port_type_list> ] ) status
# show interface ( <port_type> [ <v_port_type_list> ] ) veriphy
# show interface vlan [ <vlist> ]
```

Clear: # clear statistics { [interface] (<port_type> [<v_port_type_list>]) }

3.9.18.2 (config)# interface vlan

Syntax: (config)# interface vlan <vlist>

Explanation: Enter Config Interface VLAN mode for this specific interface.

Example: Enter Config Interface VLAN 1 for port 1.

```
# config t
(config)#
(config)# interface vlan 1
(config-if-vlan)#
```

3.9.19 (config)# ip

3.9.19.1 (config)# ip arp inspection

Syntax: (config)# ip arp inspection

Explanation: Enable ARP inspection function.

Negation: (config)# no ip arp inspection

Show: > show ip arp inspection [interface (<port_type> [<in_port_type_list>]) | vlan <in_vlan_list>]
show ip arp inspection [interface (<port_type> [<in_port_type_list>]) | vlan <in_vlan_list>]

Clear: # clear ip arp

3.9.19.2 (config)# ip arp inspection entry interface

Syntax: (config)# ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>

Explanation: Create ARP static entry.

Parameters:

<port_type> <in_port_type_id>: Specify the port type and port number.

<vlan_var>: Specify a configured VLAN ID.

<mac_var>: Specify an allowed source MAC address in ARP request packets.

<ipv4_var>: Specify an allowed source IP address in ARP request packets.

Negation: (config)# no ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>

Show: # show ip arp inspection entry [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]

Clear: # clear ip arp

3.9.19.3 (config)# ip arp inspection translate

Syntax: (config)# ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>]

Explanation: Translate the dynamic entry to static one.

Parameters:

<port_type> <in_port_type_id>: Specify the port type and port number.

<vlan_var>: Specify a configured VLAN ID.

<mac_var>: Specify an allowed source MAC address in ARP request packets.

<ipv4_var>: Specify an allowed source IP address in ARP request packets.

Show: # show ip arp inspection entry [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]

3.9.19.4 (config)# ip arp inspection vlan

Syntax: (config)# ip arp inspection vlan <in_vlan_list>

Explanation: Specify ARP inspection is enabled on which VLAN.

Parameters:

<in_vlan_list>: Specify a list of VLAN ID to be used for ARP inspection.

Negation: (config)# no ip arp inspection vlan <in_vlan_list>

Show: < show ip arp
show ip arp

Clear: # clear ip arp

3.9.19.5 (config)# ip arp inspection vlan <in_vlan_list> logging

Syntax: (config)# ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }

Explanation: Enable log function.

Parameters:

{ deny | permit | all }: Specify one of the log types.

Deny: Log denied entries.

Permit: Log permitted entries.

All: Log all entries.

Negation: (config)# no ip arp inspection vlan <in_vlan_list> logging

Show: < show ip arp
show ip arp

Clear: # clear ip arp

3.9.19.6 (config)# ip dhcp excluded-address

Syntax: (config)# ip dhcp excluded-address <low_ip> [<high_ip>]

Parameters:

<low_ip> [<high_ip>]: Specify the IP address range that will not be used for DHCP IP assignment.

Explanation: Configure IP addresses that are not used for DHCP IP allocation.

Example: Exclude IP address 1.2.3.4 to 1.2.3.10 from DHCP IP allocation pool..

```
# config t
(config)# ip dhcp excluded-address 1.2.3.4 1.2.3.10
(config)# exit
# show ip dhcp excluded-address
      Low Address      High Address
      -----
01  1.2.3.4          1.2.3.10

#
```

Negation: (config)# no ip dhcp excluded-address <low_ip> [<high_ip>]

Show: # show ip dhcp excluded-address

3.9.19.7 (config)# ip dhcp pool

Syntax: (config)# ip dhcp pool <pool_name>

Parameters:

<pool_name>: Specify the DHCP pool name in 32 characters.

Explanation: Configure the pool name for DHCP IP addresses.

Negation: (config)# no ip dhcp pool <pool_name>

Show: # show ip dhcp pool

3.9.19.8 (config)# ip dhcp relay

Syntax: (config)# ip dhcp relay

Explanation: Enable DHCP relay function.

Example: Enable DHCP relay function.

```
# config t
(config)# ip dhcp relay
```

Negation: (config)# no ip dhcp relay

Show: > show ip dhcp relay [statistics]
show ip dhcp relay [statistics]

Clear: # clear ip dhcp relay statistics

3.9.19.9 (config)# ip dhcp relay information option

Syntax: (config)# ip dhcp relay information option

Explanation: Enable DHCP Relay option 82 function. Please note that “Relay Mode” must be enabled before this function is able to take effect.

Example: Enable DHCP Relay option 82 function

```
# config t
(config)# ip dhcp relay information option
```

Negation: (config)# no ip dhcp relay information option

3.9.19.10 (config)# ip dhcp relay information policy {drop | keep | replace}

Syntax: (config)# ip dhcp relay information policy { drop | keep | replace }

Explanation: Specify DHCP Relay information reforwarding policy action.

Parameters:

{ drop | keep | replace }: Specify one of the relay information policy options.

drop: Drop the packet when it receives a DHCP message that already contains relay information.

keep: Keep the client’s DHCP information.

replace: Replace (rewrite) the DHCP client packet information with the switch's relay information. This is the default setting.

Example: Keep the client's DHCP information.

```
# config t
(config)# ip dhcp relay information policy keep
```

Negation: (config)# no ip dhcp relay information policy

3.9.19.11 (config)# ip dhcp server

Syntax: (config)# ip dhcp server

Explanation: Enable DHCP server function globally.

Example: Enable DHCP server function.

```
# config t
(config)# ip dhcp server
```

Negation: (config)# no ip dhcp server

Show: > show ip dhcp server
show ip dhcp server

3.9.19.12 (config)# ip dhcp snooping

Syntax: (config)# ip dhcp snooping

Explanation: Enable DHCP snooping function globally. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Example: Enable DHCP snooping function.

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

Negation: (config)# no ip dhcp snooping

Show: > show ip dhcp snooping [interface (<port_type> [<in_port_list>])]
show ip dhcp snooping [interface (<port_type> [<in_port_list>])]
show ip dhcp snooping table

Clear: # clear ip dhcp snooping statistics [interface (<port_type> [<in_port_list>])]

3.9.19.13 (config)# ip dns proxy

Syntax: (config)# ip dns proxy

Explanation: Enable DNS (Domain Name System) proxy function.

```
# config t
(config)# ip dns proxy
```

Negation: (config)# no ip dns proxy

3.9.19.14 (config)# ip helper-address

Syntax: (config)# ip helper-address <v_ipv4_ucast>

Explanation: Configure DHCP Relay server IPv4 address.

Parameters:

<v_ipv4_ucast>: Specify DHCP Relay server IPv4 address that is used by the switch's DHCP relay agent

Negation: (config)# no ip helper-address

3.9.19.15 (config)# ip http secure-certificate

Syntax: (config)# ip http secure-certificate { upload <url_file> [pass-phrase <pass_phrase>] | delete | generate }

Explanation: Upload or generate HTTPs certificate.

Parameters:

{ upload <url_file> [pass-phrase <pass_phrase>] | delete | generate }: Upload a certificate via URL link and protected by a passphrase if necessary. You can also delete or generate a certificate by issuing "delete" or "generate" command.

Show: # show ip http server secure status

3.9.19.16 (config)# ip http secure-server

Syntax: (config)# ip http secure-server

Explanation: Enable the HTTPS operation mode. When the current connection is HTTPS and HTTPS mode operation is disabled, web browser will automatically redirect to an HTTP connection.

Example: Enable the HTTPS operation mode.

```
# config t
(config)# ip http secure-server
```

Negation: (config)# no ip http secure-server

Show: # show ip http server secure status

3.9.19.17 (config)# ip http secure-redirect

Syntax: (config)# ip http secure-redirect

Explanation: Enable the HTTPS redirect mode operation. It applies only if HTTPS mode is "Enabled". Automatically redirects HTTP of web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled.

Example: Enable HTTPs automatic redirect mode.

```
# config t
(config)# ip http secure-redirect
```

Negation: (config)# no ip http secure-redirect

Show: # show ip http server secure status

3.9.19.18 (config)# ip igmp host-proxy

Syntax: (config)# ip igmp host-proxy [leave-proxy]

Explanation: When enabled, the switch suppresses leave messages unless received from the last member port in the group. IGMP leave proxy suppresses all unnecessary IGMP leave messages so that a non-querier switch forwards an IGMP leave packet only when the last dynamic member port leaves a multicast group.

Parameters:

[leave-proxy]: The parameter is optional. Enable leave-proxy function.

Negation: (config)# no ip igmp host-proxy [leave-proxy]

Show: # show ip igmp snooping detail

3.9.19.19 (config)# ip igmp snooping

Syntax: (config)# ip igmp snooping

Explanation: Globally enable IGMP Snooping feature. When enabled, this device will monitor network traffic and determine which hosts will receive multicast traffic. The switch can passively monitor or snoop on IGMP Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

Negation: (config)# no ip igmp snooping

Show: # show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

Clear: # clear ip igmp snooping [vlan <v_vlan_list>] statistics

3.9.19.20 (config)# ip igmp snooping vlan

Syntax: (config)# ip igmp snooping vlan <v_vlan_list>

Explanation: Enable IGMP function for specific VLANs.

Parameters:

<v_vlan_list>: Specify valid IGMP VLANs.

Negation: (config)# no ip igmp snooping vlan [<v_vlan_list>]

Show: # show ip igmp snooping

Clear: # clear ip igmp snooping [vlan <v_vlan_list>] statistics

3.9.19.21 (config)# ip igmp ssm-range

Syntax: (config)# ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>

Explanation: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Parameters:

<v_ipv4_mcast>: Specify valid IPv4 multicast address.

<ipv4_prefix_length>: Specify the prefix length ranging from 4 to 32.

Negation: (config)# no ip igmp ssm-range

3.9.19.22 (config)# ip igmp unknown-flooding

Syntax: (config)# ip igmp unknown-flooding

Explanation: Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

Negation: (config)# no ip igmp unknown-flooding

3.9.19.23 (config)# ip name-server

Syntax: (config)# ip name-server [<order>] { <v_ipv4_ucast> | { <v_ipv6_ucast> [interface vlan <v_vlan_id_static>] } | dhcp [ipv4 | ipv6] [interface vlan <v_vlan_id_dhcp>] }

Explanation: Set up DNS IP address manually or obtain DNS IP address via specific VLAN DHCP server.

Parameters:

[<order: 0-3>]: Indicates the preference of DNS server. The default value is 0.

{ <v_ipv4_ucast> | { <v_ipv6_ucast> [interface vlan <v_vlan_id_static>] } | dhcp [ipv4 | ipv6] [interface vlan <v_vlan_id_dhcp>] }: Specify one of the options.

<v_ipv4_ucast>: Manually specify unicast IPv4 name server address.

<v_ipv6_ucast> [interface vlan <v_vlan_id_static>]: Manually specify unicast IPv6 name server address.

dhcp [ipv4 | ipv6] [interface vlan <v_vlan_id_dhcp>]: Configure DNS IP address via specific VLAN DHCP server.

Negation: (config)# no ip name-server [<order: 0~3>]

Show: > show ip name-server
show ip name-server

3.9.19.24 (config)# ip route

Syntax: (config)# ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>

Explanation: Configure a static IP route.

Parameters:

<v_ipv4_addr>: Specify IPv4 address. The IP route is the destination IP network or host address of this route. Valid format is dotted decimal notation.

<v_ipv4_netmask>: The route mask is a destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Only a default route will have a mask length of 0 (as it will match anything).

<v_ipv4_gw>: This is the IP address of the gateway. Valid format is dotted decimal notation. Gateway and Network must be of the same type.

Example: Add a new ip route with the following settings.

```
# config t
(config)# ip route 192.168.1.240 255.255.255.0 192.168.1.254
```

Negation: (config)# no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>

Show: > show ip route
show ip route

3.9.19.25 (config)# ip routing

Syntax: (config)# ip routing

Explanation: Enable IPv4 and IPv6 routing.

Example: Enable IPv4 and IPv6 routing.

```
# config t
(config)# ip routing
```

Negation: (config)# no ip routing

Show: > show ip route
 > show ipv6 route [interface vlan <vlan_list>]
 # show ip route
 # show ipv6 route [interface vlan<vlan_list>]

```
# show ip route
127.0.0.1/32 via 127.0.0.1 <UP HOST>
224.0.0.0/4 via 127.0.0.1 <UP>
# show ipv6 route interface vlan 1
::1/128 via ::1 <UP HOST>
```

3.9.19.26 (config)# ip source binding interface

Syntax: (config)# ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var>

Explanation: Create a static entry.

Parameters:

<port_type> <in_port_type_id>: Specify a port type and port number to which a static entry is bound.

<vlan_var>: Specify VLAN ID that has been configured.

<ipv4_var>: Specify a valid IPv4 address.

<mac_var>: Specify the MAC addresss for the entered IP address.

Negation: (config)# no ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var>

Show: # show ip source binding [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]

3.9.19.27 (config)# ip ssh

Syntax: (config)# ip ssh

Explanation: Enable SSH mode.

Example: Enable SSH mode.

```
# config t
(config)# ip ssh
```

Negation: (config)# no ip ssh

Show: # show ip ssh

NOTE: SSH is preferred to Telnet, unless the management network is trusted. Telnet passes authentication credentials in plain text, making those credentials susceptible to packet capture and analysis. SSH provides a secure authentication method. The SSH in this device uses version 2 of SSH protocol.

3.9.19.28 (config)# ip verify source

Syntax: (config)# ip verify source

Explanation: Enable IP source guard function.

Negation: (config)# no ip verify source

Show: > show ip verify source [interface (<port_type> [<in_port_type_list>])]
show ip verify source [interface (<port_type> [<in_port_type_list>])]

3.9.19.29 (config)# ip verify source translate

Syntax: (config)# ip verify source translate

Explanation: Translate Dynamic entries to Static ones.

3.9.19.30 (config-if)# ip arp inspection check-vlan

Syntax: (config-if)# ip arp inspection check-vlan

Explanation: Enable check vlan function.

Negation: (config-if)# no ip arp inspection check-vlan

3.9.19.31 (config-if)# ip arp inspection logging

Syntax: (config-if)# ip arp inspection logging { deny | permit | all }

Explanation: Enable log function on a specific interface.

Parameters:

{ deny | permit | all }: Specify one of the log types.

deny: Log denied entries.

permit: Log permitted entries.

all: Log all entries.

Negation: (config-if)# no ip arp inspection logging

3.9.19.32 (config-if)# ip arp inspection trust

Syntax: (config-if)# ip arp inspection trust

Explanation: Enable trust state on the selected interfaces.

Negation: (config-if)# no ip arp inspection trust

3.9.19.33 (config-if)# ip dhcp snooping trust

Syntax: (config-if)# ip dhcp snooping trust

Explanation: Set this interface to DHCP Snooping trusted port.

Negation: (config-if)# no ip dhcp snooping trust

Show: > show ip dhcp snooping [interface (<port_type> [<in_port_list>])]
show ip dhcp snooping [interface (<port_type> [<in_port_list>])]

3.9.19.34 (config-if)# ip igmp snooping filter

Syntax: (config-if)# ip igmp snooping filter <profile_name>

Explanation: Use this command to filter specific multicast traffic on a per port basis.

Parameters:

<profile_name>: Specify the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, IGMP join reports received on a port are dropped.

Negation: (config-if)# no ip igmp snooping filter

Show: > show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.19.35 (config-if)# ip igmp snooping immediate-leave

Syntax: (config-if)# ip igmp snooping immediate-leave

Explanation: Enable fast leave function on a specific port. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

Negation: (config-if)# no ip igmp snooping immediate-leave

Show: > show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.19.36 (config-if)# ip igmp snooping max-groups

Syntax: (config-if)# ip igmp snooping max-groups <throttling>

Explanation: Specify the maximum number of multicast groups that a port can join at the same time.

Parameters:

<throttling>: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. The allowed range can be specified is 1 to 10.

Negation: (config-if)# no ip igmp snooping max-groups

Show: > show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.19.37 (config-if)# ip igmp snooping mrouter

Syntax: (config-if)# ip igmp snooping mrouter

Explanation: Set this interface to Router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Negation: (config-if)# no ip igmp snooping mrouter

Show: > show ip igmp snooping mrouter [detail]
show ip igmp snooping mrouter [detail]

3.9.19.38 (config-if)# ip verify source

Syntax: (config-if)# ip verify source

Explanation: Enable IP Source Guard on this interface

Negation: (config-if)# no ip verify source

Show: > show ip verify source [interface (<port_type> [<in_port_type_list>])]
show ip verify source [interface (<port_type> [<in_port_type_list>])]

3.9.19.39 (config-if)# ip verify source limit

Syntax: (config-if)# ip verify source limit <0-2>

Explanation: Specify the maximum number of dynamic clients that can be learned on a port. The available options are 0, 1, 2. If the port mode is enabled and the maximum number of dynamic clients is equal 0, the switch will only forward IP packets that are matched in static entries for a given port.

Parameters:

<0-2>: Specify the maximum number of dynamic clients that can be learned on a port.

Negation: (config-if)# no ip verify source limit

Show: > show ip verify source [interface (<port_type> [<in_port_type_list>])]
show ip verify source [interface (<port_type> [<in_port_type_list>])]

3.9.19.40 (config-if-vlan)# ip address

Syntax: (config-if-vlan)# ip address { { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }

Explanation: Configure IPv4 address for this VLAN interface.

Parameters:

<address> <netmask>: Specify IPv4 address and subnet mask.

dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]]: Use DHCP server to automatically assign IP address.

fallback <fallback_address> <fallback_netmask>: specify Fallback IP address and subnet mask.

timeout <fallback_timeout>: Specify Fallback timeout value.

Negation: (config-if-vlan)# no ip address

Show: > show ip interface brief
show ip interface brief

3.9.19.41 (config-if-vlan)# ip dhcp server

Syntax: (config-if-vlan)# ip dhcp server

Explanation: Enable DHCP server on this specific VLAN.

Negation: (config-if-vlan)# no ip dhcp server

Show: > show ip dhcp server
show ip dhcp server

3.9.19.42 (config-if-vlan)# ip igmp snooping

Syntax: (config-if-vlan)# ip igmp snooping

Explanation: Enable IGMP Snooping on this specific VLAN.

Negation: (config-if-vlan)# no ip igmp snooping

Show: > show ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]
show ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

3.9.19.43 (config-if-vlan)# ip igmp snooping compatibility

Syntax: (config-if-vlan)# ip igmp snooping compatibility { auto | v1 | v2 | v3 }

Explanation: Configure IGMP Snooping version used for this specific VLAN.

Parameters:

{ auto | v1 | v2 | v3 }: Specify one of the IGMP Snooping options.

auto: Compatible with Version 1, Version 2, and Version 3.

v1: Compatible with IGMP version 1.

v2: Compatible with IGMP version 2.

v3: Compatible with IGMP version 3.

Negation: (config-if-vlan)# no ip igmp snooping compatibility

3.9.19.44 (config-if-vlan)# ip igmp snooping last-member-query-interval

Syntax: (config-if-vlan)# ip igmp snooping last-member-query-interval <ipmc_lmqi>

Explanation: LMQI stands for Last Member Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The allowed range is 0~31744 tenths of a second.

Parameters:

<ipmc_lmqi: 0-31744>: Specify LMQI (Last Member Query Interval) value.

Negation: (config-if-vlan)# no ip igmp snooping last-member-query-interval

3.9.19.45 (config-if-vlan)# ip igmp snooping priority

Syntax: (config-if-vlan)# ip igmp snooping priority <cos_priority>

Explanation: Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0 -7.

Parameters:

<cos_priority: 0-7>: Specify COS for this specific VLAN. The valid range is 0 to 7.

Negation: (config-if-vlan)# no ip igmp snooping priority

3.9.19.46 (config-if-vlan)# ip igmp snooping querier

Syntax: (config-if-vlan)# ip igmp snooping querier { election | address <v_ipv4_ucast> }

Parameters:

{ election | address <v_ipv4_ucast> }: Elect the IGMP Snooping querier or use the specified IPv4 unicast address as a querier.

Explanation: Elect or specify IGMP Snooping querier IP address.

Negation: (config-if-vlan)# no ip igmp snooping querier { election | address }

3.9.19.47 (config-if-vlan)# ip igmp snooping query-interval

Syntax: (config-if-vlan)# ip igmp snooping query-interval <ipmc_qi>

Explanation: Specify IPMC Query interval value.

Parameters:

<ipmc_qi: 1-31744>: Specify IPMC Query interval value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ip igmp snooping query-interval

3.9.19.48 (config-if-vlan)# ip igmp snooping query-max-response-time

Syntax: (config-if-vlan)# ip igmp snooping query-max-response-time <ipmc_qri>

Explanation: Specify IPMC Query Response time value.

Parameters:

<ipmc_qri>: Specify IPMC Query Response time value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ip igmp snooping query-max-response-time

3.9.19.49 (config-if-vlan)# ip igmp snooping robustness-variable

Syntax: (config-if-vlan)# ip igmp snooping robustness-variable <ipmc_rv>

Explanation: The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

Parameters:

<ipmc_rv: 1-255>: Specify IPMC Robustness Variable value. The valid value is 1~255.

Negation: (config-if-vlan)# no ip igmp snooping robustness-variable

3.9.19.50 (config-if-vlan)# ip igmp snooping unsolicited-report-interval

Syntax: (config-if-vlan)# ip igmp snooping unsolicited-report-interval <ipmc_uri>

Explanation: The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. The allowed range for URI is 0 -31744 seconds.

Parameters:

<ipmc_uri: 0-31744>: Specify Unsolicited Report Interval value. The valid value is 0~31744.

Negation: (config-if-vlan)# no ip igmp snooping unsolicited-report-interval

3.9.19.51 (config-if-vlan)# ipv6 address

Syntax: (config-if-vlan)# ipv6 address <subnet>

Explanation: Configure IPv6 address for this VLAN interface.

Parameters:

<subnet>: Specify IPv6 address in X:X:X:X/<0-128> format.

Negation: (config-if-vlan)# no ipv6 address [<ipv6_subnet>]

Show: > show ip interface brief
 > show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]
 # show ip interface brief
 # show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]

3.9.19.52 (config-if-vlan)# ipv6 address {autoconfig | dhcp | rapid-commit}

Syntax: (config-if-vlan)# ipv6 address {autoconfig | dhcp | rapid-commit}

Explanation: Configure how IPv6 address is obtained .

Parameters:

{autoconfig | dhcp | rapid-commit}: Manual configure IPv6 address or use DHCP server to obtain IPv6 address. Or configure DHCPv6 to support rapid commit option (DHCPv6 option 14). When rapid commit is enabled, the server recognizes the Rapid Commit option in Solicit messages sent from the DHCPv6 client. The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-message exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, and is beneficial in environments in which networks are under a heavy load.

Negation: (config-if-vlan)# no ipv6 address {autoconfig | dhcp | rapid-commit}

Show: > show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]
 # show ipv6 dhcp-client [interface vlan <v_vlan_list>]
 # show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]

3.9.19.53 (config-if-vlan)# ipv6 mld snooping

Syntax: (config-if-vlan)# ipv6 mld snooping

Explanation: Enable MLD (Multicast Listener Discovery) Snooping on this specific VLAN.

Negation: (config-if-vlan)# no ipv6 mld snooping

Show: > show ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]
 # show ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

3.9.19.54 (config-if-vlan)# ipv6 mld snooping compatibility

Syntax: (config-if-vlan)# ipv6 mld snooping compatibility { auto | v1 | v2 }

Explanation: Configure MLD Snooping version used for this specific VLAN.

Parameters:

{ auto | v1 | v2 | v3 }: Specify one of the MLD Snooping options.

auto: Compatible with Version 1, Version 2.

v1: Compatible with MLD version 1.

v2: Compatible with MLD version 2.

Negation: (config-if-vlan)# no ipv6 mld snooping compatibility

3.9.19.55 (config-if-vlan)# ipv6 mld snooping last-member-query-interval

Syntax: (config-if-vlan)# ipv6 mld snooping last-member-query-interval <ipmc_lmqi>

Explanation: LMQI stands for Last Member Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The allowed range is 0~31744 tenths of a second.

Parameters:

<ipmc_lmqi: 0-31744>: Specify LMQI (Last Member Query Interval) value.

Negation: (config-if-vlan)# no ipv6 mld snooping last-member-query-interval

3.9.19.56 (config-if-vlan)# ipv6 mld snooping priority <cos_priority>

Syntax: (config-if-vlan)# ipv6 mld snooping priority <cos_priority>

Explanation: Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0 -7.

Parameters:

<cos_priority: 0-7>: Specify COS for this specific VLAN. The valid range is 0 to 7.

Negation: (config-if-vlan)# no ipv6 mld snooping priority

3.9.19.57 (config-if-vlan)# ipv6 mld snooping querier election

Syntax: (config-if-vlan)# ipv6 mld snooping querier election

Explanation: Enable MLD Snooping querier election function.

Negation: (config-if-vlan)# no ipv6 mld snooping querier election

3.9.19.58 (config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>

Syntax: (config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>

Explanation: Specify MLD Query interval value.

Parameters:

<ipmc_qi: 1-31744>: Specify IPMC Query interval value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ipv6 mld snooping query-interval

3.9.19.59 (config-if-vlan)# ipv6 mld snooping query-max-response-time <ipmc_qri>

Syntax: (config-if-vlan)# ipv6 mld snooping query-max-response-time <ipmc_qri>

Explanation: Specify MLD Query Response time value.

Parameters:

<ipmc_qri>: Specify MLD Query Response time value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ipv6 mld snooping query-max-response-time

3.9.19.60 (config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>

Syntax: (config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>

Explanation: The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

Parameters:

<ipmc_rv: 1-255>: Specify IPMC Robustness Variable value. The valid value is 1~255.

Negation: (config-if-vlan)# no ipv6 mld snooping robustness-variable

3.9.19.61 (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <ipmc_uri>

Syntax: (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <ipmc_uri>

Explanation: The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. The allowed range for URI is 0 -31744 seconds.

Parameters:

<ipmc_uri: 0-31744>: Specify Unsolicited Report Interval value. The valid value is 0~31744.

Negation: (config-if-vlan)# no ipv6 mld snooping unsolicited-report-interval

3.9.20 (config)# ipmc

3.9.20.1 (config)# ipmc profile

Syntax: (config)# ipmc profile

Explanation: Enable IPMC (IP multicast) profile globally.

Negation: (config)# no ipmc profile

Show: # show ipmc profile

3.9.20.2 (config)# ipmc profile <profile_name>

Syntax: (config)# ipmc profile <profile_name>

Parameters:

<profile_name: word16>: Specify the desired profile name in 16 characters. When entered is pressed, the command will change to (config-ipmc-profile)#.

Explanation: Set up an IPMC profile.

Example: Create an IPMC profile named "goldpass".

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)#
```

Negation: (config)# no ipmc profile <profile_name>

Show: # show ipmc profile [<profile_name>] [detail]

3.9.20.3 (config)# ipmc range

Syntax: (config)# ipmc range <entry_name> { <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }

Explanation: Specify the multicast IP range. The available IP range is from 224.0.0.0~239.255.255.255.

Parameters:

<entry_name>: The name used in specifying the address range.

{ <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }: Specify the multicast IP range. The available IP range is from 224.0.0.0~239.255.255.255.

Negation: (config)# no ipmc range <entry_name>

Show: # show ipmc profile [<profile_name>] [detail]

3.9.20.4 (config-ipmc-profile)# default range

Syntax: (config-ipmc-profile)# default range <entry_name>

Parameters:

<entry_name: word16>: Specify an entry name in 16 characters for this IPMC profile.

Explanation: To set default IPMC Profile Rule for a specific IPMC Profile.

Example: To default IPMC Profile Rule (Entry 1) for specific IPMC Profile.

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)# default range 1
```

Negation: (config-ipmc-profile)# no range <entry_name>

Show: # show ipmc profile

#show ipmc profile [<profile_name>] [detail]

3.9.20.5 (config-ipmc-profile)# description

Syntax: (config-ipmc-profile)# description <profile_desc>

Parameters:

<profile_desc: line 64>: Additional description for the designated profile in 64 characters.

Explanation: Specify descriptive information for the designated profile.

Example: Provide descriptive information for IPMC profile goldpass.

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)# description 1stclasscustomer
```

Negation: (config-ipmc-profile)# no description

Show: # show ipmc profile
#show ipmc profile [<profile_name>] [detail]

3.9.20.6 (config-ipmc-profile)# range

Syntax: (config-ipmc-profile)# range <entry_name> { permit | deny } [log] [next <next_entry>]

Parameters:

<entry_name>: Specify an entry name.

{ permit | deny }: Specify the action taken upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Permit: Group address matches the range specified in the rule will be learned.

Deny: Group address matches the range specified in the rule will be dropped.

[log]: Log when matching

[next <next_entry>]: Specify next entry used in profile

Explanation: To set action of an entry for a specific IPMC profile.

Negation: (config-ipmc-profile)# no range <entry_name>

Show: # show ipmc profile
#show ipmc profile [<profile_name>] [detail]

3.9.21 (config)# ipv6 mld host-proxy

3.9.21.1 (config)# ipv6 mld host-proxy

Syntax: (config)# ipv6 mld host-proxy

Explanation: Enable IPv6 MLD proxy. When MLD proxy is enabled, the switch exchanges MLD messages with the router on its upstream interface, and performs the host portion of the MLD task on the upstream interface as follows:

- When queried, it sends multicast listener reports to the group.
- When a host joins a multicast group to which no other host belongs, it sends unsolicited multicast listener reports to that group.
- When the last host in a particular multicast group leaves, it sends an unsolicited multicast listener done report to the all-routers address (FF02::2) for MLDv1.

Example: Enable IPv6 MLD Proxy.

```
# config t
(config)# ipv6 mld host-proxy
(config)#
```

Negation: (config)# no ipv6 mld host-proxy

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.21.2 (config)# ipv6 mld host-proxy leave-proxy

Syntax: (config)# ipv6 mld host-proxy leave-proxy

Explanation: Enable IPv6 MLD leave proxy. To prevent multicast router from becoming overloaded with leave messages, MLD snooping suppresses leave messages unless received from the last member port in the group. When the switch acts as the querier, the leave proxy feature will not function.

Example: Enable IPv6 MLD leave proxy.

```
# config t
(config)# ipv6 mld host-proxy leave-proxy
(config)#
```

Negation: (config)# no ipv6 mld host-proxy leave-proxy

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.21.3 (config)# ipv6 mld snooping

Syntax: (config)# ipv6 mld snooping

Explanation: Enable MLD Snooping feature globally. When enabled, this device will monitor network traffic and determine which hosts would like to receive multicast traffic. The switch can passively monitor or snoop on MLD Listener Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

Example: Enable IPv6 MLD snooping.

```
# config t
(config)# ipv6 mld snooping
(config)#
```

Negation: (config)# no ipv6 mld snooping

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.21.4 (config)# ipv6 mld snooping vlan

Syntax: (config)# ipv6 mld snooping vlan <v_vlan_list>

Parameters:

<v_vlan_list>: Specify VLAN ID for MLD.

Negation: (config)# no ipv6 mld snooping vlan [<v_vlan_list>]

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
> show ipv6 mld snooping mrouter [detail]
show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ipv6 mld snooping mrouter [detail]

Clear: # clear ipv6 mld snooping [vlan <v_vlan_list>] statistics

3.9.21.5 (config)# ipv6 mld ssm-range

Syntax: (config)# ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>

Parameters:

<v_ipv6_mcast>: Specify valid IPv6 mluticast address.

<ipv6_prefix_length>: Specify prefix length range from 8 to 128.

Explanation: Specify SSM (Source-Specific Multicast) Range. This setting allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Example: Configure MLD SSM with the ff3e::7728/128 settings.

```
# config t
(config)# ipv6 mld ssm-range ff3e::7728 128
```

Negation: (config)# no ipv6 mld ssm-range

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.21.6 (config)# ipv6 mld unknown-flooding

Syntax: (config)# ipv6 mld unknown-flooding

Explanation: Enable forwarding mode for unregistered (not-joined) IP multicast traffic.

Example: To flood unregistered IPv6 multicast traffic

```
# config t
(config)# ipv6 mld unknown-flooding
```

Negation: (config)# no ipv6 mld unknown-flooding

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
> show ipv6 mld snooping mrouter [detail]
show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ipv6 mld snooping mrouter [detail]

3.9.21.7 (config)# ipv6 route

Syntax: (configure)# ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }

Parameters:

<v_ipv6_subnet>: Specify IPv6 route address.

{ <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }: Specify one of the options. This could be either IPv6 next hop unicast address or an interface.

Explanation: Configure a static IPv6 route.

Negation: (config)# no ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }

Show: # show ipv6 route [interface vlan <v_vlan_list>]

3.9.21.8 (config-if)# ipv6 mld snooping filter

Syntax: (config-if)# ipv6 mld snooping filter <profile_name>

Explanation: Use this command to filter specific multicast traffic on a per port basis.

Parameters:

<profile_name>: Specify the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, IGMP join reports received on a port are dropped.

Negation: (config-if)# no ipv6 mld snooping filter

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.21.9 (config-if)# ipv6 mld snooping immediate-leave

Syntax: (config-if)# ipv6 igmp snooping immediate-leave

Explanation: Enable fast leave function on a specific port. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

Negation: (config-if)# no ipv6 mld snooping immediate-leave

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.21.10 (config-if)# ipv6 mld snooping max-groups

Syntax: (config-if)# ip igmp snooping max-groups <throttling>

Explanation: Specify the maximum number of multicast groups that a port can join at the same time.

Parameters:

<throttling>: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. The allowed range can be specified is 1 to 10.

Negation: (config-if)# no ipv6 mld snooping max-groups

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.21.11 (config-if)# ipv6 mld snooping mrouter

Syntax: (config-if)# ipv6 mld snooping mrouter

Explanation: Set this interface to Router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Negation: (config-if)# no ipv6 mld snooping mrouter

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
> show ipv6 mld snooping mrouter [detail]

```
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping mrouter [ detail ]
```

3.9.22 (config)# lacp

3.9.22.1 (config)# lacp system-priority

Syntax: (configure)# lacp system-priority <v_1_to_65535>

Parameters:

<v_1_to_65535>: The priority of the port. The allowed value range is from 1 to 65535.

Explanation: Configure system priority for LACP function. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

Example: Set LACP system priority value to 100.

```
# config t
(config)# lacp system-priority 100
```

Negation: (config)# no lacp system-priority <v_1_to_65535>

Show: # show lacp { internal | statistics | system-id | neighbour }

3.9.22.2 (config-if)# lacp

Syntax: (config-if)# lacp

Explanation: Enable LACP on this interface.

Example: Enable LACP on port 1.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# lacp
(config-if)#
```

Negation: (config-if)# no lacp

Show: # show lacp { internal | statistics | system-id | neighbour }

Clear: # clear lacp statistics

3.9.22.3 (config-if)# lacp key

Syntax: (config-if)# lacp key { <v_1_to_65535> | auto }

Explanation: Configure a LACP key for this interface.

Parameters:

{ <v_1_to_65535> | auto }: Specify a LACP key for this interface. The “auto” setting sets the key as appropriate by the physical link speed. If you want a user-defined key value, enter a value between 1 and 65535. Ports in an aggregated link group must have the same LACP port Key. In order to allow a port to join an aggregated group, the port Key must be set to the same value.

Negation: (config-if)# no lacp key { <v_1_to_65535> | auto }

Show: # show lacp { internal | statistics | system-id | neighbour }

3.9.22.4 (config-if)# lacp port-priority <v_1_to_65535>

Syntax: (config-if)# lacp port-priority <v_1_to_65535>

Explanation: Configure a LACP key for this interface.

Parameters:

<v_1_to_65535>: Specify a LACP port priority for this interface. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

Negation: (config-if)# no lacp port-priority <v_1_to_65535>

Show: # show lacp { internal | statistics | system-id | neighbour }

3.9.22.5 (config-if)# lacp role { active | passive }

Syntax: (config-if)# lacp role { active | passive }

Explanation: Configure LACP role for this interface.

Parameters:

{ active | passive }: Specify either “Active” or “Passive” role depending on the device’s capability of negotiating and sending LACP control packets. Ports that are designated as “Active” are able to process and send LACP control frames. Hence, this allows LACP compliant devices to negotiate the aggregated link so that the group may be changed dynamically as required. In order to add or remove ports from the group, at least one of the participating devices must set to “Active” LACP ports.

Negation: (config-if)# no lacp role { active | passive }

Show: # show lacp { internal | statistics | system-id | neighbour }

3.9.22.6 (config-if)# lacp timeout { fast | slow }

Syntax: (config-if)# lacp timeout { fast | slow }

Explanation: Configure timeout mode.

Parameters:

{ fast | slow }: The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

Negation: (config-if)# no lacp timeout { fast | slow }

Show: # show lacp { internal | statistics | system-id | neighbour }

3.9.23 (config)# line

3.9.23.1 (config)# line

Syntax: (configure)# line { <0~16> | console 0 | vty <0~15> }

Explanation: Enter the specific line. When Enter is pressed, the command line changes to "(config-line)#".

Parameters:

{ <0~16> | console 0 | vty <0~15> }: Specify one of the options.

<0~16> : List of line numbers.

console 0: Console line connection.

vtty <0~15>: VTY lines are the Virtual Terminal lines of the device, used solely to control inbound Telnet connections. They are virtual, in the sense that they are a function of software - there is no hardware associated with them.

Example: Enter Console 0 mode.

```
# config t
(config)# line console 0
(config-line)#
```

Show: > show line [alive]
show line [alive]

3.9.23.2 (config-line)# do

Syntax: (config-line)# do <command>

Explanation: To run EXEC. commands.

Parameters:

<command>: Enter the EXEC. command

Example: Show aaa settings.

```
# config t
(config)# line console 0
(config-line)# do show aaa
console : local
telnet   : local
ssh      : local
http     : local
(config-line)#
```

3.9.23.3 (config-line)# editing

Syntax: (config-line)# editing

Explanation: Enable command line editing.

Negation: (config-line)# no editing

Show: > show line [alive]
show line [alive]

3.9.23.4 (config-line)# end

Syntax: (config-line)# end

Explanation: Return to EXEC. mode.

Example: Return to EXEC. mode.

```
# config t
(config)# line console 0
(config-line)# end
#
```

3.9.23.5 (config-line)# exec-banner

Syntax: (config-line)# exec-banner

Explanation: Enable the display of EXEC banner.

Example: Enable the display of EXEC banner.

```
# config t
(config)# line console 0
(config-line)# exec-banner
```

Negation: (config-line)# no exec-banner

Show: > show line [alive]
show line [alive]

3.9.23.6 (config-line)# exec-timeout

Syntax: (config-line)# exec-timeout <min> [<sec>]

Parameters:

<min>: Specify timeout in minutes. The allowed range is 0 to 1440. Specify "0" to disable timeout function (CLI session will never timeout.)

[<sec>]: Specify timeout in seconds. The allowed range is 0 to 3600.

Negation: (config-line)# no exec-timeout

Show: > show line [alive]
show line [alive]

3.9.23.7 (config-line)# exit

Syntax: (config-line)# exit

Explanation: Return to Config mode.

Example: Return to Config mode.

```
# config t
(config)# line console 0
(config-line)# exit
(config)#
```

3.9.23.8 (config-line)# help

Syntax: (config-line)# help

Explanation: Show the Help explanation.

Example: Show Help explanation.


```
# config t
(config)# line console 0
(config-line)# help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what Parameters match the input
   (e.g. 'show pr?'.)
```

3.9.23.9 (config-line)# history size

Syntax: (config-line)# history size <history_size>

Explanation: Control how many history commands are displayed.

Parameters:

<history_size>: The allowed range is 0 to 32. 0 means “disable”.

Example: Set history size to 10.

```
# config t
(config)# line console 0
(config-line)# history size 10
```

Negation: (config-line)# no history size

Show: > show line [alive]
show line [alive]

3.9.23.10 (config-line)# length

Syntax: (config-line)# length <length>

Explanation: Configure the number of lines displayed on the screen.

Parameters:

<length>: Specify the number of lines displayed on the screen. The allowed range is 3 to 512. Specify “0” for no pausing.

Example: Display 20 lines on the screen.

```
# config t
(config)# line console 0
(config-line)# length 20
(config-line)#
```

Negation: (config-line)# no length

Show: > show line [alive]
show line [alive]

3.9.23.11 (config-line)# location

Syntax: (config-line)# location <location>

Explanation: Configure the descriptive location of this device.

Parameters:

<location>: Location description for the terminal. The characters allowed are 32.

Example: Configure the location "cabinet5a".

```
# config t
(config)# line console 0
(config-line)# location cabinet5a
(config-line)#
```

Negation: (config-line)# no location

Show: > show line [alive]
show line [alive]

3.9.23.12 (config-line)# motd-banner

Syntax: (config-line)# motd-banner

Explanation: Enable the display of motd (message of the day) banner.

Example: Enable motd banner.

```
# config t
(config)# line console 0
(config-line)# motd-banner
(config-line)#
```

Negation: (config-line)# no motd-banner

Show: > show line [alive]
show line [alive]

3.9.23.13 (config-line)# privilege level

Syntax: (config-line)# privilege level <privileged_level>

Explanation: Configure the privilege level for the terminal line.

Parameters:

<privileged_level>: Privilege level for the terminal line. The allowed range is 0 to 15.

Example: Change the privilege level to 5 for vty 1.

```
# config t
(config)# line vty 1
(config-line)# privilege level 5
(config-line)#
```

Negation: (config-line)# no privilege level

Show: > show line [alive]
show line [alive]

3.9.23.14 (config-line)# width

Syntax: (config-line)# width <width>

Explanation: Configure the width of the terminal line.

Parameters:

<width>: Specify the width of the terminal line. The allowed range is 40 to 512. Specify "0" for unlimited width.

Example: Change of width of vty 1 to 60.

```
# config t
(config)# line vty 1
(config-line)# width 60
(config-line)#
```

Negation: (config-line)# no width

Show: > show line [alive]
show line [alive]

3.9.24 (config)# lldp

3.9.24.1 (config)# lldp holdtime

Syntax: (config)# lldp holdtime <val>

Explanation: This setting defines how long LLDP frames are considered valid and is used to compute the TTL. The

default is 4.

Parameters:

<val>: Specify the holdtime value. The allowed value is 2 to 10.

Example: Set the holdtime to 5.

```
# config t
(config)# lldp holdtime 5
```

Negation: (config)# no lldp holdtime

3.9.24.2 (config)# lldp reinit

Syntax: (config)# lldp reinit <val>

Explanation: Configure a delay between the shutdown frame and a new LLDP initialization.

Parameters:

<val>: Specify a value between 1 and 10 (seconds).

Example: Set the LLDP re-initiation value to 3.

```
# config t
(config)# lldp reinit 3
```

Negation: (config)# no lldp reinit

3.9.24.3 (config)# lldp timer

Syntax: (config)# lldp timer <val>

Explanation: Configure the interval between LLDP frames are sent to its neighbors for updated discovery information. The default is 30 seconds.

Parameters:

<val>: Specify a value between 5 and 32768 (seconds).

Example: Set the LLDP timer value to 35.

```
# config t
(config)# lldp timer 35
```

Negation: (config)# no lldp timer

3.9.24.4 (config)# lldp transmission-delay

Syntax: (config)# lldp transmission-delay <val>

Parameters:

<val>: Specify a value between 1 and 8192 (seconds).

Explanation: Configure a delay between the LLDP frames that contain changed configurations. Tx Delay cannot be larger than 1/4 of the Tx interval value.

Example: Set the LLDP transmission delay value to 2.

```
# config t
(config)# lldp transmission-delay 2
```

Negation: (config)# no lldp transmission-delay

3.9.24.5 (config)# lldp med datum

Syntax: (config)# lldp med datum { wgs84 | nad83-navd88 | nad83-mlw }

Explanation: The Map Datum is used for the coordinates given in above options.

Parameters:

{ wgs84 | nad83-navd88 | nad83-mlw }: Specify one of the options.

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Example: Set the map datum to wgs84.

```
# config t
(config)# lldp med datum wgs84
```

Negation: (config)# no lldp med datum

3.9.24.6 (config)# lldp med fast

Syntax: (config)# lldp med fast <v_1_to_10>

Explanation: Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPDU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind, LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. With Fast start repeat count it is possible to specify the number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including between Network Connectivity Devices, or to other types of links.

Parameters:

<v_1_to_10>: Specify a valid value between 1 and 10.

Example: Set the value to 5.

```
# config t
(config)# lldp med fast 5
```

Negation: (config)# no lldp med fast

3.9.24.7 (config)# lldp med location-tlv altitude

Syntax: (config)# lldp med location-tlv altitude { meters | floors } <v_word11>

Explanation: Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). “meters” means meters of Altitude defined by the vertical datum specified; while, “floors” means altitude in a form more relevant in buildings which have different floor-to-floor dimensions.

Parameters:

{ meters | floors }: Specify one of the options.

<v_word11>: Specify a value for the specified option.

Example: Set the altitude value to “floors 10”.

```
# config t
(config)# lldp med location-tlv altitude floors 10
```

Negation: (config)# no lldp med location-tlv altitude

3.9.24.8 (config)# lldp med location-tlv civic-addr

Syntax: (config)# lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } <v_string250>

Explanation: Configure civic address information.

Parameters:

{ country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }: Specify one of the options.

country: The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

state: National subdivisions (state, canton, region, province, prefecture).

county: County, parish, gun (Japan), district.

city: City, township, shi (Japan) - Example: Copenhagen.

district: City division, borough, city district, ward, chou (Japan).

block: Neighbourhood, block.

street: Street - Example: Poppelvej.

leading-street-direction: Example: N.

trailings-street-suffix: Example: SW.

street-suffix: Ave, Platz.

house-no: Specify house number.

house-no-suffix: Example: A, 1/2.

landmark: Landmark or vanity address - Example: Columbia University.

additional-info: Example: South Wing.

Name: Example: Flemming Jahn.

zip-code: Postal/zip code - Example: 2791.

building: Building (structure). Example: Low Library.

apartment: Unit (Apartment, suite). Example: Apt 42.

floor: Example: 4.

room-number: Room number - Example: 450F.

place-type: Example: Office.

postal-community-name: Example: Leonia.

p-o-box: Example: 12345.

additional code: Example: 1320300003.

Example: Set the country code to “UK”.

```
# config t
(config)# lldp med location-tlv civic-addr country UK
```

Negation: (config)# no lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }

3.9.24.9 (config)# lldp med location-tlv elin-addr

Syntax: (config)# lldp med location-tlv elin-addr <v_word25>

Explanation: Configure a value for Emergency Location Information.

Parameters:

<v_word25>: A value for Emergency Location Information (ELIN).

Example: Set the emergency location information to “911”.

```
# config t
(config)# lldp med location-tlv elin-addr 911
```

Negation: (config)# no lldp med location-tlv elin-addr

3.9.24.10 (config)# lldp med location-tlv latitude

Syntax: (config)# lldp med location-tlv latitude { north | south } <v_word8>

Explanation: Configure a value for latitude. Latitude value should be between 0 and 90.

Parameters:

{ north | south } : Specify one of the options, either north or south.

<v_word8>: Specify latitude value for the selected option.

Example: Set the north latitude to 5.

```
# config t
(config)# lldp med location-tlv latitude north 5
```


Negation: (config)# no lldp med location-tlv latitude

3.9.24.11 (config)# lldp med location-tlv longitude

Syntax: (config)# lldp med location-tlv longitude { west | east } <v_word9>

Explanation: Configure a value for longitude. Longitude value should be between 0 and 180.

Parameters:

{ west | east }: Specify one of the options, either west or east.

<v_word9>: Specify longitude value for the selected option.

Example: Set the west longitude to 90.

```
# config t
(config)# lldp med location-tlv longitude west 90
```

Negation: (config)# no lldp med location-tlv longitude

3.9.24.12 (config)# lldp med media-vlan-policy

Syntax: (config)# lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { tagged <v_vlan_id> | untagged } [l2-priority <v_0_to_7>] [dscp <v_0_to_63>]

Explanation: Configure a LLDP MED policy ID for a service.

Parameters:

<policy_index>: Specify a policy ID. The valid range is from 0 to 31.

{ voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling }: Specify one of the services for this policy ID.

{ tagged <v_vlan_id> | untagged }: Specify whether this service is tagged or untagged. When “tagged” is specified, a VLAN ID should be provided.

[l2-priority <v_0_to_7>]: Specify a value for L2 priority. The valid value is from 0 to 7.

[dscp <v_0_to_63>]: Specify a value for DSCP. The valid value is from 0 to 63.

Example: Create a policy ID 1 for tagged Voice VLAN.

```
# config t
(config)# lldp med media-vlan-policy 1 voice tagged 100 l2-priority 7 DSCP 63
```

Negation: (config)# no lldp med media-vlan-policy <policies_list>

Show: > show lldp med media-vlan-policy [<v_0_to_31>]

```
# show lldp med media-vlan-policy [ <v_0_to_31> ]
```

3.9.24.13 (config-if)# lldp cdp-aware

Syntax: (config-if)# lldp cdp-aware

Explanation: Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table).

Example: Set interface 1 to CDP aware.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# lldp cdp-aware
```

Negation: (config-if)# no lldp cdp-aware

Show: > show lldp neighbors [interface (<port_type> [<v_port_type_list>])]
show lldp neighbors [interface (<port_type> [<v_port_type_list>])]

3.9.24.14 (config-if)# lldp med media-vlan policy-list

Syntax: (config-if)# lldp med media-vlan policy-list <v_range_list>

Explanation: To apply MED Media-VLAN policy of LLDP on this interface.

Parameters:

<v_range_list>: Assign a policy to this interface.

Negation: (config-if)# no lldp med media-vlan policy-list <v_range_list>

Show: > show lldp med media-vlan-policy [<v_0_to_31>]
show lldp med media-vlan-policy [<v_0_to_31>]

3.9.24.15 (config-if)# lldp med transmit-tlv

Syntax: (config-if)# lldp med transmit-tlv [capabilities] [location] [network-policy]

Explanation: To configure LLDP-MED TLV Type for specific interface.

Parameters:

[capabilities]: Enable transmission of the optional capabilities TLV.

[location]: Enable transmission of the optional location TLV.

[network-policy]: Enable transmission of the optional network policy TLV.

Negation: (config-if)# no lldp med transmit-tlv [capabilities] [location] [network-policy]

Show: > show lldp med media-vlan-policy [<v_0_to_31>]
show lldp med media-vlan-policy [<v_0_to_31>]

3.9.24.16 (config-if)# lldp receive

Syntax: (config-if)# lldp receive

Explanation: The switch will analyze LLDP information received from neighbours.

Negation: (config-if)# no lldp receive

Show: > show lldp statistics [interface (<port_type> [<v_port_type_list>])]
show lldp statistics [interface (<port_type> [<v_port_type_list>])]

3.9.24.17 (config-if)# lldp tlv-select

Syntax: (config-if)# lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

Explanation: To configure LLDP-MED TLV attributes for specific interface.

Parameters:

{ management-address | port-description | system-capabilities | system-description | system-name }: Specify a LLDP TLV attribute. LLDP uses several attributes to discover neighbour devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent from this device.

Negation: (config-if)# no lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

Show: > show lldp neighbors [interface (<port_type> [<v_port_type_list>])]
show lldp neighbors [interface (<port_type> [<v_port_type_list>])]

3.9.24.18 (config-if)# lldp transmit

Syntax: (config-if)# lldp transmit

Explanation: To configure LLDP Tx only mode for specific interface

Negation: (config-if)# no lldp transmit

Show: # show lldp statistics [interface (<port_type> [<v_port_type_list>])]

3.9.25 (config)# logging

3.9.25.1 (config)# logging on

Syntax: (config)# logging on

Explanation: This sets the server mode operation. When the mode of operation is enabled (on), the syslog message will send out to syslog server (at the server address). The syslog protocol is based on UDP communication and received on UDP port 514. Syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out, even if the syslog server does not exist. When the mode of operation is disabled, no syslog packets are sent out.

Example: Enable log server operation.

```
# config t
(config)# logging on
```

Negation: (config)# no logging on

Show: # show logging

Clear: # clear logging [info] [warning] [error] [switch <switch_list>]

3.9.25.2 (config)# logging host

Syntax: (config)# logging host { <v_ipv4_ucast> | <v_word45> }

Parameters:

{ <hostname> | <ipv4_ucast> }: Specify one of the options. The hostname is the domain name of the log server; while the latter is IPv4 address of the log server.

Explanation: Configure log server address.

Example: Use IPv4 address to configure log server.

```
# config t
(config)# logging host 192.168.1.253
```

Negation: (config)# no logging host

Show: # show logging
show logging <logging_id: 1-4294967295>
show logging [info] [warning] [error]

3.9.25.3 (config)# logging level

Syntax: (config)# logging level { info | warning | error }

Explanation: Configure what kind of messages will send to syslog server.

Parameters:

{ info | warning | error }: Specify one of the log message options.

Info: Send information, warnings and errors.

Warning: Send warnings and errors.

Error: Send errors only.

Example: Send error messages to log server.

```
# config t
(config)# logging level error
```

Show: # show logging
show logging <logging_id: 1-4294967295>
show logging [info] [warning] [error]

3.9.26 (config)# loop-protect

3.9.26.1 (config)# loop-protect

Syntax: (config)# loop-protect

Explanation: Enable loop protection function.

Example: Enable loop protection function.

```
# config t
(config)# loop-protect
```

Negation: (config)# no loop-protect

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.9.26.2 (config)# loop-protect shutdown-time

Syntax: (config)# loop-protect shutdown-time <t>

Explanation: Configure the period for which a port will be kept disabled.

Parameters:

<t: 0-604800>: Specify a shutdown time value. The valid values are from 0 to 604800 seconds. 0 means that a port is kept disabled until next device restart.

Example: Set the shutdown time value to 180 seconds.

```
# config t
(config)# loop-protect shutdown-time 180
```

Negation: (config)# no loop-protect shutdown-time

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.9.26.3 (config)# loop-protect transmit-time

Syntax: (config)# loop-protect transmit-time <t>

Explanation: Configure the interval between each loop protection PDU sent on each port.

Parameters:

<t: 1-10>: Specify a transmit time value. The valid values are from 1 to 10 seconds.

Example: Set the transmit time value to 5 seconds.

```
# config t
(config)# loop-protect transmit-time 5
```

Negation: (config)# no loop-protect transmit-time

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.9.26.4 (config-if)# loop-protect

Syntax: (config-if)# loop-protect

Explanation: Enable loop protection function on this interface.

Negation: (config-if)# no loop-protect

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.9.26.5 (config-if)# loop-protect action

Syntax: (config-if)# loop-protect action { [shutdown] [log] }

Explanation: Configure the action taken when loops are detected on a port.

Parameters:

{ [shutdown] [log] }: When a loop is detected on a port, the loop protection will immediately take appropriate actions. Actions will be taken include “Shutdown Port”, “Shutdown Port and Log” or “Log Only”.

Negation: (config-if)# no loop-protect action

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.9.26.6 (config-if)# loop-protect tx-mode

Syntax: (config-if)# loop-protect tx-mode

Explanation: Enable a port to actively generate loop protection PDUs.

Negation: (config-if)# no loop-protect tx-mode

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.9.27 (config)# mac

3.9.27.1 (config)# mac address-table aging-time

Syntax: (config)# mac address-table aging-time <v_0_10_to_1000000>

Explanation: Configure the aging time for a learned MAC to be appeared in MAC learning table.

Parameters:

<v_0_10_to_1000000>: Specify an aging time value for MAC address table. The valid values are from 10 to 1000000 (seconds). Using "0" to disable aging time function.

Example: Set the aging time to 600 seconds.

```
# config t
(config)# mac address-table aging-time 600
```

Negation: (config)# no mac address-table aging-time
(config)# no mac address-table aging-time <v_0_10_to_1000000>

Show: > show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]]
show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]]
show mac address-table aging-time

3.9.27.2 (config)# mac address-table static

Syntax: (config)# mac address-table static <v_mac_addr> vlan <v_vlan_id> interface (<port_type> [<v_port_type_list>])

Explanation: Configure the static MAC address mapping table.

Parameters:

<v_mac_addr>: Specify MAC address in "xx:xx:xx:xx:xx:xx" format.

vlan <v_vlan_id>: Specify the VLAN ID for this entry.

interface (<port_type> [<v_port_type_list>]): Specify the interface port type and the port number.

Example: Add a static MAC address "11:11:22:22:33:33" to MAC address table.

```
# config t
(config)# mac address-table static 11:11:22:22:33:33 vlan 1 interface
GigabitEthernet 1/1-10
```

Negation: (config)# no mac address-table static <v_mac_addr> vlan <v_vlan_id> interface (<port_type> [<v_port_type_list>])

Show: > show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]
show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]

Clear: # clear mac address-table

3.9.27.3 (config-if)# mac address-table learning

Syntax: (config)# mac address-table learning [secure]

Explanation: Set this interface to secure mode.

Parameters:

[secure]: Only static MAC entries listed in “Static MAC Table Configuration” are learned. Others will be dropped.

NOTE: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Negation: (config-if)# no mac address-table learning [secure]

Show: > show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]
show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]

Clear: # clear mac address-table

3.9.28 (config-if)# media-type

Syntax: (config-if)# media-type { rj45 | sfp | dual }

Explanation: Configure the media type supported for this specific interface.

Parameters:

{ rj45 | sfp | dual }: The options are RJ-45, SFP, or dual (both RJ-45 & SFP are supported.).

Negation: (config-if)# no media-type

3.9.29 (config-if)# mtu

Syntax: (config-if)# mtu <max_length>

Explanation: Configure the maximum transmission unit for this specific interface.

Parameters:

<max_length: 1518-10056>: Specify the MTU. The range is 1518 to 10056 bytes.

Negation: (config-if)# no mtu

Show: # show interface (<port_type> [<v_port_type_list>]) status

3.9.30 (config)# monitor session

Syntax: (config)# monitor session <session_number> [destination { interface (<port_type> [<di_list>]) | remote vlan <drid> reflector-port <port_type> <rportid> } | source { interface (<port_type> [<si_list>]) [both | rx | tx] | remote vlan <srvid> | vlan <source_vlan_list> | cpu [both | rx | tx] }]

Explanation: Configure which port traffic should be mirrored to.

Parameters:

<session_number <1-5>: Specify a session number (1 to 5) to this entry.

[destination { interface (<port_type> [<di_list>]) | remote vlan <drid> reflector-port <port_type> <rportid> } | source { interface (<port_type> [<si_list>]) [both | rx | tx] | remote vlan <srvid> | vlan <source_vlan_list> | cpu [both | rx | tx] }]: Specify the mirroring source.

Negation: (config)# no monitor session <session_number> [destination { interface (<port_type> [<di_list>]) | remote vlan <drid> reflector-port <port_type> <rportid> } | source { interface (<port_type> [<si_list>]) [both | rx | tx] | remote vlan <srvid> | vlan <source_vlan_list> | cpu [both | rx | tx] }]

3.9.31 (config)# mvr

3.9.31.1 (config)# mvr

Syntax: (config)# mvr

Explanation: Enable MVR function.

Example: Enable MVR function.

```
# config t
(config)# mvr
```

Negation: (config)# no mvr

Show: > show mvr

```
# show mvr
```

3.9.31.2 (config)# mvr name <mvr_name> channel

Syntax: (config)# mvr name <mvr_name> channel <profile_name>

Explanation: Configure MVR name and channel.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<profile_name>: Specify a channel name for this MVR entry. The allowed characters are 16.

Example: Set up a MVR entry “video1” and its corresponding channel profile name “1”.

```
# config t
(config)# mvr name video1 channel 1
```

Negation: (config)# no mvr name <mvr_name> channel

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.3 (config)# mvr name <mvr_name> frame priority

Syntax: (config)# mvr name <mvr_name> frame priority <cos_priority>

Explanation: Configure the priority for transmitting IGMP/MLD control frames for the specified MVR entry.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<cos_priority>: Specify a Cos priority for this MVR entry. The allowed range is from 0 to 7.

Example: Set up a MVR entry “video1” and its corresponding priority value “0”.

```
# config t
(config)# mvr name video1 frame priority 0
```

Negation: (config)# no mvr name <mvr_name> frame priority

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.4 (config)# mvr name <mvr_name> frame tagged

Syntax: (config)# mvr name <mvr_name> frame tagged

Explanation: Tagged IGMP/MLD frames will be sent.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

Example: Set “video1” MVR entry to send tagged IGMP/MLD frames.

```
# config t
(config)# mvr name video1 frame tagged
```

Negation: (config)# no mvr name <mvr_name> frame tagged

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.5 (config)# mvr name <mvr_name> igmp-address

Syntax: (config)# mvr name <mvr_name> igmp-address <v_ipv4_ucast>

Explanation: Configure IGMP IPv4 address for the specified MVR entry.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<v_ipv4_ucast>: Specify the IPv4 unicast address as source address used in IP header for IGMP control frames.

Example: Set up a MVR entry “video1” and its corresponding IGMP address “10.1.1.100”.

```
# config t
(config)# mvr name video1 igmp-address 10.1.1.100
```

Negation: (config)# no mvr name <mvr_name> igmp-address

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.6 (config)# mvr name <mvr_name> last-member-query-interval

Syntax: (config)# mvr name <mvr_name> last-member-query-interval <ipmc_lmqi>

Explanation: Configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<ipmc_lmqi>: Specify the LMQI (Last Member Query Interval) value. By default, LMQI is set to 5 tenths of a second (0.5 second). The allowed range is from 0 to 31744 tenths of a second.

Example: Set LMQI value to 600 tenths of a second.

```
# config t
(config)# mvr name video1 last-member-query-interval 600
```

Negation: (config)# no mvr vlan <mvr_name> last-member-query-interval

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.7 (config)# mvr name <mvr_name> mode

Syntax: (config)# mvr name <mvr_name> mode { dynamic | compatible }

Explanation: Configure MVR mode.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

{ dynamic | compatible }: Specify one of the options.

Dynamic: MVR allows dynamic MVR membership reports on source ports. (This is the default mode.)

Compatible: MVR membership reports are forbidden on source ports.

Example: Set MVR mode to dynamic.

```
# config t
(config)# mvr name video1 mode dynamic
```

Negation: (config)# no mvr name <mvr_name> mode

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

```
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```

3.9.31.8 (config)# mvr vlan <v_vlan_list> [name <mvr_name>]

Syntax: (config)# mvr vlan <v_vlan_list> [name <mvr_name>]

Explanation: Configure a MVR VLAN and its corresponding MVR name.

Parameters:

<v_vlan_list>: Specify multicast VLAN ID.

[name <mvr_name>]: Specify a name for this MVR entry. This argument is optional.

Example: Set up MVR VLAN 201 and its corresponding name.

```
# config t
(config)# mvr vlan 201 video1
```

Negation: (config)# no mvr vlan <v_vlan_list>

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.9 (config)# mvr vlan <v_vlan_list> channel

Syntax: (config)# mvr vlan <v_vlan_list> channel <profile_name>

Explanation: Configure MVR name and channel.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

<profile_name>: Specify a channel name for this MVR entry. The allowed characters are 16.

Example: Set up Set up MVR VLAN 201 and its corresponding channel.

```
# config t
(config)# mvr vlan 201 channel 1
```

Negation: (config)# no mvr vlan <v_vlan_list> channel

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.10 (config)# mvr vlan <v_vlan_list> frame priority

Syntax: (config)# mvr vlan <v_vlan_list> frame priority <cos_priority>

Explanation: Configure the priority for transmitting IGMP/MLD control frames for the specified MVR VLAN ID.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

<cos_priority>: Specify a Cos priority for this MVR entry. The allowed range is from 0 to 7.

Example: Set up a MVR VLAN 201 and its corresponding priority value "0".

```
# config t
(config)# mvr vlan 201 frame priority 0
```

Negation: (config)# no mvr vlan <v_vlan_list> frame priority

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.11 (config)# mvr vlan <v_vlan_list> frame tagged

Syntax: (config)# mvr vlan <v_vlan_list> frame tagged

Explanation: Tagged IGMP/MLD frames will be sent.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

Example: Set MVR VLAN 201 to send tagged IGMP/MLD frames.

```
# config t
(config)# mvr vlan 201 frame tagged
```

Negation: (config)# no mvr vlan <v_vlan_list> frame tagged

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.12 (config)# mvr vlan <v_vlan_list> igmp-address

Syntax: (config)# mvr vlan <v_vlan_list> igmp-address <v_ipv4_ucast>

Explanation: Configure IGMP IPv4 address for the specified MVR entry.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

<ipv4_ucast>: Specify the IPv4 unicast address as source address used in IP header for IGMP control frames.

Example: Set up a MVR VLAN 201 and its corresponding IGMP address "10.1.1.100".

```
# config t
(config)# mvr vlan 201 igmp-address 10.1.1.100
```

Negation: (config)# no mvr vlan <v_vlan_list> igmp-address

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.13 (config)# mvr vlan <v_vlan_list> last-member-query-interval

Syntax: (config)# mvr vlan <v_vlan_list> last-member-query-interval <ipmc_lmqi>

Explanation: Configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

<ipmc_lmqi>: Specify the LMQI (Last Member Query Interval) value. By default, LMQI is set to 5 tenths of a second (0.5 second). The allowed range is from 0 to 31744 tenths of a second.

Example: Set LMQI value to 600 tenths of a second.

```
# config t
(config)# mvr vlan 201 last-member-query-interval 600
```

Negation: (config)# no mvr vlan <v_vlan_list> last-member-query-interval

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.14 (config)# mvr vlan <v_vlan_list> mode

Syntax: (config)# mvr vlan <v_vlan_list> mode { dynamic | compatible }

Explanation: Configure MVR mode.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

{ dynamic | compatible }: Specify one of the options.

Dynamic: MVR allows dynamic MVR membership reports on source ports. (This is the default mode.)

Compatible: MVR membership reports are forbidden on source ports.

Example: Set MVR mode to dynamic.

```
# config t
(config)# mvr vlan 201 mode dynamic
```

Negation: (config)# no mvr vlan <v_vlan_list> mode

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.9.31.15 (config-if)# mvr immediate-leave

Syntax: (config-if)# mvr immediate-leave

Explanation: Enable immediate leave function. When enabled, the device immediately removes a port from a multicast stream as soon as it receives leave message for that group. This option only applies to an interface configured as MVR receivers.

Example: Enable immediate leave function on port 1.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# mvr immediate-leave
```

Negation: (config-if)# no mvr immediate leave

3.9.31.16 (config-if)# mvr name

Syntax: (config-if)# mvr name <mvr_name> type { source | receiver }

Explanation: Configure port role of specific MVR profile for specific interface.

Parameters:

<mvr_name>: Specify a MVR name. The maximum length of the MVR name string is 16. Both alphabets and numbers are allowed for use.

{ source | receiver }: Specify MVR port role.

source: MVR source port.

receiver: MVR receiver port.

Negation: (config-if)# no mvr name <mvr_name> type

3.9.31.17 (config-if)# mvr vlan

Syntax: (config-if)# mvr vlan <v_vlan_list> type { source | receiver }

Explanation: Configure port role of a specific MVR VLAN ID for this specific interface.

Parameters:

<v_vlan_list>: MVR Multicast VLAN list

{ source | receiver }: Specify MVR port role.

source: MVR source port.

receiver: MVR receiver port.

Negation: (config-if)# no mvr immediate leave

3.9.32 (config)# ntp

3.9.32.1 (config)# ntp

Syntax: (config)# ntp

Explanation: Enable NTP function.

Example: Enable NTP function.

```
# config t
(config)# ntp
```

Negation: (config)# no ntp

Show: # show ntp status

3.9.32.2 (config)# ntp server

Syntax: (config)# ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }

Explanation: Configure a list of NTP server's address.

Parameters:

< index_var: 1-5>: Specify the index number of NTP server. The allowed range is from 1 to 5. The NTP servers are tried in numeric order. If 'Server 1' is unavailable, the NTP client will try to contact 'Server 2'.

{ <ipv4_var> | <ipv6_var> | <name_var> }: Specify one of the three options.

<ipv4_var>: IPv4 address.

<ipv6_var>: IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once.

<name_var>: The domain name for NTP server.

Example: Set the NTP server 1 to 192.168.1.253.

```
# config t
(config)# ntp server 1 ip-address 192.168.1.253
```

Negation: (config)# no ntp server <index_var>

Show: # show ntp status

3.9.33 (config)# port-security

3.9.33.1 (config)# port-security

Syntax: (config)# port-security

Explanation: Enable port security function globally.

Example: Enable port security function globally.

```
# config t
(config)# port-security
```

Negation: (config)# no port-security

Show: > show port-security switch [interface (<port_type> [<v_port_type_list>])]
show port-security switch [interface (<port_type> [<v_port_type_list>])]

3.9.33.2 (config)# port-security aging

Syntax: (config)# port-security aging

Explanation: Enable port security aging function. If enabled, secured MAC addresses are subject to aging as discussed in “Aging time” command. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Example: Enable port security aging function.

```
# config t
(config)# port-security aging
```

Negation: (config)# no port-security aging

Show: > show port-security port [interface (<port_type> [<v_port_type_list>])]
show port-security port [interface (<port_type> [<v_port_type_list>])]

3.9.33.3 (config)# port-security aging time

Syntax: (config)# port-security aging time <v_10_to_10000000>

Explanation: Configure a desired aging time value. If “Aging” is enabled, secured MAC addresses are subject to aging as discussed this command. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Parameters:

<v_10_to_10000000>: Specify the aging time value. The allowed range is between 10 and 10,000,000 seconds.

Example: Set the aging time value to 1800 seconds.

```
# config t
(config)# port-security aging time 1800
```

Negation: (config)# no port-security aging time

Show: > show port-security port [interface (<port_type> [<v_port_type_list>])]
show port-security port [interface (<port_type> [<v_port_type_list>])]

3.9.33.4 (config-if)# port-security

Syntax: (config-if)# port-security

Explanation: Enable the port security function on the selected ports.

Example: Enable Gigabit Ethernet port 1-10's port security function.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security
```

Negation: (config-if)# no port-security

Show: > show port-security switch [interface (<port_type> [<v_port_type_list>])]
show port-security switch [interface (<port_type> [<v_port_type_list>])]

3.9.33.5 (config-if)# port-security maximum

Syntax: (config-if)# port-security maximum [<v_1_to_1024>]

Explanation: The maximum number of MAC addresses that can be secured on this port. The number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

Parameters:

[<v_1_to_1024>]: Specify a value between 1 and 1024.

Example: Limit Gigabit Ethernet port 1-10's MAC addresses can be learnt to 5.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security maximum 5
```

Negation: (config-if)# no port-security maximum

Show: > show port-security port [interface (<port_type> [<v_port_type_list>])]
show port-security port [interface (<port_type> [<v_port_type_list>])]

3.9.33.6 (config-if)# port-security violation

Syntax: (config-if)# port-security violation { protect | trap | trap-shutdown | shutdown }

Explanation: If the limit is exceeded, the specified action will take effect.

Parameters:

{ protect | trap | trap-shutdown | shutdown }: Specify one of the actions taken when the limit is exceeded.

protect: Do not allow more than the specified limit of MAC addresses to access on a port. No action is further taken.

trap: If Limit + 1 MAC addresses are seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit is exceeded.

trap-shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new addresses will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

- * Boot the switch
- * Disable and re-enable Limit Control on the port or the switch
- * Click the "Reopen" button

Example: Send a SNMP trap when the limit is exceeded.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security violation trap
```

Negation: (config-if)# no port-security violation

Show: > show port-security port [interface (<port_type> [<v_port_type_list>])]
show port-security port [interface (<port_type> [<v_port_type_list>])]

3.9.34 (config)# privilege

Syntax: (config)# privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <privilege> <cmd>

Explanation: This command is used to change the privilege level of commands available in Configuration mode.

Parameters:

{ exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile }: Specify the group command that you want to configure.

level <privilege>: Specify the privilege level. The allowed range is 0 to 15.

<cmd>: Initial valid words and literals of the command to modify, in 128 characters.

Example: The following example sets the privilege level to 15 for any Exec mode (user or privileged) command that start with the letter "v"

```
# config t
(config)# privilege exec level 15 host
```

Negation: (config)# no privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <0-15> <cmd>

Show: > show privilege
show privilege

3.9.35 (config-if)# pvlan

3.9.35.1 (config-if)# pvlan

Syntax: (config-if)# pvlan <pvlan_list>

Explanation: This command is used to configure private VLANs. New Private VLANs can be added and existing VLANs can be modified. Private VLANs are based on the source port mask and there are no connections to VLANs which means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Parameters:

<pvlan_list>: Specify the private VLAN ID.

Negation: (config-if)# no pvlan <pvlan_list>

Show: # show pvlan <pvlan_list>

3.9.35.2 (config-if)# pvlan isolation

Syntax: (config-if)# pvlan isolation

Explanation: Enable Port Isolation function on this specific interface. Port Isolation is used to prevent communications between customer ports in a same Private VLAN. The port that is isolated from others cannot forward any unicast, multicast or broadcast traffic to any other ports in the same PVLAN.

Negation: (config-if)# no pvlan isolation

Show: # show pvlan isolation [interface (<port_type> [<plist>])]

3.9.36 (config)# qos

3.9.36.1 (config)# qos map cos-dscp

Syntax: (config)# qos map cos-dscp <cos> dpl <dpl> dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Parameters:

cos-dscp <cos>: Map COS to DSCP. Indicate the Class of Service level. The allowed range is 0 to 7. A CoS class of 0 has the lowest priority, while 7 has the highest priority.

dpl <dpl>: Specify the Drop Precedence Level. The allowed range is 0 to 7.

dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num> 0-63>: The allowed number is from 0 to 63.
be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Explanation: Configure the COS-DSCP mapping.

Example: The following example sets DPL to 4, DSCP to cs4.

```
# config t
(config)# qos map cos-dscp 4 dpl 4 dscp cs4
```

Negation: (config)# no qos map cos-dscp <cos> dpl <dpl>

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.2 (config)# qos map dscp-classify

Syntax: (config)# qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Parameters:

dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Explanation: Configure the DSCP Ingress classification.

Example: The following example sets DSCP Ingress classification to cs4.

```
# config t
(config)# qos map dscp-classify cs4
```

Negation: (config)# no qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Show: # show qos
show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.9.36.3 (config)# qos map dscp-cos

Syntax: (config)# qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <cos> dpl <dpl>

Explanation: Configure the DSCP-based QoS Ingress classification.

Parameters:

dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

cos <cos>: Indicate the Class of Service level. The allowed range is 0 to 7. A CoS class of 0 has the lowest priority, while 7 has the highest priority.

dpl <dpl>: Specify the Drop Precedence Level. The allowed range is 0 to 7.

Negation: (config)# no qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Show: # show qos
show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.9.36.4 (config)# qos map dscp-egress-translation

Syntax: (config)# qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { <dscp_num_tr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Explanation: Configure the DSCP Egress Mapping Table.

Parameters:

dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }; Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Example: The following example maps cs4 to cs5.

```
# config t
(config)# qos map dscp-egress-translation cs4 to cs5
```

Negation: (config)# no qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } <dpl>

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.5 (config)# qos map dscp-ingress-translation

Syntax: (config)# qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { <dscp_num_tr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Explanation: Configure the DSCP Ingress Mapping Table.

Parameters:

dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }; Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Example: The following example maps cs4 to cs5.

```
# config t
(config)# qos map dscp-ingress-translation cs4 to cs5
```

Negation: (config)# no qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ] }
```

3.9.36.6 (config)# qos qce refresh

Syntax: (config)# qos qce refresh

Explanation: To refresh QCE.

Example: Refresh QCE.

```
# config t
(config)# qos qce refresh
```

3.9.36.7 (config)# qos qce update

Syntax: (config)# qos qce { [update] } <qce_id> [{ next <qce_id_next> } | last] [interface (<port_type> [<port_list>])] [smac { <smac> | <smac_24> | any }] [dmac { <dmac> | unicast | multicast | broadcast | any }] [tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <ot_vid> | any }] [pcp { <ot_pcp> | any }] [dei { <ot_dei> | any }] } *1] [inner-tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <it_vid> | any }] [pcp { <it_pcp> | any }] [dei { <it_dei> | any }] } *1] [frame-type { any | { etype { <etype_type> | any } }] | llc [dsap { <llc_dsap> | any }] [ssap { <llc_ssap> | any }] [control { <llc_control> | any }] }] { snap [{ <snap_data> | any }] } | { ipv4 [proto { <pr4> | tcp | udp | any }] [sip { <sip4> | any }] [dip { <dip4> | any }] [dscp { <dscp4> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7

```
| ef | va } | any } ] [ fragment { yes | no | any } ] [ sport { <sp4> | any } ] [ dport { <dp4> | any } ] ] { { ipv6 [ proto
{ <pr6> | tcp | udp | any } ] [ sip { <sip6> | any } ] [ dip { <dip6> | any } ] [ dscp { <dscp6> | { be | af11 | af12 | af13 |
af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ]
[ sport { <sp6> | any } ] [ dport { <dp6> | any } ] ] } ] [ action { [ cos { <action_cos> | default } ] [ dpl { <action_dpl> |
default } ] [ pcpc-dei { <action_pcpc> <action_dei> | default } ] [ dscp { <action_dscp_dscp> | { be | af11 | af12 | af13 |
af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | default } ]
[ policy { <action_policy> | default } ] } ] *1 ]
```

Explanation: To update the QCE.

Parameters:

[[update]]: Update the QCE.

<qce_id>: Specify the QCE ID.

[{ next <qce_id_next> } | last]: Put this QCE next to the specified one or to the last one.

[interface (<port_type> [<port_list>])]: Specify port type and port number that apply to this updated QCE rule.

[smac { <smac> | <smac_24> | any }]: Set up the matched SMAC.

[dmac { <dmac> | unicast | multicast | broadcast | any }]: Set up the matched DMAC.

[tag { [type { untagged | tagged | c-tagged | s-tagged | any }]]: Set up the matched tag type.

[vid { <ot_vid> | any }]: Specify a specific VID or VID range or specify “any” to allow any VIDs.

[pcpc { <ot_pcpc> | any }]: Specify a specific PCP or PCP range or specify “any” to allow any PCP values.

[dei { <ot_dei> | any }]]: Specify a specific DEI or specify “any” to allow any DEI.

[frame-type { any | { etype [{ <etype_type> | any }]] { llc [dsap { <llc_dsap> | any }] [ssap { <llc_ssap> | any }] [control { <llc_control> | any }]] { snap [{ <snap_data> | any }]] { ipv4 [proto { <pr4> | tcp | udp | any }] [sip { <sip4> | any }] [dip { <dip4> | any }] [dscp { <dscp4> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [fragment { yes | no | any }] [sport { <sp4> | any }] [dport { <dp4> | any }]] { { ipv6 [proto { <pr6> | tcp | udp | any }] [sip { <sip6> | any }] [dip { <dip6> | any }] [dscp { <dscp6> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [sport { <sp6> | any }] [dport { <dp6> | any }]] }]]: Specify the frame type that applies to this QCE rule.

any: By default, any is used which means that all types of frames are allowed.

etype: This option can only be used to filter Ethernet II formatted packets. (Options: Any, Specific – 600-ffff hex; Default: ffff). Note that 800 (IPv4) and 86DD (IPv6) are excluded. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

llc: LLC refers to Link Logical Control and further provides three options.

dsap: DSAP stands for Destination Service Access Point address. By default, any is used. Specify “any” or indicate a value (0x00 to 0xFF).

ssap: SSAP stands for Source Service Access Point address. By default, any is used. Specify “any” or indicate a value (0x00 - 0xFF).

control: Control field may contain command, response, or sequence information depending on whether the LLC frame type is Unnumbered, Supervisory, or Information. By default, any is used. Specify “any” or indicate a value (0x00 to 0xFF).

snap: SubNetwork Access Protocol can be distinguished by an OUI and a Protocol ID. (Options for PID: Any, Specific (0x00-0xffff); Default: Any) If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

ipv4:

proto: IPv4 frame type includes Any, TCP, UDP, Other. If “TCP” or “UDP” is specified, you might further define Sport (Source port number) and Dport (Destination port number).

sip: Specify source IP type. By default, any is used. Indicate self-defined source IP and submask format. The address and mask must be in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero

dscp: By default, any is used. Indicate a DSCP value or a range of DSCP value.

fragment: By default, any is used. Datagrams sometimes may be fragmented to ensure they can pass through a network device that uses a maximum transfer unit smaller than the original packet’s size.

ipv6:

proto: IPv6 protocol includes Any, TCP, UDP, Other. If “TCP” or “UDP” is specified, you may need to further define Sport (Source port number) and Dport (Destination port number).

sip: Specify source IP type. By default, any is used. You can also indicate self-defined source IP and submask format.

dscp: By default, any is used. You can also indicate a DSCP value or a range of DSCP value.

[action { [cos { <action_cos> | default }] }: Specify the classification action taken on ingress frame if the parameters match the frame’s content. If a frame matches the QCE, it will be put in the queue corresponding to the specified QoS class or placed in a queue based on basic classification rules.

[dpl { <action_dpl> | default }]: If a frame matches the QCE, the drop precedence level will be set to the specified value or left unchanged.

[pcp-dei { <action_pcp> <action_dei> | default }]: If a frame matches the QCE, the PCP or DEI value will be set to the specified one.

[dscp { <action_dscp_dscp> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | default }] [policy { <action_policy> | default }] *1]: If a frame matches the QCE, the DSCP value will be set to the specified one.

Negation: (config)# no qos qce <qce_id_range>

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.9.36.8 (config)# qos storm

Syntax: (config)# qos storm { unicast | multicast | broadcast } <rate> [fps | kfps | kbps | mbps]

Explanation: Configure broadcast storm control rate for QoS

Parameters:

{ unicast | multicast | broadcast }: Specify the storm type that you want to configure.

{ { <rate> [kfps] } | { 1024 kfps } }: User-define storm frame rate or set storm rate to 1024 kfps.

Example: The following example sets broadcast storm control for QoS to 1024 kfps.

```
# config t
(config)# qos storm broadcast 1024 kfps
```

Negation: (config)# no qos storm { unicast | multicast | broadcast }

Show: # show qos storm

3.9.36.9 (config)# qos wred queue

Syntax: (config)# qos wred group <group> queue <queue> min-th <min_th> mdp-1 <mdp_1> mdp-2 <mdp_2> mdp-3 <mdp_3>

Explanation: Apply RED on a particular queue or set up the minimum threshold & drop probability value.

Parameters:

queue <queue>: Specify the queue number. Queue 0 to 5 can apply to Random Early Detection (RED). However, RED cannot be applied to Queue 6 and 7.

min-th <min_th>: Specify the lowest RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This valid value for this field is 0~100.

mdp-1 <mdp_1>: Controls the drop probability for the frames marked in drop precedence level 1 when the average queue filling level is 100%. The valid value is 0~100.

mdp-2 <mdp_2>: Controls the drop probability for the frames marked in drop precedence level 2 when the average queue filling level is 100%. The valid value is 0~100.

mdp-3 <mdp_3>: Controls the drop probability for the frames marked in drop precedence level 3 when the average queue filling level is 100%. The valid value is 0~100.

Negation: (config)# no qos wred queue <queue>

Show: # show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.9.36.10 (config-if)# qos cos

Syntax: (config-if)# qos cos <cos>

Explanation: Configure CoS value on this selecte infterface.

Parameters:

<cos>: Specify COS value (1-7).

Negation: (config-if)# no qos cos

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.11 (config-if)# qos dei

Syntax: (config-if)# qos dei <dei>

Explanation: Configure DEI (Drop Eligible Indicator) value on this selecte infterface.

Parameters:

<dei>: Specify DEI for untagged frames.

Negation: (config-if)# no qos dei

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.12 (config-if)# qos dpl

Syntax: (config-if)# qos dpl <dpl>

Explanation: Configure DPL value on this selecte infterface.

Parameters:

<dpl>: Specify the default Drop Precedence Level

Negation: (config-if)# no qos dpl

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.13 (config-if)# qos dscp-classify

Syntax: (config-if)# qos dscp-classify { zero | selected | any }

Explanation: Configure a classification method.

Parameters:

{ zero | selected | any }: Specify a classification method.

zero: Classify if incoming DSCP is 0.

selected: Classify only selected DSCP for which classification is enabled in DSCP Translation table

any: Classify all DSCP.

Negation: (config-if)# no qos dscp-classify

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.14 (config-if)# qos dscp-remark

Syntax: (config-if)# qos dscp-remark { rewrite | remap | remap-dp }

Explanation: Configure port egress rewriting of DSCP values.

Parameters:

{ rewrite | remap | remap-dp }: Specify an option.

rewrite: Rewrite DSCP field with classified DSCP value.

remap: Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. Depending on the frame's DP level, the remapped DSCP value is either taken from the DSCP Translation table, Egress Remap DP0 or DP1 field.

remap-dp: Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. The remapped DSCP value is always taken from the DSCP Translation table, Egress Remap DP0 field.

Negation: (config-if)# no qos dscp-remark

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.15 (config-if)# qos dscp-translate

Syntax: (config-if)# qos dscp-translate

Explanation: Configure DSCP ingress translation of QoS for specific interface.

Negation: (config-if)# no qos dscp-translate

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.16 (config-if)# qos map cos-tag cos

Syntax: (config-if)# qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>

Explanation: Configure (QoS class, DP level) to (PCP, DEI) Mapping of QoS for specific interface.

Parameters:

cos <cos: 0-7>: Specify a QoS class value.

dpl <dpl:0-1>: Specify a DPL value (0 or 1).

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value.

dei <dei: 0-1>: Specify a DEI value (0 or 1).

Negation: (config-if)# no qos map cos-tag cos <cos> dpl <dpl>

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.17 (config-if)# qos map tag-cos pcp

Syntax: (config-if)# qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>

Explanation: Configure (PCP, DEI) to (QoS class, DP level) Mapping of QoS for specific interface.

Parameters:

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value.

dei <dei: 0-1>: Specify a DEI value (0 or 1).

cos <cos: 0-7>: Specify a QoS class value.

dpl <dpl:0-1>: Specify a DPL value (0 or 1).

Negation: (config-if)# no qos map tag-cos pcp <pcp> dei <dei>

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```


3.9.36.18 (config-if)# qos pcp

Syntax: (config-if)# qos pcp <pcp>

Explanation: Configure PCP value for specific interface.

Parameters:

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value.

Negation: (config-if)# no qos pcp

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.19 (config-if)# qos policer

Syntax: (config-if)# qos policer <rate> [fps] [flowcontrol]

Explanation: Configure PCP value for specific interface.

Parameters:

<rate>: Indicate the rate for the policer. By default, 500kbps is used. The allowed range for kbps and fps is 100 to 1000000. The allowed range for Mbps and kfps is 1 to 3300Mbps.

[fps]: Rate is fps. By default, kbps is used.

[flowcontrol]: Enable Flow Control. If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames

Negation: (config-if)# no qos policer

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.20 (config-if)# qos queue-policer queue

Syntax: (config-if)# qos queue-policer queue <queue> <rate>

Explanation: Configure Ingress Queue Policers Rate of QoS for specific interface.

Parameters:

<queue: 0-7>: Specify a queue or a range.

<rate: 100-3300000>: Specify Policer rate in kbps.

Negation: (config-if)# no qos queue-policer queue <queue>

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.21 (config-if)# qos queue-shaper queue

Syntax: (config-if)# qos queue-shaper queue <queue> <rate> [excess]

Explanation: Configure Egress Queue Policers Rate of QoS for specific interface.

Parameters:

<queue: 0-7>: Specify a queue or a range.

<rate: 100-3300000>: Specify Policer rate in kbps.

[excess]: Allow all excess bandwidth.

Negation: (config-if)# no qos queue-shaper queue <queue>

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.22 (config-if)# qos shaper

Syntax: (config-if)# qos shaper <rate>

Explanation: Configure Egress Queue Policers Rate of QoS for specific interface.

Parameters:

<rate: 100-3300000>: Specify Policer rate in kbps.

Negation: (config-if)# no qos shaper

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

3.9.36.23 (config-if)# qos tag-remark

Syntax: (config-if)# qos tag-remark { pcpc <pcpc> dei <dei> | mapped }

Explanation: Configure the appropriate remarking mode used by this port.

Parameters:

{ pcpc <pcpc> dei <dei> | mapped }: Specify a remarking mode.

pcpc <pcpc> dei <dei>: Specify PCP and DEI value.

mapped: Use the mapping of the classified QoS class values and DP levels to PCP/DEI values.

Negation: (config-if)# no qos tag-remark

Show: # show qos
show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.9.36.24 (config-if)# qos trust dscp

Syntax: (config-if)# qos trust dscp

Explanation: Enable DSCP Classification of QoS for specific interface.

Negation: (config-if)# no qos trust dscp

Show: # show qos
show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.9.36.25 (config-if)# qos trust tag

Syntax: (config-if)# qos trust tag

Explanation: Enable VLAN tag Classification of QoS for specific interface.

Negation: (config-if)# no qos trust tag

Show: # show qos
show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.9.36.26 (config-if)# qos wred-group

Syntax: (config-if)# qos wred-group <wred_group>

Explanation: Assign a WRED group to this interface.

Parameters:

<wred_group>: Specify a WRED group. The valid number is 1~3.

Negation: (config-if)# no qos wred-group

Show: # show qos wred

3.9.36.27 (config-if)# qos wrr

Syntax: (config-if)# qos wrr <w0> <w1> <w2> <w3> <w4> <w5>

Explanation: Assign weight for QoS queueing method. WRR stands for Weighted Round Robin and uses default queue weights. The number of packets serviced during each visit to a queue depends on the percentages you configure for the queues.

Parameters:

<w0: 1-100>: Specify weight for queue 0.

<w1: 1-100>: Specify weight for queue 1.

<w2: 1-100>: Specify weight for queue 2.

<w3: 1-100>: Specify weight for queue 3.

<w4: 1-100>: Specify weight for queue 4.

<w5: 1-100>: Specify weight for queue 5.

Negation: (config-if)# no qos wrr

Show: # show qos

```
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ]
[ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } }
```

3.9.37 (config)# radius-server

3.9.37.1 (config)# radius-server attribute 32

Syntax: (config)# radius-server attribute 32 <id>

Explanation: Configure Radius attribute 32 string.

Parameters:

<id>: Specify Radius server identifier. The allowed characters are 1 to 253.

```
# config t
(config)# radius-server attribute 32 cabinet5aSW
```

Negation: (config)# no radius-server attribute 32

Show: # show radius-server [statistics]

3.9.37.2 (config)# radius-server attribute 4

Syntax: (config)# radius-server attribute 4 <ipv4>

Explanation: Configure NAS IPv4 address.

Parameters:

<ipv4>: Specify NAS IPv4 address.

Example: Set NAS IPv4 address to 100.1.1.25.

```
# config t
(config)# radius-server attribute 4 100.1.1.25
```

Negation: (config)# no radius-server attribute 4

Show: # show radius-server [statistics]

3.9.37.3 (config)# radius-server attribute 95

Syntax: (config)# radius-server attribute 95 <ipv6>

Explanation: Configure NAS IPv6 address.

Parameters:

<ipv6>: Specify NAS IPv6 address.

Negation: (config)# no radius-server attribute 95

Show: # show radius-server [statistics]

3.9.37.4 (config)# radius-server deadtime

Syntax: (config)# radius-server deadtime <minutes>

Explanation: Configure RADIUS server deadtime value. Deadtime is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Parameters:

<deadtime>: Specify RADIUS server deadtime value. The valid range is 1 to 1440 (minutes).

Example: Set RADIUS server to 60.

```
# config t
(config)# radius-server deadtime 60
```

Negation: (config)# no radius-server deadtime

Show: # show radius-server [statistics]

3.9.37.5 (config)# radius-server host

Syntax: (config)# radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>] [timeout <seconds>] [retransmit <retries>] [key <key>]

Explanation: This command is used to configure Radius server.

Parameters:

<host_name>: Specify the hostname or IP address for the radius server. The allowed characters are 1 to 255.

[auth-port <auth_port>]: Specify the UDP port to be used on the RADIUS server for authentication.

[acct-port <acct_port>]: Specify the UDP port to be used on the RADIUS server for accounting.

[timeout <seconds>]: Specify a timeout value. If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

[retransmit <retries>]: Specify a value for retransmit retry. If retransmit value is specified here, it will replace the global retransmit value. If you prefer to use the global value, leave this field blank.

[key <key>]: Specify a secret key. If secret key is specified here, it will replace the global secret key. If you prefer to use the global value, leave this field blank.

Negation: (config)# no radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>]

Show: # show radius-server [statistics]

3.9.37.6 (config)# radius-server key

Syntax: (config)# radius-server key <key>

Explanation: Configure RADIUS server key value. This key is shared between the RADIUS sever and the switch.

Parameters:

<key>: Specify RADIUS server secret key value. The valid range is 1 to 63.

Example: Set RADIUS server secret key to 803321

```
# config t
(config)# radius-server key 803321
```

Negation: (config)# no radius-server key

3.9.37.7 (config)# radius-server retransmit

Syntax: (config)# radius-server retransmit <retries>

Explanation: Configure the number of times to retransmit request packets to an authentication server that does not respond. If the server does not respond after the last retransmit is sent, the switch considers the authentication server is dead.

Parameters:

<retries>: Specify RADIUS server retransmit value. The valid range is 1 to 1000.

Example: Set RADIUS server retransmit value to 5

```
# config t
(config)# radius-server retransmit 5
```

Negation: (config)# no radius-server retransmit

Show: # show radius-server [statistics]

3.9.37.8 (config)# radius-server timeout

Syntax: (config)# radius-server timeout <seconds>

Explanation: Configure the time the switch waits for a reply from an authentication server before it retransmits the request.

Parameters:

<seconds>: Specify RADIUS server timeout value. The valid range is 1 to 1000.

Example: Set RADIUS server timeout to 60

```
# config t
(config)# radius-server timeout 60
```

Negation: (config)# no radius-server timeout

Show: # show radius-server [statistics]

3.9.38 (config)# rmon

3.9.38.1 (config)# rmon alarm

Syntax: (config)# rmon alarm <id> <oid_str> <interval> { absolute | delta } rising-threshold <rising_threshold> [<rising_event_id>] falling-threshold <falling_threshold> [<falling_event_id>] { [rising | falling | both] }

Syntax: (config)# rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <ifIndex> <interval> { absolute | delta } rising-threshold <rising_threshold> [<rising_event_id>] falling-threshold <falling_threshold> [<falling_event_id>] { [rising | falling | both] }

Explanation: Configure RMON alarm settings. RMON Alarm configuration defines specific criteria that will generate response events. It can be set to test data over any specified time interval and can monitor absolute or changing values. Alarms can also be set to respond to rising or falling thresholds.

Parameters:

<id>: Indicates the index of the entry. The range is from 1 to 65535.

<oid_str>: The object number of the MIB variable to be sampled. Only variables of the type ifEntry.n.n may be sampled. Possible variables are ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifOutDiscards, ifErrors, ifInUnknownProtos, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifOutErrors.

<interval>: The polling interval for sampling and comparing the rising and falling threshold. The range is from 1 to 2³¹ (2147483647) seconds.

{ absolute | delta }: Test for absolute or relative change in the specified variable.

Absolute: The variable is compared to the thresholds at the end of the sampling period.

Delta: The last sample is subtracted from the current value and the difference is compared to the thresholds.

rising-threshold <rising_threshold>: If the current value is greater than the rising threshold and the last sample value is less than this threshold, then an alarm will be triggered. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. The threshold range is -2147483647 to 2147483647.

[<rising_event_id>]: Indicates the rising index of an event. The range is 1 - 65535.

falling-threshold <falling_threshold>: If the current value is less than the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the falling threshold. (Range: -2147483647 to 2147483647)

[<falling_event_id>]: Indicates the falling index of an event. The range is 0 - 65535.

{ [rising | falling | both] }: Specify a method that is used to sample the selected variable and calculate the value to be compared against the thresholds.

rising: Trigger alarm when the first value is larger than the rising threshold.

falling: Trigger alarm when the first value is less than the falling threshold.

both: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold.

Negation: (config)# no rmon alarm <id>

Show: # show rmon alarm [<id_list>]
show rmon history [<id_list>]
show rmon statistics [<id_list>]

3.9.38.2 (config)# rmon event

Syntax: (config)# rmon event <id> [log] [trap <community>] { [description <description>] }

Explanation: Configure RMON Event settings.

Parameters:

<id>: Specify an ID index. The range is 1 - 65535.

[log]: When the event is triggered, a RMON log entry will be generated.

[trap <community>]: A password-like community string sent with the trap. Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page prior to configuring it here. The allowed characters are 0 - 127.

{ [description <description>] }: Enter a descriptive comment for this entry.

Negation: (config)# no rmon event <id>

Show: # show rmon alarm [<id_list>]
show rmon history [<id_list>]

3.9.38.3 (config-if)# rmon collection history

Syntax: (config-if)# rmon collection history <id> [buckets <buckets>] [interval <interval>]

Explanation: RMON History Configuration is to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A RMON historical record can be used to monitor intermittent problems.

Parameters:

<id>: Specify an ID index. The range is 1~65535.

[buckets <buckets>]: The number of buckets requested for this entry. The allowed range is 1~65535.

[interval <interval>]: Indicates the polling interval. By default, 1800 seconds is specified. The allowed range is 1~3600 seconds.

Negation: (config-if)# no rmon collection history <id>

Show: # show rmon history [<id_list>]

3.9.38.4 (config-if)# rmon collection stats

Syntax: (config-if)# rmon collection stats <id>

Explanation: Configure RMON Statistics table using this command.

Parameters:

<id>: Specify an ID index. The range is 1~65535.

Negation: (config-if)# no rmon collection stats <id>

Show: # show rmon statistics [<id_list>]

3.9.39 (config)# sflow

3.9.39.1 (config)# sflow agent-ip

Syntax: (config)# sflow agent-ip { ipv4 <v_ipv4_addr> | ipv6 <v_ipv6_addr> }

Explanation: Specify a valid IPv4 or IPv6 address for sFlow agent.

Parameters:

{ ipv4 <v_ipv4_addr> | ipv6 <v_ipv6_addr> }: Specify a valid IPv4 or IPv6 address.

Negation: (config)# no sflow agent-ip

Show: # show sflow

3.9.39.2 (config)# sflow collector-address

Syntax: (config)# sflow collector-address [<ipv4_var> | <ipv6_var> | <domain_name>]

Explanation: Specify a valid IP address or hostname for sFlow receiver.

Parameters:

[<ipv4_var> | <ipv6_var> | <domain_name>]: Specify IP address or domain name of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

Negation: (config)# no sflow collector-address [<host_name>]

Show: # show sflow

3.9.39.3 (config)# sflow collector-port

Syntax: (config)# sflow collector-port <collector_port>

Explanation: Configure the UDP port on which the sFlow receiver listens to sFlow datagrams.

Parameters:

[<collector_port: 1~65535>]: Specify the UDP port on which the sFlow receiver listens to sFlow datagrams.

Negation: (config)# no sflow collector-port [<collector_port>]

Show: # show sflow

3.9.39.4 (config)# sflow max-datagram-size

Syntax: (config)# sflow max-datagram-size <datagram_size>

Explanation: Configure the maximum number of data bytes that can be sent in a single sample datagram.

Parameters:

<datagram_size>: Specify the maximum datagram size. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Negation: (config)# no sflow max-datagram-size

Show: # show sflow

3.9.39.5 (config)# sflow timeout

Syntax: (config)# sflow timeout <timeout>

Explanation: Configure the number of seconds remaining before sampling stops and the current sFlow owner is released.

Parameters:

<timeout>: Specify the number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.

Negation: (config)# no sflow timeout

Show: # show sflow

3.9.39.6 (config-if)# sflow

Syntax: (config-if)# sflow

Explanation: Enables flow sampling on this port.

Negation: (config-if)# no sflow

Show: # show sflow

3.9.39.7 (config-if)# sflow sampling-rate

Syntax: (config-if)# sflow sampling-rate [<sampling_rate>]

Explanation: Configure the statistical sampling rate for packet sampling.

Parameters:

[<sampling_rate>] : Specify the statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 to 4294967295.

Negation: (config-if)# no sflow sampling-rate

Show: # show sflow

```
# show sflow statistics { receiver | samplers [ interface [ <samplers_list> ] ( <port_type>
[ <v_port_type_list> ] ) ] }
```

3.9.39.8 (config-if)# sflow max-sampling-size

Syntax: (config-if)# sflow max-sampling-size [<max_sampling_size>]

Explanation: Configure the maximum number of bytes that should be copied from a sampled packet to the sFlow datagram.

Parameters:

[<max_sampling_size>] : Specify the maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

Negation: (config-if)# no sflow max-sampling-size

Show: # show sflow

show sflow statistics { receiver | samplers [interface [<samplers_list>] (<port_type> [<v_port_type_list>])] }

3.9.39.9 (config-if)# sflow counter-poll-interval

Syntax: (config-if)# sflow counter-poll-interval [<poll_interval>]

Explanation: Configure the counter polling interval.

Parameters:

[<poll_interval>] : Specify the counter polling interval. This indicates the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.

Negation: (config-if)# no sflow counter-poll-interval [<sampler_idx_list>]

Show: # show sflow

show sflow statistics { receiver | samplers [interface [<samplers_list>] (<port_type> [<v_port_type_list>])] }

3.9.40 (config-if)# shutdown

Syntax: (config-if)# shutdown

Explanation: Shutdown this specific interface.

Negation: (config-if)# no shutdown

Show: # show interface (<port_type> [<v_port_type_list>]) status

3.9.41 (config)# snmp-server

3.9.41.1 (config)# snmp-server

Syntax: (config)# snmp-server

Explanation: Enable SNMP server service.

Example: Enable SNMP server service.

```
# config t
(config)# snmp-server
```

Negation: (config)# no snmp-server

Show: # show snmp

3.9.41.2 (config)# snmp-server access

Syntax: (config)# snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [read <view_name>] [write <write_name>]

Explanation: Configure SNMP access settings.

Parameters:

<group_name>: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

model { v1 | v2c | v3 | any }: Indicates the security model that this entry should belong to. Possible security models are:

any: Any security model accepted(v1|v2c|usm).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

v3: User-based Security Model (USM) for SNMPv3.

level { auth | noauth | priv }: Indicates the security level that this entry should belong to. Possible security models are:

auth: Authentication and no privacy.

noauth: No authentication and no privacy.

priv: Authentication and privacy.

[read <view_name>]: The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

[write <write_name>]: The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Negation: (config)# no snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv }

Show: # show snmp access [<group_name> { v1 | v2c | v3 | any } { auth | noauth | priv }]

3.9.41.3 (config)# snmp-server community v2c

Syntax: (config)# snmp-server community v2c <comm> [ro | rw]

Explanation: Configure Read or Write community string.

Parameters:

<comm>: Indicate a community read or write access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E.

[ro | rw]: Indicates whether the specified community applies to read only access string or read & write access string.

Example: Set Write community access string to private123.

```
# config t
(config)# snmp-server community v2c private124 rw
```

Negation: (config)# no snmp-server community v2c

Show: # show snmp

3.9.41.4 (config)# snmp-server community v3

Syntax: (config)# snmp-server community v3 <v3_comm> [<v_ipv4_addr> <v_ipv4_netmask>]

Explanation: Configure SNMP server community v3 value.

Parameters:

<v3_comm>: Specify SNMPv3 community string.

[<v_ipv4_addr> <v_ipv4_netmask>]: Specify IPv4 address and subnet mask address.

Negation: (config)# no snmp-server community v3 <word127>

Show: # show snmp
show snmp community v3

3.9.41.5 (config)# snmp-server contact

Syntax: (config)# snmp-server contact <v_line255>

Explanation: Configure system contact information.

Parameters:

<v_line255>: Specify system contact information. This could be a person's name, email address or other descriptions. The allowed string length is 0 – 255 and the allowed content is the ASCII characters from 32 – 126.

Example: Set system contact information to “admin@acme.com”

```
# config t
(config)# snmp-server contact admin@acme.com
```

Negation: (config)# no snmp-server contact

3.9.41.6 (config)# snmp-server engine-id local

Syntax: (config)# snmp-server engine-id local <engineID>

Explanation: Configure SNMP server v3 Engine ID value.

Parameters:

<engineID>: Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-F's are not allowed. Changes to the Engine ID will clear all original local users.

Negation: (config)# no snmp-server engine-id local

Show: # show snmp

3.9.41.7 (config)# snmp-server host

Syntax: (config)# snmp-server host <conf_name>

Explanation: Configure SNMP server hostname.

Parameters:

<conf_name: word 32>: Specify a host name. Once “Enter” is pressed, the CLI prompt changes to (config-snmps-host)#.

Example: Set SNMP server hostname to RemoteSnmp

```
# config t
(config)# snmp-server host RemoteSnmp
```

Negation: (config)# snmp-server host <conf_name>

Show: # show snmp host [<conf_name>] [system] [switch] [power] [interface] [aaa]

3.9.41.8 (config)# snmp-server location

Syntax: (config)# snmp-server location <v_line255>

Parameters:

<v_line255>: Specify the descriptive location of this device. The allowed string length is 0 – 255.

Example: Set the location to “Cabinet A22”

```
# config t
(config)# snmp-server location Cabinet A22
```

Negation: (config)# no snmp-server location

3.9.41.9 (config)# snmp-server security-to-group model

Syntax: (config)# snmp-server security-to-group model { v1 | v2c | v3 } name <security_name> group <group_name>

Explanation: Configure SNMPv3 Group settings.

Parameters:

{ v1 | v2c | v3 }: Indicates the security model that this entry should belong to.

<security_name>: A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

<group_name>: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Negation: (config)# no snmp-server security-to-group model { v1 | v2c | v3 } name <security_name>

Show: # show snmp security-to-group [{ v1 | v2c | v3 } <security_name>]

3.9.41.10 (config)# snmp-server trap

Syntax: (config)# snmp-server trap

Explanation: Enable SNMP server trap function.

Example: Enable SNMP server trap function.

```
# config t
(config)# snmp-server trap
```

Negation: (config)# no snmp-server trap

Show: # show snmp

3.9.41.11 (config)# snmp-server user

Syntax: (config)# snmp-server user <username> engine-id <engineID> [{ md5 <md5_passwd> | sha <sha_passwd> } [priv { des | aes } <priv_passwd>]]

Explanation: Configure SNMPv3 User settings.

Parameters:

<username: word 32>: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

engine-id <engineID>: An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it is a remote user.

{ md5 <md5_passwd> | sha <sha_passwd> }: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

md5 <md5_passwd>: An optional flag to indicate that this user uses MD5 authentication protocol. A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32 characters. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters from 0x21 to 0x7E.

sha <sha_passwd>: An optional flag to indicate that this user uses SHA authentication protocol. A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32 characters. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters from 0x21 to 0x7E.

[priv { des | aes } <priv_passwd>]: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

DES: An optional flag to indicate that this user uses DES authentication protocol.

AES: An optional flag to indicate that this user uses AES authentication protocol.

<priv_passwd>: A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Negation: (config)# no snmp-server user <username> engine-id <engineID>

Show: #show snmp user [<username> <engineID>]

3.9.41.12 (config)# snmp-server version

Syntax: (config)# snmp-server version { v1 | v2c | v3 }

Explanation: Configure SNMP server version.

Parameters:

{ v1 | v2c | v3 }: Specify which SNMP server version you want to use.

Example: Set SNMP server version to v3.

```
# config t
(config)# snmp-server version v3
```

Negation: (config)# no snmp-server version

Show: # show snmp

3.9.41.13 (config)# snmp-server view

Syntax: (config)# snmp-server view <view_name> <oid_subtree> { include | exclude }

Explanation: Configure SNMPv3 MIB view name.

Parameters:

<view_name>: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

<oid_subtree>: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128.

{ include | exclude }: Indicates the view type that this entry should belong to. Possible view types are:

included: An optional flag to indicate that this view subtree should be included.

excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

Negation: (config)# no snmp-server view <view_name> <oid_subtree>

Show: # show snmp view [<view_name> <oid_subtree>]

3.9.41.14 (config-if)# snmp-server host <conf_name> traps

Syntax: (config-if)# snmp-server host <conf_name> traps [linkup] [linkdown] [lldp]

Explanation: Configure SNMP trap events for the selected interface.

Parameters:

<conf_name: word 32>: Specify the name of the trap.

traps [linkup] [linkdown] [lldp]: Enable the selected interfaces' trap events.

[linkup]: Port link up trap.

[**linkdown**]: Port link down trap.

[**lldp**]: LLDP (Link Layer Discovery Protocol) trap.

Negation: (config-if)# no snmp-server host <conf_name> traps

3.9.41.15 (config-snmps-host)# host <v_ipv6_ucast>

Syntax: (config-snmps-host)# host <v_ipv6_ucast> [<udp_port>] [traps | informs]

Explanation: Indicates the SNMP trap destination address.

Parameters:

<v_ipv6_ucast>: Specify the IPv6 address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). Also allowed is a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z; a-z), digits (0-9), dot (.) and dash (-). Spaces are not allowed. The first character must be an alpha character, and the first and last characters cannot be a dot or a dash.

[<udp_port>]: Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. The default SNMP trap port is 162.

[traps | informs]: Specify one of the options.

Negation: (config-snmps-host)# no host

3.9.41.16 (config-snmps-host)# host <v_ipv4_ucast>

Syntax: (config-snmps-host)# host { <v_ipv4_ucast> | <v_word45> } [<udp_port>] [traps | informs]

Explanation: Configure the SNMP trap destination IPv4 address.

Parameters:

{ <v_ipv4_ucast> | <v_word45> }: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). Also allowed is a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z; a-z), digits (0-9), dot (.) and dash (-). Spaces are not allowed. The first character must be an alpha character, and the first and last characters cannot be a dot or a dash.

[<udp_port>]: Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. The default SNMP trap port is 162.

[traps | informs]: Specify one of the options.

Negation: (config-snmps-host)# no host

3.9.41.17 (config-snmps-host)# version

Syntax: (config-snmps-host)# version { v1 [<v1_comm>] | v2 [<v2_comm>] | v3 [probe | engineID <v_word10_to_32>] [<securtname>] }

Parameters:

{ v1 [<v1_comm>] | v2 [<v2_comm>] | v3 [probe | engineID <v_word10_to_32>] [<securtname>] }: Specify one of the SNMP versions.

v1 [v1_comm]: Support SNMPv1 and trap community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 0x21 to 0x7E.

v2 [v2_comm]: Support SNMPv2c and trap community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 0x21 to 0x7E.

v3 [probe | engineID <v_word10_to_32>] [<securtname>]: Support SNMPv3.

[probe | engineID <v_word10_to_32>]: Indicates the SNMP trap probe security engine ID or SNMP trap security engine ID. SNMPv3 sends traps and informs use USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

[<securtname>]: Indicates the SNMP trap security name. SNMPv3 traps and informs use USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Explanation: Configure SNMP version and its corresponding values.

Example: Support SNMPv2c version.

```
# config t
(config-snmps-host)# version v2 public
```

Negation: (config-snmps-host)# no version

3.9.41.18 (config-snmps-host)# informs retries

Syntax: (config-snmps-host)# informs retries <retries> timeout <timeout>

Explanation: Configure SNMP trap retry times and timeout.

Parameters:

<retries>: Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

<timeout>: Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

Negation: (config-snmps-host)# no informs

3.9.41.19 (config-snmps-host)# shutdown

Syntax: (config-snmps-host)# shutdown

Parameters: None.

Explanation: Disable the SNMP trap mode.

Example: Disable the SNMP trap mode.

```
# config t
(config-snmps-host)# shutdown
```

Negation: (config-snmps-host)# no shutdown

3.9.41.20 (config-snmps-host)# traps

Syntax: (config-snmps-host)# traps [aaa authentication] [system [coldstart] [warmstart]] [switch [stp] [rmon]]

Explanation: Configure SNMP trap events.

Parameters:

[aaa authentication]: Authentication, Authorization and Accounting. A trap will be issued at any authentication failure.

[system [coldstart] [warmstart]]: The system trap events include the following.

coldstart: The switch has booted from a powered off or due to power cycling (power failure).

warmstart: The switch has been rebooted from an already powered on state.

[switch [stp] [rmon]]: Indicates that the Switch group's traps. Possible traps are:

stp: Enable STP trap.

rmon: Enable RMON trap.

Example: Send a trap notice when any authentication fails.

```
# config t
(config-snmps-host)# traps aaa authentication
```

Negation: (config-snmps-host)# no traps

Show: # show snmp host [<conf_name>] [system] [switch] [interface] [aaa]

3.9.42 (config)# spanning-tree

3.9.42.1 (config)# spanning-tree aggregation

Syntax: (config)# spanning-tree aggregation

Explanation: Enable aggregation mode of Spanning Tree.

```
# config t
(config)# spanning-tree aggregation
(config-stp-aggr) #
```

Show: # show spanning-tree

3.9.42.2 (config-stp-aggr)# spanning-tree

Syntax: (config-stp-aggr)# spanning-tree

Explanation: Enable Spanning Tree under aggregation mode.

Negation: (config-stp-aggr)# no spanning-tree

Show: # show spanning-tree

3.9.42.3 (config-stp-aggr)# spanning-tree auto-edge

Syntax: (config-stp-aggr)# spanning-tree auto-edge

Explanation: Enable auto edge function. When enabled, a port is automatically determined to be at the edge of the network when it receives no BPDUs.

Negation: (config-stp-aggr)# no spanning-tree auto-edge

Show: # show spanning-tree

3.9.42.4 (config-stp-aggr)# spanning-tree bpdu-guard

Syntax: (config-stp-aggr)# spanning-tree bpdu-guard

Explanation: Enable BPDU guard function. This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

Negation: (config-stp-aggr)# no spanning-tree bpdu-guard

Show: # show spanning-tree

3.9.42.5 (config-stp-aggr)# spanning-tree edge

Syntax: (config-stp-aggr)# spanning-tree edge

Explanation: If an interface is attached to end nodes, you can set it to “Edge”.

Negation: (config-stp-aggr)# no spanning-tree edge

Show: # show spanning-tree

3.9.42.6 (config-stp-aggr)# spanning-tree link-type

Syntax: (config-stp-aggr)# spanning-tree link-type { point-to-point | shared | auto }

Explanation: Configure the link type attached to an interface.

Parameters:

{ point-to-point | shared | auto }: Select the link type attached to an interface.

point-to-point: It is a point-to-point connection.

shared: It is a shared medium connection

auto: The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

Negation: (config-stp-aggr)# no spanning-tree link-type

Show: # show spanning-tree

3.9.42.7 (config-stp-aggr)# spanning-tree mst <instance> cost

Syntax: (config-stp-aggr)# spanning-tree mst <instance> cost { <cost> | auto }

Explanation: Configure MSTI and its’ path cost value.

Parameters:

mst <instance: 0-15>: Specify MST instance number. Specify “0” to denote CIST. Specify “1-15” to denote MSTI 1-15.

cost { <cost> | auto }: Specify a Path cost value that is used to determine the best path between devices. Valid values are 1 to 200000000. If “auto” mode is specified, the system automatically detects the speed and duplex mode to decide the path cost. Please note that path cost takes precedence over port priority.

Negation: (config-stp-aggr)# no spanning-tree mst <instance> cost

Show: # show spanning-tree

3.9.42.8 (config-stp-aggr)# spanning-tree mst <instance> port-priority

Syntax: (config-stp-aggr)# spanning-tree mst <instance> port-priority <prio>

Explanation: Configure MSTI and its' port priority.

Parameters:

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1-15.

port-priority <prio>: Specify a port priority value.

Negation: (config-stp-aggr)# no spanning-tree mst <instance> port-priority

Show: # show spanning-tree

3.9.42.9 (config-stp-aggr)# spanning-tree restricted-role

Syntax: (config-stp-aggr)# spanning-tree restricted-role

Explanation: Enable restricted role function. If enabled, this causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority.

Negation: (config-stp-aggr)# no spanning-tree restricted-role

Show: # show spanning-tree

3.9.42.10 (config-stp-aggr)# spanning-tree restricted-tcn

Syntax: (config-stp-aggr)# spanning-tree restricted-tcn

Explanation: Enable restricted TCN function. If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

Negation: (config-stp-aggr)# no spanning-tree restricted-tcn

Show: # show spanning-tree

3.9.42.11 (config)# spanning-tree edge bpdu-filter

Syntax: (config)# spanning-tree edge bpdu-filter

Explanation: Enable edge BPDU filtering function. The purpose of Port BPDU Filtering is to prevent the switch from sending BPDU frames on ports that are connected to end devices.

Example: Enable edge BPDU filtering function.

```
# config t
(config)# spanning-tree edge bpdu-filter
```


Negation: (config)# no spanning-tree edge bpdu-filter

Show: # show spanning-tree

3.9.42.12 (config)# spanning-tree edge bpdu-guard

Syntax: (config)# spanning-tree edge bpdu-guard

Explanation: Enable edge BPDU guard function. Edge ports generally connect directly to PC, file servers or printers. Therefore, edge ports are configured to allow rapid transition. Under normal situations, edge ports should not receive configuration BPDUs. However, if they do, this probably is due to malicious attacks or mis-settings. When edge ports receive configuration BPDUs, they will be automatically set to non-edge ports and start a new spanning tree calculation process.

BPDU Guard is therefore used to prevent the device from suffering malicious attacks. With this function enabled, when edge ports receive configuration BPDUs, STP disables those affected edge ports. After a period of recovery time, those disabled ports are re-activated.

Example: Enable edge BPDU guard function.

```
# config t
(config)# spanning-tree edge bpdu-guard
```

Negation: (config)# no spanning-tree edge bpdu-guard

Show: # show spanning-tree

3.9.42.13 (config)# spanning-tree mode

Syntax: (config)# spanning-tree mode { stp | rstp | mstp }

Parameters:

{ stp | rstp | mstp }: Specify one of the STP protocol versions.

Explanation: Configure the desired STP protocol version.

Example: Set the spanning tree mode to MSTP.

```
# config t
(config)# spanning-tree mode mstp
```

Negation: (config)# no spanning-tree mode

Show: # show spanning-tree

3.9.42.14 (config)# spanning-tree mst <instance> priority <prio>

Syntax: (config)# spanning-tree mst <instance> priority <prio>

Parameters:

<instance: 0-7>: Specify an instance ID. "0" means CIST. "1-7" means MSTI 1-7.

<prio: 0-61440>: Specify a priority value.

Explanation: Specify an appropriate priority for a MSTI instance. Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Note that lower numeric values indicate higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Example: Map MST Instance 1 to priority 61440.

```
# config t
(config)# spanning-tree mst 1 priority 61440
```

Negation: (config)# no spanning-tree mst <instance> priority

Show: # show spanning-tree

3.9.42.15 (config)# spanning-tree mst <instance> vlan <v_vlan_list>

Syntax: (config)# spanning-tree mst <instance> vlan <v_vlan_list>

Parameters:

<instance: 0-7>: Specify an instance ID. "0" means CIST. "1-7" means MSTI 1-7.

<v_vlan_list>: Specify a list of VLANs for the specified MST instance. Separate VLANs with a comma and use hyphen to denote a range of VLANs. (Example: 2,5,20-40)

Explanation: Specify VLANs mapped to a certain MSTI. Both a single VLAN and a range of VLANs are allowed.

Example: Map MST Instance 1 to VLAN 90 and VLAN 101-105.

```
# config t
(config)# spanning-tree mst 1 vlan 90,101-105
```

Negation: (config)# no spanning-tree mst <instance> vlan

3.9.42.16 (config)# spanning-tree mst forward-time

Syntax: (config)# spanning-tree mst forward-time <fwdtime>

Parameters:

<fwdtime: 4-30>: Specify forward delay value between 4 and 30 (seconds).

Explanation: For STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network.

Example: Set the forward delay to 15 seconds.

```
# config t
(config)# spanning-tree mst forward-time 15
```

Negation: (config)# no spanning-tree mst forward-time

Show: # show spanning-tree

3.9.42.17 (config)# spanning-tree mst max-age

Syntax: (config)# spanning-tree mst max-age <maxage> [forward-time <fwdtime>]

Parameters:

<maxage: 6-40>: Specify the max age value. The valid range is from 6 to 40.

[forward-time <fwdtime>]: For STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network. Valid values are 4-30 seconds.

Explanation: If another switch in the spanning tree does not send out a hello packet for a period of time, it is considered to be disconnected. Valid values are 6 to 40 seconds, and Max Age values must be smaller than or equal to (Forward Delay-1)*2.

Example: Set the max age to 20 seconds.

```
# config t
(config)# spanning-tree mst max-age 20
```

Negation: (config)# no spanning-tree mst max-age

Show: # show spanning-tree

3.9.42.18 (config)# spanning-tree mst max-hops

Syntax: (config)# spanning-tree mst max-hops <maxhops>

Parameters:

<maxhops>: Specify the maximum hop count value. The valid range is from 6 to 40.

Explanation: The maximum number of hops allowed for MST region before a BPDU is discarded. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the BPDU is discarded. The default hop count is 20. The allowed range is 6-40.

Example: Set the maximum hop count to 20.

```
# config t
(config)# spanning-tree mst max-hops 20
```

Negation: (config)# no spanning-tree mst max-hops

Show: # show spanning-tree

3.9.42.19 (config)# spanning-tree mst name

Syntax: (config)# spanning-tree mst name <name> revision <v_0_to_65535>

Parameters:

name <name>: Specify a name for this MSTI. By default, the switch's MAC address is used. The maximum length is 32 characters. In order to share spanning trees for MSTI, bridges must have the same configuration name and revision value.

revision <v_0_to_65535>: Specify a revision number for this MSTI. The allowed range is 0 – 65535.

Explanation: Configure a name and revision number for this MSTI.

Negation: (config)# no spanning-tree mst name

Show: # show spanning-tree

3.9.42.20 (config)# spanning-tree recovery interval

Syntax: (config)# spanning-tree recovery interval <interval>

Parameters:

<interval>: The time that has to pass before a port in the error-disabled state can be enabled. The allowed range is 30 – 86400 (seconds).

Explanation: When enabled, a port that is in the error-disabled state can automatically be enabled after a certain time.

Example: Set the spanning tree recovery interval to 50.

```
# config t
(config)# spanning-tree recovery interval 50
```

Negation: (config)# no spanning-tree recovery interval

Show: # show spanning-tree

3.9.42.21 (config)# spanning-tree transmit hold-count

Syntax: (config)# spanning-tree transmit hold-count <holdcount>

Parameters:

<holdcount:1-10>: Specify the transmit hold-count. The allowed transmit hold count is 1 to 10.

Explanation: The number of BPDU sent by a bridge port per second. When exceeded, transmission of the next BPDU will be delayed. By default, it is set to 6. The allowed transmit hold count is 1 to 10. Please note that increasing this value might have a significant impact on CPU utilization and decreasing this value might slow down convergence. It is recommended to remain Transmit Hold Count to the default setting.

Example: Set the spanning tree transmit hold-count to 6.

```
# config t
(config)# spanning-tree transmit hold-count 6
```

Negation: (config)# no spanning-tree transmit hold-count

Show: # show spanning-tree

3.9.42.22 (config-if)# spanning-tree

Syntax: (config-if)# spanning-tree

Explanation: Enable Spanning Tree on this interface.

Negation: (config-if)# no spanning-tree

Show: # show spanning-tree

3.9.42.23 (config-if)# spanning-tree auto-edge

Syntax: (config-if)# spanning-tree auto-edge

Explanation: Enable auto edge function on this interface. When enabled, a port is automatically determined to be at the edge of the network when it receives no BPDUs.

Negation: (config-if)# no spanning-tree auto-edge

Show: # show spanning-tree

3.9.42.24 (config-if)# spanning-tree bpdu-guard

Syntax: (config-if)# spanning-tree bpdu-guard

Explanation: Enable BPDU guard function on this interface. This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

Negation: (config-if)# no spanning-tree bpdu-guard

Show: # show spanning-tree

3.9.42.25 (config-if)# spanning-tree edge

Syntax: (config-if)# spanning-tree edge

Explanation: If an interface is attached to end nodes, you can set it to "Edge".

Negation: (config-if)# no spanning-tree edge

Show: # show spanning-tree

3.9.42.26 (config-if)# spanning-tree link-type

Syntax: (config-if)# spanning-tree link-type { point-to-point | shared | auto }

Explanation: Configure the link type attached to an interface.

Parameters:

{ point-to-point | shared | auto }: Select the link type attached to an interface.

point-to-point: It is a point-to-point connection.

shared: It is a shared medium connection

auto: The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

Negation: (config-if)# no spanning-tree link-type

Show: # show spanning-tree

3.9.42.27 (config-if)# spanning-tree mst <instance> cost

Syntax: (config-if)# spanning-tree mst <instance> cost { <cost> | auto }

Explanation: Configure MSTI and its' path cost value.

Parameters:

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1-15.

cost { <cost> | auto }: Specify a Path cost value that is used to determine the best path between devices. Valid values are 1 to 200000000. If "auto" mode is specified, the system automatically detects the speed and duplex mode to decide the path cost. Please note that path cost takes precedence over port priority.

Negation: (config-if)# no spanning-tree mst <instance> cost

Show: # show spanning-tree

3.9.42.28 (config-if)# spanning-tree mst <instance> port-priority

Syntax: (config-if)# spanning-tree mst <instance> port-priority <prio>

Explanation: Configure MSTI and its' port priority.

Parameters:

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1-15.

port-priority <prio>: Specify a port priority value.

Negation: (config-if)# no spanning-tree mst <instance> port-priority

Show: # show spanning-tree

3.9.42.29 (config-if)# spanning-tree restricted-role

Syntax: (config-if)# spanning-tree restricted-role

Explanation: Enable restricted role function. If enabled, this causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority.

Negation: (config-if)# no spanning-tree restricted-role

Show: # show spanning-tree

3.9.42.30 (config-if)# spanning-tree restricted-tcn

Syntax: (config-if)# spanning-tree restricted-tcn

Explanation: Enable restricted TCN function. If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

Negation: (config-if)# no spanning-tree restricted-tcn

Show: # show spanning-tree

3.9.43 (config-if)# speed

Syntax: (config-if)# speed { 10g | 1000 | 100 | 10 | auto { [10] [100] [1000] } }

Explanation: Configure port speed for this specific interface.

Negation: (config-if)# no speed

Show: # show interface (<port_type> [<v_port_type_list>]) status

3.9.44 (config-if)# switchport

3.9.44.1 (config-if)# switchport access vlan

Syntax: (config-if)# switchport access vlan <pvid>

Explanation: Configure access VLAN ID for this interface.

Parameters:

<pvid>: Indicate the access VLAN ID (PVID) for this interface.

Example: Set the interface 1's access VLAN ID to 10.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# switchport access vlan 10
(config-if)#
```

Negation: (config-if)# no switchport access vlan

Show: # show vlan status

3.9.44.2 (config-if)# switchport forbidden vlan

Syntax: (config-if)# switchport forbidden vlan { add | remove } <vlan_list>

Explanation: Add or remove a port from the forbidden VLAN list.

Parameters:

{ add | remove }: Add or remove this specific interface from the forbidden VLAN list.

<vlan_list>: Specify the VLAN ID.

Negation: (config-if)# no switchport access vlan

Show: > show switchport forbidden [{ vlan <vid> } | { name <name> }]
show switchport forbidden [{ vlan <vid> } | { name <name> }]

3.9.44.3 (config-if)# switchport hybrid acceptable-frame-type

Syntax: (config-if)# switchport hybrid acceptable-frame-type { all | tagged | untagged }

Explanation: Configure the accepted frame types. Available options include “all” (accept all frames), “tagged” (accept only tagged frames), “untagged” (accept only untagged frames). This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, frame type is set to All.

Parameters:

{ all | tagged | untagged }: Specify the frame type for this interface. Available options include “all” (accept all frames), “tagged” (accept only tagged frames), “untagged” (accept only untagged frames).

Negation: (config-if)# no switchport hybrid acceptable-frame-type

Show: # show vlan status

3.9.44.4 (config-if)# switchport hybrid allowed vlan

Syntax: (config-if)# switchport hybrid allowed vlan { all | none | [add | remove | except] <vlan_list> }

Explanation: Configure allowed VLANs when this interface is in hybrid mode.

Parameters:

{ all | none | [add | remove | except] <vlan_list> }: Specify one of the options.

all: All VLANs.

none: No VLANs.

add: Add VLANs to the current list.

remove: Remove VLANs from the current list

except: All VLANs except the following specified in <vlan_list>.

<vlan_list>: Specify the VLAN list.

Negation: (config-if)# no switchport hybrid allowed vlan

Show: # show vlan status

3.9.44.5 (config-if)# switchport hybrid egress-tag

Syntax: (config-if)# switchport hybrid egress-tag { none | all [except-native] }

Explanation: Determines egress tagging of a port.

Parameters:

{ none | all [except-native] }: Determines egress tagging of a port.

none: All VLANs are untagged.

all: All VLANs are tagged.

all [except-native]: All VLANs except the configured PVID will be tagged.

Negation: (config-if)# no switchport hybrid egress-tag

Show: # show vlan status

3.9.44.6 (config-if)# switchport hybrid ingress-filtering

Syntax: (config-if)# switchport hybrid ingress-filtering

Explanation: Enable ingress filtering function on this specific interface. If Ingress Filtering is enabled and the ingress port is not a member of a VLAN, the frame from the ingress port is discarded. By default, ingress filtering is disabled.

Negation: (config-if)# no switchport hybrid ingress-filtering

Show: # show vlan status

3.9.44.7 (config-if)# switchport hybrid native vlan

Syntax: (config-if)# switchport hybrid native vlan <pvid>

Explanation: Configures the VLAN identifier in Hybrid mode for the port. The allowed values are from 1 through 4095. The default value is 1.

Parameters:

<pvid>: Specify the port VLAN ID for this specific interface.

Negation: (config-if)# no switchport hybrid native vlan

Show: # show vlan status

3.9.44.8 (config-if)# switchport hybrid port-type

Syntax: (config-if)# switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }

Explanation: Configures the port type in Hybrid mode for the port.

Parameters:

{ unaware | c-port | s-port | s-custom-port }: There are four port types available. Each port type's ingress and egress action is described in the following table.

Action Port Type	Ingress Action	Egress Action
Unaware	When a tagged frame is received on a port, 1. If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing are also affected by egress rule.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
C-port	When a tagged frame is received on a port, 1. If a tagged frame with TPID=0x8100, it is forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by C-port will be set to 0x8100.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-port	When a tagged frame is received on a port, 1. If a tagged frame with TPID=0x88A8, it is forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TPID of frame transmitted by S-port will be set to 0x88A8
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-custom port	When a tagged frame is received on a port, 1. If a tagged frame with TPID=0x88A8, it is forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TPID of frame transmitted by S-custom-port will be set to a self-customized value, which can be set by the user using the column of Ethertype for Custom S-ports.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	

Negation: (config-if)# no switchport hybrid port-type

Show: # show vlan status

3.9.44.9 (config-if)# switchport mode

Syntax: (config-if)# switchport mode { access | trunk | hybrid }

Explanation: Configure VLAN mode for this specific interface.

Parameters:

{ access | trunk | hybrid }: Specify the VLAN mode.

Negation: (config-if)# no switchport mode

Show: # show vlan status

3.9.44.10 (config-if)# switchport trunk allowed vlan

Syntax: (config-if)# switchport trunk allowed vlan { all | none | [add | remove | except] <vlan_list> }

Explanation: Configure allowed VLANs when this interface is in trunk mode.

Parameters:

{ all | none | [add | remove | except] <vlan_list> }: Specify one of the options.

all: All VLANs.

none: No VLANs.

add: Add VLANs to the current list.

remove: Remove VLANs from the current list

except: All VLANs except the following specified in <vlan_list>.

<vlan_list>: Specify the VLAN list.

Negation: (config-if)# no switchport trunk allowed vlan

Show: # show vlan status

3.9.44.11 (config-if)# switchport trunk native vlan

Syntax: (config-if)# switchport trunk native vlan <pvid>

Explanation: Configure native VLAN ID in trunk mode for this specific interface.

Parameters:

<pvid>: Specify the port VLAN ID for this specific interface.

Negation: (config-if)# no switchport trunk native vlan

Show: # show running-config

3.9.44.12 (config-if)# switchport trunk vlan tag native

Syntax: (config-if)# switchport trunk vlan tag native

Explanation: Configure this specific interface to tag native VLAN traffic.

Negation: (config-if)# no switchport trunk vlan tag native

3.9.44.13 (config-if)# switchport vlan ip-subnet id

Syntax: (config-if)# switchport vlan ip-subnet id <vce_id> <ipv4> vlan <vid>

Explanation: IP Subnet-based VLAN configuration is to map untagged ingress frames to a specific VLAN if the source address is found in the IP subnet-to-VLAN mapping table. When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

Parameters:

<vce_id>: Specify index of the entry. Valid range is 1~128.

<ipv4>: Specify IP address and subnet mask. The format is xx.xx.xx.xx/mm.mm.mm.mm.

<vid>: Indicate the VLAN ID.

Negation: (config-if)# no switchport vlan ip-subnet id <vce_id_list>

Show: # show vlan ip-subnet [id <subnet_id>]

3.9.44.14 (config-if)# switchport vlan mac

Syntax: (config-if)# switchport vlan mac <mac_addr> vlan <vid>

Explanation: This command is to set up VLANs based on source MAC addresses. When ingress untagged frames are received by a port, source MAC address is processed to decide which VLAN these untagged frames belong. When source MAC addresses does not match the rules created, untagged frames are assigned to the receiving port's native VLAN ID (PVID).

Parameters:

<mac_addr>: Indicate the source MAC address. Please note that the source MAC address can only map to one VLAN ID.

vlan <vid>: Map this MAC address to the associated VLAN ID.

Negation: (config-if)# no switchport vlan mac <mac_addr> vlan <vid>

Show: # show vlan mac [address <mac_addr>]

3.9.44.15 (config-if)# switchport vlan protocol group

Syntax: (config-if)# switchport vlan protocol group <grp_id> vlan <vid>

Explanation: Configure VLAN protocol group for this specific interface.

Parameters:

<grp_id: word 16>: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

<vid>: Specify the VLAN ID that applies to this rule.

Negation: (config-if)# no switchport vlan protocol group <grp_id> vlan <vid>

Show: # show vlan protocol [eth2 { <etype> | arp | ip | ipx | at }] [snap { <oui> | rfc-1042 | snap-8021h } <pid>] [llc <dsap> <ssap>]

3.9.44.16 (config-if)# switchport voice vlan discovery-protocol

Syntax: (config-if)# switchport voice vlan discovery-protocol { oui | lldp | both }

Explanation: Configure a method for detecting VoIP traffic. By default, OUI is used.

Parameters:

oui: Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to manufacturers and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.

lldp: Use LLDP (IEEE 802.1ab) to discover VoIP devices attached to a port. LLDP checks that the “telephone bit” in the system capability TLV is turned on or not.

both: Use both OUI table and LLDP to detect VoIP traffic on a port.

Negation: (config-if)# no switchport voice vlan discovery-protocol

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.9.44.17 (config-if)# switchport voice vlan mode

Syntax: (config-if)# switchport voice vlan mode { auto | force | disable }

Explanation: Configure Voice VLAN mode on a per port basis.

Parameters:

auto: Enable the Voice VLAN auto detection mode. When voice (VoIP) traffic is detected on a port, the port will be added as a tagged member to the Voice VLAN. When Auto mode is selected, you need to further decide a method for detecting voice traffic in “Discovery Protocol” field, either OUI or LLDP (802.1ab).

force: Enable Voice VLAN feature on a particular port.

disabled: Disable Voice VLAN feature on a particular port.

Negation: (config-if)# no switchport voice vlan mode

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.9.44.18 (config-if)# switchport voice vlan security

Syntax: (config-if)# switchport voice vlan security

Explanation: Enable security filtering feature on a per port basis. When enabled, any non-VoIP packets received on a port with Voice VLAN ID will be discarded. VoIP traffic is identified by source MAC addresses configured in the telephony OUI list or through LLDP which is used to discover VoIP devices attached to the switch.

Negation: (config-if)# no switchport voice vlan security

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.9.45 (config)# tacacs-server

3.9.45.1 (config)# tacacs-server timeout

Syntax: (config)# tacacs-server timeout <seconds>

Explanation: The time the switch waits for a reply from a TACACS+ server before it retransmits the request.

Parameters:

<seconds:1-1000>: Specify a value for timeout. The allowed timeout range is between 1 and 1000.

Negation: (config)# no tacacs-server timeout

Show: # show tacacs-server

3.9.45.2 (config)# tacacs-server deadtime

Syntax: (config)# tacacs-server deadtime <minutes>

Explanation: Deadtime is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Parameters:

<minutes:1-1440>: Specify a value for tacacs-server deadtime. The allowed deadtime range is between 1 to 1440 minutes.

Negation: (config)# no tacacs-server deadtime

Show: # show tacacs-server

3.9.45.3 (config)# tacacs-server key

Syntax: (config)# tacacs-server key <key>

Explanation: Specify the secret key up to 63 characters. This is shared between a TACACS+ sever and the switch.

Parameters:

<key:1-63>: Specify a shared secret key value.

Negation: (config)# no tacacs-server key

Show: # show tacacs-server

3.9.45.4 (config)# tacacs-server host

Syntax: (config)# tacacs-server host <host_name> [port <port>] [timeout <seconds>] [key <key>]

Explanation: Configure radius server settings.

Parameters:

<host_name>: Specify a hostname or IP address for the TACACS+ server.

[port <port>]: Specify the TCP port number to be used on a TACACS+ server for authentication.

[timeout <seconds>]: If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

[key <key>]: If secret key is specified here, it will replace the global secret key. If you prefer to use the global value, leave this field blank.

Negation: (config)# no tacacs-server host <host_name> [port <port>]

Show: # show tacacs-server

3.9.46 (config)# udld

3.9.46.1 (config)# udld

Syntax: (config)# udld { aggressive | enable | message time-interval <v_interval> }

Explanation: Configure all ports to UDLD aggressive mode or normal mode and set up message interval. UDLD (Unidirectional Link Detection) protocol can monitor the physical configuration of the links between devices and ports that support UDLD. UDLD can perform tasks that auto-negotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When you enable both auto-negotiation and UDLD, Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols. UDLD works by exchanging protocol packets between the neighboring devices. In order for UDLD to work, both devices on the link must support UDLD and have it enabled on respective ports.

Parameters:

{ aggressive | enable | message time-interval <v_interval> }: Specify one of the options:

aggressive: Set all ports to Aggressive mode. In aggressive mode, if the link state of the port is determined to be bi-directional and the UDLD information times out while the link on the port is still up, UDLD tries to re-establish the state of the port. If not successful, the port is put into the errdisable state.

enable: Set all ports to Normal mode. In normal mode, if the link state of the port was determined to be bi-directional and the UDLD information times out, no action is taken by UDLD. The port state for UDLD is marked as undetermined. The port behaves according to its STP state.

message time-interval <v_interval>: Specify message interval value. The valid interval range is 7~90 seconds. Aging of UDLD information happens when the port that runs UDLD does not receive UDLD packets from the neighbor port for duration of hold time. The hold time for the port is dictated by the remote port and depends on the message interval at the remote side. The shorter the message interval, the shorter the hold time and the faster the detection.

Negation: (config)# no udld { aggressive | enable }

Show: # show udld [interface (<port_type> [<plist>])]

3.9.46.2 (config-if)# udld port

Syntax: (config-if)# udld port [aggressive] [message time-interval <v_interval>]

Explanation: Configure the specified ports to UDLD aggressive mode or normal mode and set up message interval. UDLD (Unidirectional Link Detection) protocol can monitor the physical configuration of the links between devices and ports that support UDLD. UDLD can perform tasks that auto-negotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When you enable both auto-negotiation and UDLD, Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols. UDLD works by exchanging protocol packets between the neighboring devices. In order for UDLD to work, both devices on the link must support UDLD and have it enabled on respective ports.

Parameters:

[aggressive]: Set the specified ports to Aggressive mode. In aggressive mode, if the link state of the port is determined to be bi-directional and the UDLD information times out while the link on the port is still up, UDLD tries to re-establish the state of the port. If not successful, the port is put into the errdisable state.

[message time-interval <v_interval>]: Specify message interval value. The valid interval range is 7~90 seconds. Aging of UDLD information happens when the port that runs UDLD does not receive UDLD packets from the neighbor port for duration of hold time. The hold time for the port is dictated by the remote port and depends on the message interval at the remote side. The shorter the message interval, the shorter the hold time and the faster the detection.

Negation: (config)# no udld port

Show: # show udld [interface (<port_type> [<plist>])]

3.9.47 (config)# upnp

3.9.47.1 (config)# upnp

Syntax: (config)# upnp

Explanation: Enable upnp operation.

Example: Enable upnp operation

```
# config t
(config)# upnp
(config)#
```

Negation: (config)# no upnp

Show: # show upnp

3.9.47.2 (config)# upnp advertising-duration

Syntax: (config)# upnp advertising-duration <v_100_to_86400>

Parameters:

<v_100_to_86400>: Specify the advertising duration. The allowed range is 100 to 86400 (seconds).

Explanation: This defines how often an UPnP advertisement is sent. The duration is carried in Simple Service Discover Protocol (SSDP) packets which informs a control point how often it should receive a SSDP advertisement message from the switch. By default, the advertising duration is set to 100 seconds. However, due to the unreliable nature of UDP, it is recommended to set to the shorter duration since the shorter the duration, the fresher is UPnP status.

Example: Set the upnp advertising duration to 150 seconds.

```
# config t
(config)# upnp advertising-duration 150
```

Negation: (config)# no upnp advertising-duration

Show: # show upnp

3.9.47.3 (config)# upnp ttl

Syntax: (config)# upnp ttl <v_1_to_255>

Parameters:

<v_1_to_255>: Specify the ttl (time to live) value. The allowed range is 1 to 255.

Explanation: TTL (Time to live) is used to configure how many steps an UPnP advertisement can travel before it disappears.

Example: Set the upnp ttl value to 10.

```
# config t
(config)# upnp ttl 10
```

Negation: (config)# no upnp ttl

Show: # show upnp

3.9.48 (config)# username

3.9.48.1 (config)# username<username>privilege<priv>password encrypted

Syntax: (config)# username <username> privilege <priv> password encrypted <encry_password>

Explanation: By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account.

Parameters:

username <username: word31>: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

password encrypted <encry_password: 4-44>: Specify the encrypted password for this new user account. The ENCRYPTED (hidden) user password. Notice the ENCRYPTED password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

Example: Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password encrypted jack30125
```

Negation: (config)# no username <username>

Show: > show users
show users

3.9.48.2 (config)# username<username>privilege<priv>password none

Syntax: (config)# username <username> privilege <priv> password none

Explanation: By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account without password

Parameters:

username <username: word31>: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

password none: No password for this user account.

Example: Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password none
```

Negation: (config)# no username <username>

Show: > show users
show users

3.9.48.3 (config)# username<username>privilege<priv>password unencrypted

Syntax: (config)# username <username> privilege <priv> password unencrypted <password>

Explanation: By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account with unencrypted password.

Parameters:

username <username: word31>: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

password unencrypted <password: line31>: Specify the unencrypted password for this user account. The UNENCRYPTED (Plain Text) user password. Any printable characters including space is accepted.

Example: Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password unencrypted jack30125
```

Negation: (config)# no username <username>

Show: > show users
show users

3.9.49 (config)# vlan

3.9.49.1 (config)# vlan

Syntax: (config)# vlan <vlist>

Explanation: Configure allowed VLANs.

Parameters:

<vlist>: This shows the allowed access VLANs. This setting only affects ports set in “Access” mode. Ports in other modes are members of all VLANs specified in “Allowed VLANs” field. By default, only VLAN 1 is specified. More allowed access VLANs can be entered by specifying the individual VLAN ID separated by comma. If you want to specify a range, separate it by a dash. For example, 1, 5,10,12-15,100. Once Enter is pressed, the prompt changes to (config-vlan)#

Example: Add VID 1,5,10,12-15,100 to the allowed VLAN list.

```
# config t
(config)# vlan 1,510,12-15,100
(config-vlan)#
```

Negation: (config)# no vlan { { ethertype s-custom-port } | <vlan_list> }

3.9.49.2 (config)# vlan ethertype s-custom-port

Syntax: (config)# vlan ethertype s-custom-port <etype>

Explanation: Configure ether type used for customer s-ports.

Parameters:

ethertype s-custom-port <etype>: Specify ether type used for customer s-ports. The valid range is 0x0600 to 0xffff.

Example: Set ether type for customer s-port to 0x88a8.

```
# config t
(config)# vlan ethertype s-custom-port 0x88a8
```

Negation: (config)# no vlan { { ethertype s-custom-port } | <vlan_list> }

3.9.49.3 (config)# vlan protocol

Syntax: (config)# vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>

Explanation: The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the

devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Parameters:

`protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } }`: There are three frame types available for selection; these are “Ethernet”, “SNAP”, and “LLC”. The value field will need to be changed accordingly.

eth2 (Ethernet): Ether Type (etype) value. By default, it is set to 0x0800. The range allowed is 0x0600 to 0xffff.

SNAP: This includes OUI (Organizationally Unique Identifier) and PID (Protocol ID) values.

OUI: A value in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value in the ranges of 0x00-0xff.

PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

LLC (Logical Link Control): This includes DSAP (Destination Service Access Point) and SSAP (Source Service Access Point) values. By default, the value is 0xff. Valid range is 0x00 to 0xff.

group <grp_id>: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

Example: Set VLAN protocol to eth2 0x88a8.

```
# config t
(config)# vlan protocol eth2 0x88a8 group a12
```

Negation: `(config)# no vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>`

Show: `# show vlan protocol [ eth2 { <etype> | arp | ip | ipx | at } ] [ snap { <oui> | rfc-1042 | snap-8021h } <pid> ] [ llc <dsap> <ssap> ]`

3.9.50 (config)# voice vlan

3.9.50.1 (config)# voice vlan

Syntax: `(config)# voice vlan`

Explanation: Enable voice vlan for voice traffic.

Negation: `(config)# no voice vlan`

Show: `# show voice vlan [ oui <oui> | interface ( <port_type> [ <port_list> ] ) ]`

3.9.50.2 (config)# voice vlan aging-time

Syntax: (config)# voice vlan aging-time <aging_time>

Explanation: Set voice vlan secure learning aging time.

Parameters:

<AgingTime : 10-10000000>: Specify voice vlan learning aging time. The allowed range is 10-10000000.

Negation: (config)# no voice vlan aging-time

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.9.50.3 (config)# voice vlan class

Syntax: (config)# voice vlan class { <traffic_class> | low | normal | medium | high }

Explanation: Set voice vlan secure learning aging time.

Parameters:

{ <traffic_class> | low | normal | medium | high }: Specify voice vlan class value or prioritize voice vlan.

<traffic_class: 0-7>: Specify voice vlan class value. The valid value is 0~7.

Negation: (config)# no voice vlan class

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.9.50.4 (config)# voice vlan oui <oui> [description <description>]

Syntax: (config)# voice vlan oui <oui> [description <description>]

Explanation: Set voice vlan secure learning aging time.

Parameters:

<oui>: Specify OUI value.

[description <description>]: Enter the description for this OUI.

Negation: (config)# no voice vlan oui <oui>

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.9.50.5 (config)# voice vlan vid

Syntax: (config)# voice vlan vid <vid>

Explanation: Set voice VLAN ID.

Parameters:

<vid>: Specify voice VLAN ID.

Negation: (config)# no voice vlan vid

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.9.51 (config)# web privilege group

Syntax: (config)# web privilege group <group_name> level { [configRoPriv <configRoPriv>] [configRwPriv <configRwPriv>] [statusRoPriv <statusRoPriv>] [statusRwPriv <statusRwPriv>] }*1

Parameters:

group <group_name>: This name identifies the privilege group. Valid words are 'Aggregation' 'DHCP' 'Debug' 'Dhcp_Client' 'Diagnostics' 'ETH_LINK_OAM' 'IP2' 'IPMC_Snooping' 'LACP' 'LLDP' 'Loop_Protect' 'MAC_Table' 'MEP' 'MVR' 'Maintenance' 'NTP' 'Ports' 'Private_VLANs' 'QoS' 'Security' 'Spanning_Tree' 'System' 'Timer' 'UPnP' 'VCL' 'VLAN_Translation' 'VLANs' 'Voice_VLAN'.

level { [configRoPriv <configRoPriv>] [configRwPriv <configRwPriv>] [statusRoPriv <statusRoPriv>] [statusRwPriv <statusRwPriv>] }*1: Every group has an authorization Privilege level for the following sub groups:

configRoPriv (configuration read-only): The privilege level is 1 to 15.

configRwPriv (configuration/execute read-write): The privilege level is 1 to 15.

statusRoPriv (status/statistics read-only): The privilege level is 1 to 15.

statusRwPriv (status/statistics read-write): The privilege level is 1 to 15.

User Privilege should be the same or greater than the authorization Privilege level to have access to that group.

Explanation: Assign Aggregation group to configRwPriv (configuration/excute read-write) level 15.

```
# config t
(config)# web privilege group aggregation level configRwPriv 15
```

Negation: (config)# no web privilege group <group_name> level

Show: > show web privilege group <group_name> level
show web privilege group <group_name> level

CHAPTER 4. WEB OPERATION & CONFIGURATION

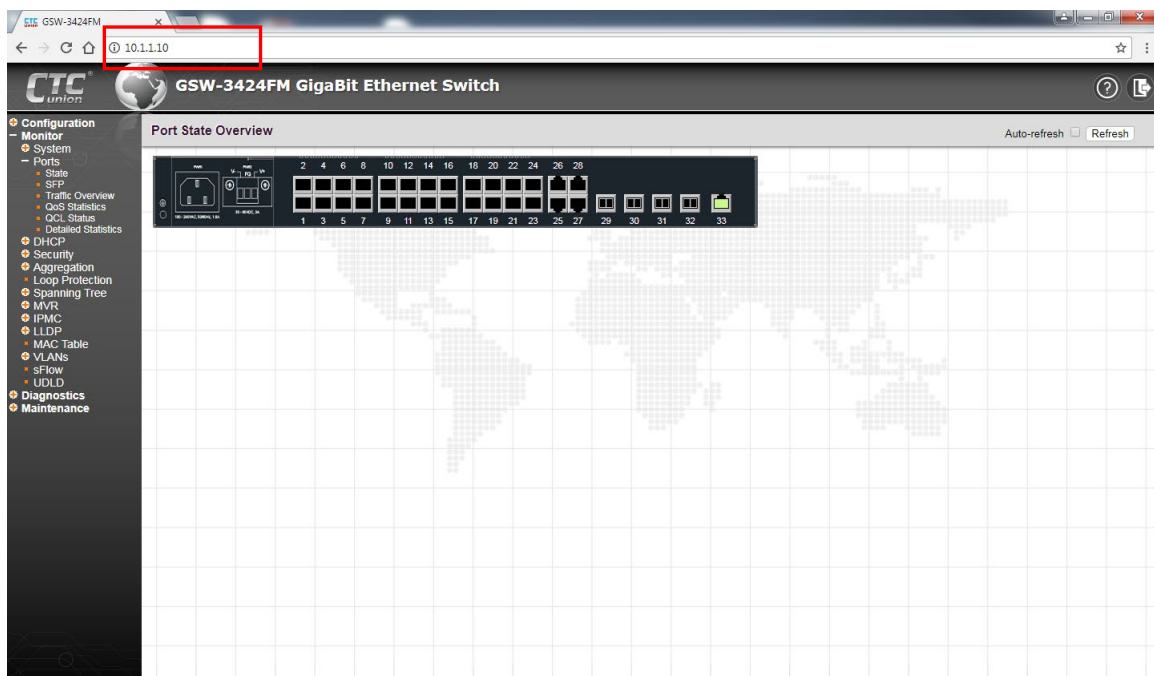
CGR-3291-NA2A provides a wide range of basic and advanced management functions that can help network engineers to design and implement their own network. The user can manage CGR-3291-NA2A via the console port or using Web interface. For the first-time users who want to use the Web interface, it is very important to know how to connect the device correctly so as to successfully access the device.

4.1 Web Management Interface Connection & Login

CGR-3291-NA2A provides one MGMT port on the front panel for accessing Web Management via IP connectivity. For the first time user, connect one end of RJ-45 cable to the CGR-3291-NA2A and the other end of RJ-45 cable to your management PC. Then, open the web browser such as IE, Firefox, etc and input **the default IP address 10.1.1.1**. Then, a standard login prompt will appear depending on the type of browser used. The example below is with Firefox browser.



Enter the factory default username “**admin**” with “**no password**”. After successfully entering the web based management, the Port State page will appear.



Web Home Page

4.2 Icons & Buttons

This switch provides some basic and frequently-used functions as icons on the top of Web management page. You can use these icons for a quick help or logout.

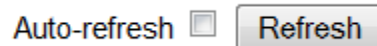
4.2.1 Port Status

The initial page, when logged in, displays a graphical overview of the port status for all optical ports. For port 1 to port 28, the "Yellow" colored port indicates a connection with a speed of 1000M; whereas, the "Green" colored port indicates a connection with a speed of 100M. For port 29 to port 32, the "Orange" colored port indicates a connection with a speed of 1000M; whereas, the "Blue" colored port indicates a connection speed of 10G.

The status display can be reached by using the left side menu, and return to **Monitor>Ports>State**.

4.2.2 Refresh

To update the screen, click the "Refresh" button. For automatic updating of the screen, the "Auto-refresh" tick box may be ticked. The screen will be auto refreshed every 3 seconds.



Unless connected directly on a local LAN, we recommend not using the auto-refresh function as it does generate a bit of traffic.

4.2.3 Help System

The switches have an online "help" system to aid the engineer when setting the parameters of the device. Each functional setting page is accompanied by a specific "help" for that functional page. The user can display this help "pop up" at any time by clicking the "help" icon.

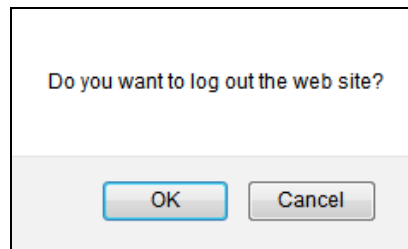


4.2.4 Logout

After completing configuration, we recommend logging out of the web GUI. This is easily accomplished by clicking the logout icon.



After clicking the logout icon, a confirmation screen will be displayed. Click "OK" to finish logging out or click "Cancel" to return to the web configuration GUI.



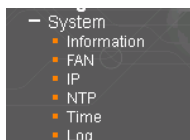
For the remainder of this section, each menu item will be explained one by one, in order as they descend down the menu screen, starting with the "System" menu.

4.3 Configuration

This section offers explanations for both basic and advanced management functions available in CGR-3291-NA2A. They are introduced below individually in separate sub-sections.

4.3.1 System

The configurations under the "System" menu include device settings such as IP address, time server, etc.



4.3.1.1 System Information Configuration

The configuration information entered here will be reported in the standard SNMP MIB2 for 'sysContact' (OID 1.3.6.1.2.1.1.4), 'sysName' (OID 1.3.6.1.2.1.1.5) and 'sysLocation' (OID 1.3.6.1.2.1.1.6). Remember to click the "Save" button after entering the configuration information.

A screenshot of a web form titled "System Information Configuration" in a purple header bar. Below the title is a table with three rows. The first row has "System Contact" and "admin@acme.com". The second row has "System Name" and "AccessSW". The third row has "System Location" and "cabinet A22". Below the table are two buttons: "Save" and "Reset".

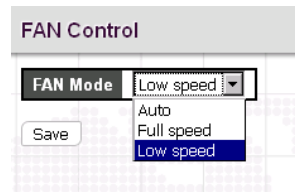
System Information Configuration	
System Contact	admin@acme.com
System Name	AccessSW
System Location	cabinet A22
Save Reset	

System Contact: Indicate the descriptive contact information. This could be a person's name, email address or other descriptions. The allowed string length is 0 – 255 and the allowed content is the ASCII characters from 32 – 126.

System Name: Indicate the hostname for this device. Alphabets (A-Z; a-z), digits (0-9) and minus sign (-) can be used. However, space characters are not allowed. The first character must be an alphabet character. The first and last character must not be a minus sign. The allowed string length is 0 – 255.

System Location: Indicate the location of this device. The allowed string length is 0 – 255.

4.3.1.2 Fan



FAN Mode: This drop-down menu adjusts fan speed of the device.

Auto: The fan speed is adjusted automatically depending on the current temperature of the device.

Full Speed: The fan operates in full speed. Check current revolutions of per minutes (RPM) in **Monitor > System > Power & Fan** section.

Low Speed: This mode slows down the fan speed. Check current revolutions of per minutes (RPM) in **Monitor > System > Power & Fan** section.

4.3.1.3 System IP

Setup the IP configuration, interface and routes.

IP Configuration

Domain Name	No Domain Name	
Mode	Host	
DNS Server 0	No DNS server	
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	☐	

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		Enable	DHCPv6		IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length		Rapid Commit	Current Lease	Address	Mask Length
☐	1	☐	0		192.168.0.1	24	☐	☒			

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
Delete				0

Add Route

Save Reset

IP Configuration

Domain Name: This setting controls the DNS name resolution done by the switch. The following modes are supported:

No Domain Name: No DNS server will be used.

Configured Domain Name: Explicitly provide the IP address of the DNS Server in dotted decimal notation.

From any DHCP interfaces: The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.

From this DHCP interface: Specify from which DHCP-enabled interface a provided DNS server should be preferred.

Mode: This pull-down menu configures whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces. When configuring this device for multiple VLANs, the Router mode should be chosen. Router mode is the default mode.

DNS Server: This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. The following modes are supported:

No DNS server: No DNS server will be used.

Configured IPv4: Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.

Configured IPv6: Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server. Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service.

From any DHCPv4 interfaces: The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.

From this DHCPv4 interface: Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.

From any DHCPv6 interfaces: The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.

From this DHCPv6 interface: Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.

DNS Proxy: When DNS proxy is enabled, the system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.

IP Interface

Click "Add Interface" to add a new IP interface. A maximum of 8 interfaces is supported.

VLAN: This is the VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

DHCPv4 Enable: When this checkbox is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

Fallback: The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables fallback mechanism. The DHCP will keep retrying until a valid lease is obtained when fallback is disabled. Valid value is from 0 to 4294967295.

IPv4 Current Lease: For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv4 Address: The IPv4 address of the interface is entered in dotted decimal notation. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

IPv4 Mask Length: The IPv4 network mask is entered by a number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

DHCPv6 Enable: When this checkbox is enabled, the system will configure the IPv6 address and mask of the interface using the DHCP protocol.

Rapid Commit: If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received. This option is only manageable when DHCPv6 client is enabled.

IPv6 Current Lease: For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv6 Address: A IPv6 address is a 128-bit record represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ::192.1.2.34. The field may be left blank if IPv6 operation on the interface is not desired.

IPv6 Mask Length: The IPv6 network mask is entered by a number of bits (prefix length). Valid values are between 1 and 128 bits for an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

IP Routes

Route Network: The IP route is the destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or for IPv6 use the :: notation.

Route Mask: The route mask is a destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

Gateway: This is the IP address of the gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.

Next Hop VLAN (Only for IPv6): The VLAN ID of the specific IPv6 interface associated with the gateway. The given VID ranging from 1 to 4095 will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not link-local, the device will ignore the next hop VLAN for the gateway.

4.3.1.4 System NTP

Setup the Network Time Protocol configuration, to synchronize this device's clock to network time.

NTP Configuration	
Mode	Enabled
Server 1	59.124.196.83
Server 2	168.95.1.12
Server 3	210.68.16.24
Server 4	
Server 5	
Save Reset	

Mode: Configure the NTP mode operation. Possible modes are:

Enabled: Enable NTP client mode operation.

Disabled: Disable NTP client mode operation.

Server #: Enter the IPv4 or IPv6 address of an NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. NTP servers can also be represented by a legally valid IPv4 address. For example, '::192.1.2.34'. The NTP servers are tried in numeric order. If 'Server 1' is unavailable, the NTP client will try to contact 'Server 2'.

4.3.1.5 System Time

Setup the device time.

Time Zone Configuration	
Time Zone	(GMT-05:00) Eastern Time (US and Canada) ▼
Acronym	EST (0 - 16 characters)

Daylight Saving Time Configuration	
Daylight Saving Time Mode	
Daylight Saving Time	Recurring ▼
Start Time settings	
Week	2 ▼
Day	Sun ▼
Month	Mar ▼
Hours	2 ▼
Minutes	0 ▼
End Time settings	
Week	1 ▼
Day	Sun ▼
Month	Nov ▼
Hours	2 ▼
Minutes	0 ▼
Offset settings	
Offset	60 (1 - 1440) Minutes

The setting example above is for Eastern Standard Time in the United States. Daylight savings time starts on the second Sunday in March at 2:00AM. Daylight savings ends on the first Sunday in November at 2:00AM. The daylight savings time offset is 60 minutes (1 hour).

Time Zone Configuration

Time Zone: Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.

Acronym: Set the acronym of the time zone.

Daylight Saving Time Configuration

Daylight Saving Time: This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select "Disable" to disable the Daylight Saving Time configuration. Select

“Recurring” and configure the Daylight Saving Time duration to repeat the configuration every year. Select “Non-Recurring” and configure the Daylight Saving Time duration for single time configuration. (Default is Disabled)

Recurring & Non-Recurring Configurations:

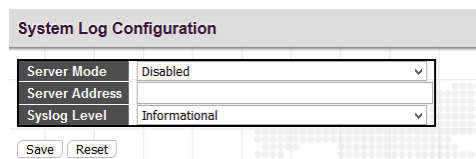
Start time settings: Select the starting week, day, month, year, hours, and minutes.

End time settings: Select the ending week, day, month, year, hours, and minutes.

Offset settings: Enter the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

4.3.1.6 System Log Configuration

Configure System Log on this page.



System Log Configuration	
Server Mode	Disabled
Server Address	
Syslog Level	Informational
Save Reset	

Server Mode: This sets the server mode operation. When the mode of operation is enabled, the syslog message will send out to syslog server (at the server address). The syslog protocol is based on UDP communication and received on UDP port 514. Syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out, even if the syslog server does not exist. When the mode of operation is disabled, no syslog packets are sent out.

Server Address: This sets the IPv4 host address of syslog server. If the switch provides DNS feature, it also can be a host name.

Syslog Level: This sets what kind of messages will send to syslog server. Possible levels are:

Error: Send specific messages which severity code is less or equal than Error (3).

Warning: Send specific messages which severity code is less or equal than Warning (4).

Notice: Send specific messages which severity code is less or equal than Notice (5).

Informational: Send specific messages which severity code is less or equal than Informational (6).

4.3.2 Power Saving

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE was developed through the IEEE802.3az task force of the Institute of Electrical and Electronic Engineers (IEEE).

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is called wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP (Link Layer Discovery Protocol) protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode. For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic. For traffic that should not be held back, urgent queues may be assigned to reduce latency yet still result in overall power saving.

4.3.2.1 Configuration

Configure EEE (Energy-Efficient Ethernet) as well as Ethernet power savings.

Port Power Savings Configuration		
Port Configuration		
Port	ActiPHY	PerfectReach
*	☐	☐
1	☐	☐
2	☐	☐
3	☐	☐
4	☐	☐
5	☐	☐
6	☐	☐
7	☐	☐
8	☐	☐
9	☐	☐
10	☐	☐
11	☐	☐
12	☐	☐
13	☐	☐
14	☐	☐
15	☐	☐
16	☐	☐
17	☐	☐
18	☐	☐
19	☐	☐
20	☐	☐
21	☐	☐
22	☐	☐
23	☐	☐
24	☐	☐
25	☐	☐
26	☐	☐
27	☐	☐

ActiPHY™: ActiPHY™ works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if an Ethernet cable is inserted. For ports with no cable connection, the PHY remains powered down to save energy.

PerfectReach™: PerfectReach™ is another power saving mechanism. PerfectReach™ works by determining the cable length and lowering the Ethernet transmit power for ports with short cables.

4.3.3 Ports

This page displays current port configurations and allows some configuration here.

Port Configuration

Refresh

Port	Description	Link	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
			Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
1		● Down	<>	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240	<> ▼	□
2		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
3		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
4		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
5		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
6		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
7		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
8		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
9		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
10		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
11		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
12		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
13		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
14		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
15		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
16		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
17		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
18		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
19		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
20		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
21		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
22		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
23		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
24		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
25		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240	Discard ▼	□
26		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240	Discard ▼	□
27		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240	Discard ▼	□
28		● Down	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240	Discard ▼	□
29		● Down	10Gbps FDX	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
30		● Down	10Gbps FDX	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
31		● Down	10Gbps FDX	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
32		● Down	10Gbps FDX	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240		□
33		● 1Gtdx	Auto	▼	✓	✓	✓	✓	✓	✓	✗	✗	✗	0-7	10240	Discard ▼	□

SaveReset

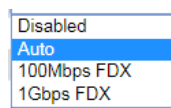
Port: The number of each port.

Description: Specify an alternate and descriptive name for a given port. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z; a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The allowed string length is 0 to 40.

Link: The current link state for each port is displayed graphically. Green indicates the link is up and red indicates that it is down.

Current Speed: This column provides the current link speed and duplex mode (Auto, 100Mbps FDX, 1Gbps FDX) of each port.

Configured Speed: This pull down selects any available link speed for the given switch port. Only speeds supported by the specific port are shown.



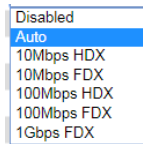
Possible fiber port settings are:

Disabled - Disables the switch port operation.

Auto - Port auto negotiating speed with the link partner, selecting the highest speed that is compatible with the link partner and negotiating the duplex mode.

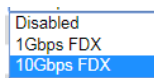
100Mbps FDX - Forces the port to 100Mbps full duplex mode.

1Gbps FDX - Forces the port to 1Gbps full duplex



Possible copper port settings are:

- Disabled - Disables the switch port operation.
- Auto nego - Port auto negotiating speed with the link partner, selecting the highest speed that is compatible with the link partner.
- 10Mbps HDX: Forces the port to 10Mbps half duplex mode.
- 10Mbps FDX: Forces the port to 10Mbps full duplex mode.
- 100Mbps HDX: Forces the port to 100Mbps half duplex mode.
- 100Mbps FDX: Forces the port to 100Mbps full duplex mode.
- 1Gbps FDX: Forces the port to 1Gbps full duplex.



Possible uplink port settings are:

- Disabled - Disables the switch port operation.
- 1Gbps FDX: Forces the port to 1Gbps full duplex.
- 10Gbps FDX: Forces the port to 10Gbps full duplex.

Flow Control: The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is also related to the setting for Configured Link Speed.

PFC: When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the Priority field, range (one or more) of priorities can be configured, for example: '0-3,7' which equals '0,1,2,3,7'. PFC is not supported through auto negotiation. PFC and Flowcontrol cannot both be enabled on the same port.

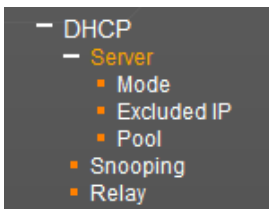
Maximum Frame Size: Enter the maximum frame size allowed for the switch port, including FCS. This switch supports up to 9600 byte packets.

Excessive Collision Mode: This setting configures the port transmit collision behavior to either "Discard" (Discard frame after 16 collisions - default) or to "Restart" (Restart backoff algorithm after 16 collisions).

Frame Length Check: This setting configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch

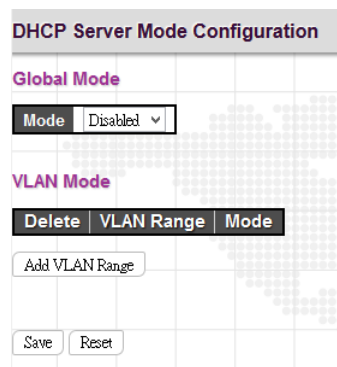
4.3.4 DHCP

The configurations under the "DHCP" menu include DHCP Server, DHCP Snooping and DHCP Relay.



4.3.4.1 Server

4.3.4.1.1 Mode



Global Mode

Mode: Enable or disable DHCP server mode. When enabled, this device can act as a DHCP server and provide IP address to clients that request for one.

VLAN Mode

Click "Add VLAN Range" to create a new entry.

VLAN Range: Enter the VLAN Range in which DHCP server is enabled or disabled. The starting VLAN ID must be smaller than or equal to the ending VLAN ID. If there is only one VLAN ID, then it can be entered either in starting or ending VLAN ID field.

Mode: Indicates the operation mode per VLAN.

Enabled: Enable DHCP server per VLAN.

Disabled: Disable DHCP server per VLAN.

NOTE: If you would like to disable DHCP server on an existing VLAN range, then follow the steps below.

1. Add one "Add VLAN Range" entry.
 2. Enter the VLAN range that you want to disable.
 3. Choose "Disabled" mode.
 4. Click "Save" to apply the change.
-

4.3.4.1.2 Excluded IP

Delete	IP Range
Delete	-

Add IP Range

Save Reset

Click “Add IP Range” to set up IP pool range.

IP Range: Enter the starting and ending IP address that are not allocated to DHCP clients. The starting IP address must be smaller or equal to the ending IP address. If there is only one excluded IP address, it can be entered either in starting or ending IP address field. The total Excluded IP address ranges can be supported is 16.

4.3.4.1.3 Pool

Delete	Name	Type	IP	Subnet Mask	Lease Time
Delete	-	-	-	-	1 days 0 hours 0 minutes

Add New Pool

Save Reset

Click “Add New Pool” to add a new entry to the list. The maximum entries supported are 640.

Name: Enter the pool name for this entry. All printable characters are supported except white space. Click on the pool name after save to configure its detailed settings.

Type: Display which type the pool is. The displayed options include Network and Host. If “-” is displayed, it means this field has not been defined yet.

IP: Display network number of the DHCP address pool. If “-” is displayed, it means this field has not been defined yet.

Subnet Mask: Display subnet mask of the DHCP address pool. If “-” is displayed, it means this field has not been defined yet.

Lease Time: Display the lease time of the configured pool.

Click on the pool name to configure its detailed settings.

DHCP Pool Configuration	
Pool	
Name	1
Setting	
Pool Name	1
Type	None
IP	
Subnet Mask	
Lease Time	1 days (0-365) 0 hours (0-23) 0 minutes (0-59)
Domain Name	
Broadcast Address	
Default Router	
DNS Server	
NTP Server	

Pool

Name: Select the pool name that you want to configure from the pull-down menu.

Setting

Pool Name: Display the pool name for this configured entry.

Type: Select the pool type.

Network: The pool defines a pool of IP addresses to service more than one DHCP client.

Host: The pool services for a specific DHCP client identified by client identifier or hardware address.

IP: Specify the network IP of the DHCP address pool.

Subnet Mask: Specify subnet mask of the DHCP address pool.

Lease Time: Specify lease time that a client needs to send requests to the DHCP server for renewed IP address. If all are 0's, then it means the lease time is infinite.

Domain Name: Specify the domain name that a client use when resolving hostname via DNS.

Broadcast Address: Specify the broadcast address in use on the client's subnet.

Default Router: Specify a list of IP addresses for routers on the clients' subnet.

DNS Server: Specify a list of Domain Name System name servers available to the client.

NTP Server: Specify a list of IP addresses indicating NTP servers available to the client.

NetBios Node Type: Select NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.

NetBIOS Scope: Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

NetBIOS Name Server: Specify a list of NBNS name servers listed in order of preference.

NIS Domain Name: Specify the name of the client's NIS domain.

NIS Server: Specify a list of IP addresses indicating NIS servers available to the client.

Client Identifier: Specify client's unique identifier to be used when the pool is the type of host.

Hardware Address: Specify client's hardware (MAC) address to be used when the pool is the type of host.

Client Name: Specify the name of client to be used when the pool is the type of host.

Vendor 1~4 Class Identifier: Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.

Vendor 1~4 Specific Information: Specify vendor specific information according to option 60 vendor class identifier.

4.3.4.2 DHCP Snooping

DHCP Snooping allows the switch to protect a network from being attacked by other devices or rogue DHCP servers. When DHCP Snooping is enabled on the switch, it can filter IP traffic on insecure (untrusted) ports that the source addresses cannot be identified by DHCP Snooping. The addresses assigned to connected clients on insecure ports can be carefully controlled by either using the dynamic binding registered with DHCP Snooping or using the static binding configured with IP Source Guard.

DHCP Snooping Configuration

Snooping Mode Disabled ▼

Port Mode Configuration

Port	Mode
*	<> ▼
1	Trusted ▼
2	Trusted ▼
3	Trusted ▼
4	Trusted ▼
5	Trusted ▼
6	Trusted ▼
7	Trusted ▼
8	Trusted ▼
9	Trusted ▼
10	Trusted ▼
11	Trusted ▼
12	Trusted ▼
13	Trusted ▼
14	Trusted ▼
15	Trusted ▼
16	Trusted ▼
17	Trusted ▼
18	Trusted ▼
19	Trusted ▼
20	Trusted ▼
21	Trusted ▼
22	Trusted ▼
23	Trusted ▼
24	Trusted ▼

DHCP Snooping Configuration

Snooping Mode: Enable or disable DHCP Snooping function globally. When DHCP snooping mode operation is enabled, the DHCP request messages from trusted ports will be processed and only allow reply packets from trusted ports.

Port Mode Configuration

Port: Port number. "Port *" rules apply to all ports.

Mode: Select the DHCP Snooping port mode. Ports can be set to either "Trusted" or "Untrusted".

Trusted: Devices under your administrative network can be set to Trusted sources. DHCP requests from Trusted ports are processed.

Untrusted: Host ports (connecting to customer devices) are treated as Untrusted sources. DHCP Snooping filters out invalid DHCP messages from Untrusted sources.

4.3.4.3 Relay Configuration

DHCP Relay Configuration	
Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Keep

DHCP Relay Configuration

Relay Mode: Enable or disable the DHCP relay function. When enabled, the agent forwards and transfers DHCP messages between the clients and server they are not in the same subnet domain. The DHCP broadcast message will not be flooded for security considerations.

Relay Server: Enter DHCP server IP address that is used by the switch's DHCP relay agent.

Relay Information Mode: Enable or disable DHCP Relay option 82 function. Please note that "Relay Mode" must be enabled before this function is able to take effect.

Relay Information Policy: Select Relay Information policy for DHCP client that includes option 82 information.

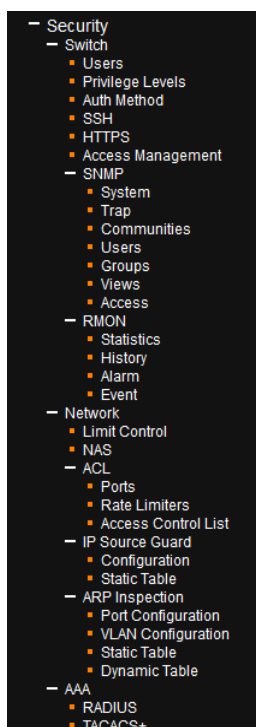
Replace: Replace the DHCP client packet information with the switch's relay information. This is the default setting.

Keep: Keep the client's DHCP information.

Drop: Drop the packet when it receives a DHCP message that already contains relay information.

4.3.5 Security

Under the security heading are three major icons, switch, network and AAA.



4.3.5.1 Switch

4.3.5.1.1 Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.

User Name	Privilege Level
admin	15

Add New User

By default, there is only one user, 'admin', assigned the highest privilege level of 15.

Click the entries in User Name column to edit the existing users. Or click the "Add New User" button to insert a new user entry.

Add User

Add User

User Settings	
User Name	normal
Password	•••••
Password (again)	•••••
Privilege Level	5

Save Reset Cancel

User Name: Enter the new user name.

Password: Enter the password for this user account.

Password (again): Retype the password for this user account.

Privilege Level: Select the appropriate privilege level for this user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

4.3.5.1.2 Privilege Levels

This page provides an overview of the privilege levels.

Privilege Level Configuration					
Group Name	Privilege Levels				
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write	
Aggregation	5 ▼	10 ▼	5 ▼	10 ▼	
Debug	15 ▼	15 ▼	15 ▼	15 ▼	
DHCP	5 ▼	10 ▼	5 ▼	10 ▼	
DHCPv6_Client	5 ▼	10 ▼	5 ▼	10 ▼	
Diagnostics	5 ▼	10 ▼	5 ▼	10 ▼	
IP	5 ▼	10 ▼	5 ▼	10 ▼	
IPMC_Snooping	5 ▼	10 ▼	5 ▼	10 ▼	
JSON_RPC	5 ▼	10 ▼	5 ▼	10 ▼	
JSON_RPC_Notification	5 ▼	10 ▼	5 ▼	10 ▼	
LACP	5 ▼	10 ▼	5 ▼	10 ▼	
LLDP	5 ▼	10 ▼	5 ▼	10 ▼	
Loop_Protect	5 ▼	10 ▼	5 ▼	10 ▼	
MAC_Table	5 ▼	10 ▼	5 ▼	10 ▼	
Maintenance	15 ▼	15 ▼	15 ▼	15 ▼	
MVR	5 ▼	10 ▼	5 ▼	10 ▼	
NTP	5 ▼	10 ▼	5 ▼	10 ▼	
Ports	5 ▼	10 ▼	1 ▼	10 ▼	
Private_VLANs	5 ▼	10 ▼	5 ▼	10 ▼	
QoS	5 ▼	10 ▼	5 ▼	10 ▼	
RMirror	5 ▼	10 ▼	5 ▼	10 ▼	
Security	5 ▼	10 ▼	5 ▼	10 ▼	
sFlow	5 ▼	10 ▼	5 ▼	10 ▼	
Spanning_Tree	5 ▼	10 ▼	5 ▼	10 ▼	
System	5 ▼	10 ▼	1 ▼	10 ▼	
UDLD	5 ▼	10 ▼	5 ▼	10 ▼	
UPnP	5 ▼	10 ▼	5 ▼	10 ▼	
VCL	5 ▼	10 ▼	5 ▼	10 ▼	

Group Name: This name identifies the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:

System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.

IP: Everything except 'ping'.

Diagnostics: 'ping'.

Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

Debug: Only present in CLI.

Privilege Levels: Every group has an authorization Privilege level for the following sub groups:

configuration read-only

configuration/execute read-write

status/statistics read-only

status/statistics read-write (e.g. for clearing of statistics)

User Privilege should be the same or greater than the authorization Privilege level to have access to that group.

4.3.5.1.3 Auth Method

This page allows you to configure how users are authenticated when they log into the switch via one of the management client interfaces.

Authentication Method Configuration

Client	Methods		
console	local ▼	no ▼	no ▼
telnet	local ▼	no ▼	no ▼
ssh	local ▼	no ▼	no ▼
http	local ▼	no ▼	no ▼

Command Authorization Method Configuration

Client	Method	Cmd Lvl	Cfg Cmd
console	no ▼	0	☐
telnet	no ▼	0	☐
ssh	no ▼	0	☐

Accounting Method Configuration

Client	Method	Cmd Lvl	Exec
console	no ▼		☐
telnet	no ▼		☐
ssh	no ▼		☐

Authentication Method Configuration

Client: The management client for which the configuration below applies.

Methods: Method can be set to one of the following values:

no: Authentication is disabled and login is not possible.

local: Use the local user database on the switch for authentication.

radius: Use remote RADIUS server(s) for authentication.

tacacs+: Use remote TACACS+ server(s) for authentication.

Note: Methods that involve remote servers will time out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

Command Authentication Method Configuration

Client: The management client for which the configuration below applies.

Methods: Method can be set to one of the following values:

no: Authentication is disabled and login is not possible.

local: Use the local user database on the switch for authentication.

radius: Use remote RADIUS server(s) for authentication.

tacacs+: Use remote TACACS+ server(s) for authentication.

Cmd Lvl: Authorize all commands with a privilege level higher than or equal to this level.

Cfg cmd: Authorize configuration commands.

Accounting Method Configuration

Client: The management client for which the configuration below applies.

Methods: Method can be set to one of the following values:

no: Authentication is disabled and login is not possible.

local: Use the local user database on the switch for authentication.

radius: Use remote RADIUS server(s) for authentication.

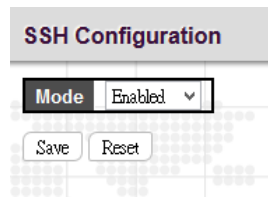
tacacs+: Use remote TACACS+ server(s) for authentication.

Cmd Lvl: Authorize all commands with a privilege level higher than or equal to this level.

Exec: Enable Exec (login) accounting.

4.3.5.1.4 SSH

Configure SSH on this page.

The image shows a web-based configuration interface for SSH. At the top, there is a title bar that says "SSH Configuration". Below this, there is a label "Mode" followed by a dropdown menu currently showing "Enabled". At the bottom of the configuration area, there are two buttons: "Save" and "Reset". The background of the interface has a subtle grid pattern.

Mode: Indicates the SSH mode operation. Possible modes are:

Enabled: Enable SSH mode operation. By default, SSH mode operation is enabled.

Disabled: Disable SSH mode operation.

NOTE: SSH is preferred to Telnet, unless the management network is trusted. Telnet passes authentication credentials in plain text, making those credentials susceptible to packet capture and analysis. SSH provides a secure authentication method. The SSH in this device uses version 2 of SSH protocol.

4.3.5.1.5 HTTPS

Configure HTTPS on this page.

HTTPS Configuration	
Mode	Disabled
Automatic Redirect	Disabled
Certificate Maintain	None
Certificate Status	Switch secure HTTP certificate is presented
Save Reset	

Mode: Indicates the HTTPS operation mode. When the current connection is HTTPS and HTTPS mode operation is disabled, web browser will automatically redirect to an HTTP connection. Possible modes are:

Enabled: Enable HTTPS mode operation.

Disabled: Disable HTTPS mode operation.

Automatic Redirect: Indicates the HTTPS redirect mode operation. It applies only if HTTPS mode "Enabled" is selected. Automatically redirects HTTP of web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are:

Enabled: Enable HTTPS redirect mode operation.

Disabled: Disable HTTPS redirect mode operation.

Certificate Maintain: Select a way to either upload or generate a certificate.

Certificate Pass Phrase: Configure private key pass phrase. The allowed string length is 0 to 60.

Certificate File: Indicates a way (either Web Browser or URL) to upload a certificate file.

Private Key File: Indicates a private key file for uploading.

4.3.5.1.6 Access Management Configuration

Configure the access management table on this page. The maximum number of entries is 16. If the application's type matches any one of the access management entries, it will be allowed access to the switch.

Access Management Configuration						
Mode: Enabled						
Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1	192.168.0.49	192.168.0.49	☒	☒	☒
Add New Entry						
Save Reset						

Click the "Add New Entry" button to insert a new entry to the list.

Mode: Indicates the access management mode operation. Possible modes are:

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

VLAN ID: Indicates the VLAN ID for the access management entry.

Start IP address: Indicates the start IP address for the access management entry.

End IP address: Indicates the end IP address for the access management entry.

HTTP/HTTPS: Checked indicates that the matched host can access the switch from HTTP/HTTPS interface.

SNMP: Checked indicates that the matched host can access the switch from SNMP.

TELNET/SSH: Indicates that the matched host can access the switch from TELNET/SSH interface.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

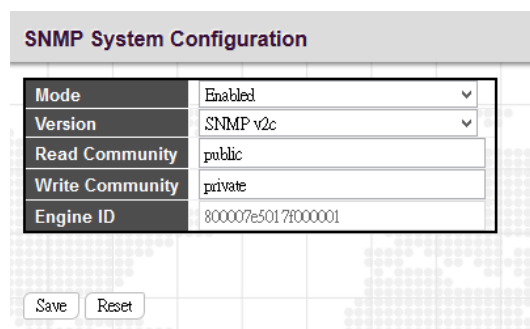
Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.3.5.1.7 SNMP

4.3.5.1.7.1 SNMP System Configuration

Configure SNMP on this page.



The screenshot shows the 'SNMP System Configuration' web page. It features a table with the following fields and values:

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Below the table are two buttons: 'Save' and 'Reset'.

Mode: Indicates the SNMP mode operation. Possible modes are:

Enabled: Enable SNMP mode operation.

Disabled: Disable SNMP mode operation.

Version: Indicates the SNMP supported version. Possible versions are:

SNMP v1: Set SNMP supported version 1.

SNMP v2c: Set SNMP supported version 2c.

SNMP v3: Set SNMP supported version 3.

Read Community: Indicates the community read access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E.

Write Community: Indicates the community write access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E. These two fields are applicable only for SNMP version v1 or v2c. If SNMP version is v3, the community string will be associated with SNMPv3 communities table. SNMPv3 provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Engine ID: Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Changes to the Engine ID will clear all original local users.

4.3.5.1.7.2 SNMP Trap Configuration

Configure SNMP trap on this page.

Global Settings

Mode: Globally enable or disable trap function.

Click the “Add New Entry” to insert a SNMP trap entry.

SNMP Trap Configuration

SNMP Trap Configuration	
Trap Config Name	
Trap Mode	Disabled
Trap Version	SNMP v2c
Trap Community	Public
Trap Destination Address	
Trap Destination Port	162
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled
Trap Security Engine ID	
Trap Security Name	None

SNMP Trap Event	
System	☐ * Warm Start ☐ Cold Start
Link up	☒ none ☐ specific ☐ all switches
Link down	☐ * Link down ☒ none ☐ specific ☐ all switches
LLDP	☒ none ☐ specific ☐ all switches
AAA	☐ * Authentication Fail
Switch	☐ * STP ☐ RMON

Save Reset

Trap Config Name: Indicates a descriptive name for this SNMP trap entry.

Trap Mode: Indicates the SNMP trap mode operation.

Enabled: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation.

Trap Version: Indicates the SNMP trap supported version. Possible versions are:

SNMP v1: Set SNMP trap supported version 1.

SNMP v2c: Set SNMP trap supported version 2c.

SNMP v3: Set SNMP trap supported version 3.

Trap Community: Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 0x21 to 0x7E.

Trap Destination Address: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). Also allowed is a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z; a-z), digits (0-9), dot (.) and dash (-). Spaces are not allowed. The first character must be an alpha character, and the first and last characters cannot be a dot or a dash.

Trap Destination port: Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. The default SNMP trap port is 162.

Trap Inform Mode: Indicates the SNMP trap inform mode operation. Possible modes are:

Enabled: Enable SNMP trap inform mode operation.

Disabled: Disable SNMP trap inform mode operation.

Trap Inform Timeout (seconds): Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

Trap Inform Retry Times: Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

Trap Probe Security Engine ID: Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:

Enabled: Enable SNMP trap probe security engine ID mode of operation.

Disabled: Disable SNMP trap probe security engine ID mode of operation.

Trap Security Engine ID: Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs use USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Trap Security Name: Indicates the SNMP trap security name. SNMPv3 traps and informs use USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

SNMP Trap Event

The image shows a configuration window titled "SNMP Trap Event". It contains four main sections: System, Interface, Authentication, and Switch. Each section has several options to be configured.

Section	Options
System	☐ * Warm Start ☒ Cold Start
Interface	Link up: ☐ none ☐ specific ☒ all switches Link down: ☐ none ☐ specific ☒ all switches LLDP: ☐ none ☐ specific ☒ all switches
Authentication	☐ * SNMP Authentication Fail
Switch	☐ * STP ☒ RMON

System: The system trap events include the following.

Warm Start: The switch has been rebooted from an already powered on state.

Cold Start: The switch has booted from a powered off or due to power cycling (power failure).

Interface: Indicates the Interface group's traps. Possible traps are:

Link Up: none/specific/all ports Link up trap.

Link Down: none/specific/all ports Link down trap.

LLDP: none/specific/all ports LLDP (Link Layer Discovery Protocol) trap.

When the "specific" radio button is selected, a popup graphic with port checkboxes allows selection specific ports.

Port	Link up	Link down	LLDP
1	☐	☐	☐
2	☐	☐	☐
3	☐	☐	☐
4	☐	☐	☐
5	☐	☐	☐
6	☐	☐	☐
7	☐	☐	☐
8	☐	☐	☐
9	☐	☐	☐
10	☐	☐	☐
11	☐	☐	☐
12	☐	☐	☐
13	☐	☐	☐
14	☐	☐	☐
15	☐	☐	☐
16	☐	☐	☐
17	☐	☐	☐
18	☐	☐	☐
19	☐	☐	☐
20	☐	☐	☐
21	☐	☐	☐
22	☐	☐	☐
23	☐	☐	☐
24	☐	☐	☐
25	☐	☐	☐
26	☐	☐	☐
27	☐	☐	☐
28	☐	☐	☐
29	☐	☐	☐
30	☐	☐	☐
31	☐	☐	☐
32	☐	☐	☐
33	☐	☐	☐

Save Reset

Authentication Fail: A trap will be issued at any SNMP authentication failure.

Switch: Indicates that the Switch group's traps. Possible traps are:

STP: Select the checkbox to enable STP trap. Clear to disable STP trap.

RMON: Select the checkbox to enable RMON trap. Clear to disable RMON trap.

After completing all the trap settings, click the "Save" button.

4.3.5.1.7.3 SNMPv3 Community Configuration

Configure SNMPv3 community table on this page. The entry index key is Community.

SNMPv3 Community Configuration			
Delete	Community	Source IP	Source Mask
☐	public	0.0.0.0	0.0.0.0
☐	private	0.0.0.0	0.0.0.0

Add New Entry Save Reset

Delete: Check to delete the entry. It will be deleted during the next save.

Community: Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string. This string is case sensitive.

Source IP: Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask: Indicates the SNMP access source address mask.

4.3.5.1.7.4 SNMPv3 User Configuration

Configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.

SNMPv3 User Configuration							
Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Engine ID: An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it is a remote user.

User Name: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Security Level: Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

SHA: An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Password: A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32 characters. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters from 0x21 to 0x7E.

Privacy Protocol: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: No privacy protocol.

DES: An optional flag to indicate that this user uses DES authentication protocol.

AES: An optional flag to indicate that this user uses AES authentication protocol.

Privacy Password: A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.3.5.1.7.5 SNMPv3 Group Configuration

Configure SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.

SNMPv3 Group Configuration			
Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	default_user	default_rw_group

Security Model: Indicates the security model that this entry should belong to. Possible security models are:

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM) for SNMPv3.

Security Name: A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

4.3.5.1.7.6 SNMPv3 View Configuration

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

SNMPv3 View Configuration			
Delete	View Name	View Type	OID Subtree
☐	default_view	included ▼	.1

View Name: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

View Type: Indicates the view type that this entry should belong to. Possible view types are:

included: An optional flag to indicate that this view subtree should be included.

excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

OID Subtree: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or an asterisk(*).

4.3.5.1.7.7 SNMPv3 Access Configuration

Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model and Security Level.

SNMPv3 Access Configuration					
Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view	None
☐	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

Delete: Check to delete the entry. It will be deleted during the next save.

Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Security Model: Indicates the security model that this entry should belong to. Possible security models are:

any: Any security model accepted(v1|v2c|usm).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM) for SNMPv3.

Security Level: Indicates the security level that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Read View Name: The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Write View Name: The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

4.3.5.1.8 RMON

4.3.5.1.8.1 RMON Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is ID.

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1. 0

Add New Entry Save Reset

Delete: Check to delete the entry. It will be deleted during the next save.

ID: Indicates the index of the entry. The range is from 1 to 65535.

Data Source: Indicates the port ID which wants to be monitored.

4.3.5.1.8.2 RMON History Configuration

RMON History Configuration is to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A RMON historical record can be used to monitor intermittent problems.

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1.	0	1800	50

Add New Entry Save Reset

ID: Indicates the index of the entry. The range is from 1 to 65535.

Data Source: Indicates the port ID which wants to be monitored.

Interval: Indicates the polling interval. By default, 1800 seconds is specified. The allowed range is 1 - 3600 seconds.

Buckets: The number of buckets requested for this entry. By default, 50 is specified. The allowed range is 1 - 3600.

Buckets Granted: The number of buckets granted.

Click the "Add New Entry" button to insert a new entry to the list.

Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the "Save" button to save settings or changes.

Click the "Reset" button to restore changed settings to the default settings.

4.3.5.1.8.3 RMON Alarm Configuration

RMON Alarm configuration defines specific criteria that will generate response events. It can be set to test data over any specified time interval and can monitor absolute or changing values. Alarms can also be set to respond to rising or falling thresholds.

RMON Alarm Configuration										
Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Delete		30	.1.3.6.1.2.1.2.2.1.	0.0	Delta ▼	0	RisingOrFalling ▼	0	0	0
Add New Entry Save Reset										

ID: Indicates the index of the entry. The range is from 1 to 65535.

Interval: The polling interval for sampling and comparing the rising and falling threshold. The range is from 1 to 2^{31} seconds.

Variable: The object number of the MIB variable to be sampled. Only variables of the type ifEntry.n.n may be sampled. Possible variables are InOctets, InUcastPkts, InNUcastPkts, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPkts, OutNUcastPkts, OutDiscards, OutErrors, and OutQLen.

Sample Type: Test for absolute or relative change in the specified variable.

Absolute: The variable is compared to the thresholds at the end of the sampling period.

Delta: The last sample is subtracted from the current value and the difference is compared to the thresholds.

Value: The statistic value during the last sampling period.

Startup Alarm: Select a method that is used to sample the selected variable and calculate the value to be compared against the thresholds.

Rising or Falling: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold.

Rising: Trigger alarm when the first value is larger than the rising threshold.

Falling: Trigger alarm when the first value is less than the falling threshold.

Rising Threshold: If the current value is greater than the rising threshold and the last sample value is less than this threshold, then an alarm will be triggered. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. The threshold range is -2147483647 to 2147483647.

Rising Index: Indicates the rising index of an event. The range is 1 - 65535.

Falling Threshold: If the current value is less than the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the falling threshold. (Range: -2147483647 to 2147483647)

Falling Index: Indicates the falling index of an event. The range is 1 - 65535.

Click the "Add New Entry" button to insert a new entry to the list.

Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the "Save" button to save settings or changes.

Click the "Reset" button to restore changed settings to the default settings.

4.3.5.1.8.4 RMON Event Configuration

RMON Event Configuration page is used to set an action taken when an alarm is triggered.

RMON Event Configuration					
Delete	ID	Desc	Type	Community	Event Last Time
☐			none	public	0

Delete: Check to delete the entry. It will be deleted during the next save.

ID: Specify an ID index. The range is 1 - 65535.

Desc: Enter a descriptive comment for this entry.

Type: Select an event type that will take when an alarm is triggered.

None: No event is generated.

Log: When the event is triggered, a RMON log entry will be generated.

snmptrap: Sends a trap message to all configured trap managers.

logandtrap: Logs an event and sends a trap message.

Community: A password-like community string sent with the trap. Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page prior to configuring it here. The allowed characters are 0 - 127.

Event Last Time: The value of sysUpTime when an event was last generated for this entry.

4.3.5.2 Network

Port Security Limit Control can restrict the number of users that can access the switch based on users' MAC address and VLAN ID on a per port basis. Once the number of users that wants to access the switch exceeds the specified number, a selected action will be taken immediately.

4.3.5.2.1 Limit Control

Port Security Limit Control Configuration

System Configuration

Mode	Disabled ▾
Aging Enabled	☐
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	Disabled ▾	4	None ▾	Disabled	Reopen
1	Disabled ▾	4	None ▾	Disabled	Reopen
2	Disabled ▾	4	None ▾	Disabled	Reopen
3	Disabled ▾	4	None ▾	Disabled	Reopen
4	Disabled ▾	4	None ▾	Disabled	Reopen
5	Disabled ▾	4	None ▾	Disabled	Reopen
6	Disabled ▾	4	None ▾	Disabled	Reopen
7	Disabled ▾	4	None ▾	Disabled	Reopen
8	Disabled ▾	4	None ▾	Disabled	Reopen
9	Disabled ▾	4	None ▾	Disabled	Reopen
10	Disabled ▾	4	None ▾	Disabled	Reopen
11	Disabled ▾	4	None ▾	Disabled	Reopen
12	Disabled ▾	4	None ▾	Disabled	Reopen
13	Disabled ▾	4	None ▾	Disabled	Reopen
14	Disabled ▾	4	None ▾	Disabled	Reopen
15	Disabled ▾	4	None ▾	Disabled	Reopen
16	Disabled ▾	4	None ▾	Disabled	Reopen

System Configuration

Mode: Enable or disable port security limit control globally. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled: If enabled, secured MAC addresses are subject to aging as discussed under Aging Period. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Aging Period: If Aging Enabled is checked, then the aging period can be set up with the desired value. By default, the aging period is set to 3600 seconds. The allowed range is 10 - 10,000,000 second.

Port Configuration

Port: Display the port number. "Port *" rules apply to all ports.

Mode: Enable or disable port security limit control on a per port basis. To make limit control function work, port security limit control needs to be enabled globally and on a port.

Limit: The maximum number of MAC addresses that can be secured on this port. The number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

Action: If the limit is exceeded, the selected action will take effect.

None: Do not allow more than the specified limit of MAC addresses to access on a port. No action is further taken.

Trap: If Limit + 1 MAC addresses are seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit is exceeded.

Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new addresses will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

- * Boot the switch
- * Disable and re-enable Limit Control on the port or the switch
- * Click the "Reopen" button

Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State: Display the current state of the port from the port security limit control's point of view. The displayed state might be one of the following:

Disabled: Limit control is either globally disabled or disabled on a port.

Ready: The limit is not reached yet.

Limit Reached: The limit is reached on a port. This state can only be shown if Action is set to None or Trap.

Shutdown: The port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

Re-open Button: If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section. Note that clicking the Reopen button causes the page to be refreshed, so non-committed changes will be lost.

4.3.5.2.2 NAS

Network Access Server configuration is useful to the networking environment that wants to authenticate clients (suplicants) before they can access resources on the protected network. To effectively control access to unknown clients, 802.1X defined by IEEE provides a port-based authentication procedure that can prevent unauthorized access to a network by requiring users to first submit credentials for authentication purposes.

A switch interconnecting clients and radius server usually acts as an authenticator and uses EAPOL (Extensible Authentication Protocol over LANs) to exchange authentication protocol messages with clients and a remote RADIUS authentication server to verify user identity and user's access right. This section is for setting up authenticator's configurations either on the system or on a per port basis. To configure backend server, please go to RADIUS configuration page.

Network Access Server Configuration

System Configuration

Mode	Disabled ▾	
Reauthentication Enabled	☐	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds
RADIUS-Assigned QoS Enabled	☐	
RADIUS-Assigned VLAN Enabled	☐	
Guest VLAN Enabled	☐	
Guest VLAN ID	1	
Max. Reauth. Count	2	
Allow Guest VLAN if EAPOL Seen	☐	

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	Force Authorized ▾	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
1	Force Authorized ▾	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized ▾	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized ▾	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized ▾	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized ▾	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized ▾	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized ▾	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize

System Configuration

Mode: Enable 802.1X and MAC-based authentication globally on the switch. If globally disabled, all ports are allowed to forward frames.

Reauthentication Enabled: Select the checkbox to set clients to be re-authenticated after an interval set in "Reauthentication Period" field. Re-authentication can be used to detect if a new device is attached to a switch port.

Reauthentication Period: Specify the time interval for a connected device to be re-authenticated. By default, the re-authenticated period is set to 3600 seconds. The allowed range is 1 - 3600 seconds.

EAPOL Timeout: Specify the time that the switch waits for a supplicant response during an authentication session before transmitting a Request Identify EAPOL packet. By default, it is set to 30 seconds. The allowed range is 1 - 65535 seconds.

Aging Period: Specify the period that is used to age out a client's allowed access to the switch via 802.1X and MAC-based authentication. The default period is 300 seconds. The allowed range is 10 - 1000000 seconds.

Hold Time: The time after an EAP Failure indication or RADIUS timeout that a client is not allowed access. This setting applies to ports running Single 802.1X, Multi 802.1X, or MAC-based authentication. By default, hold time is set to 10 seconds. The allowed range is 10 -1000000 seconds.

Radius-Assigned QoS Enabled: Select the checkbox to globally enable RADIUS assigned QoS.

Radius-Assigned VLAN Enabled: RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature.

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled: A Guest VLAN is a special VLAN typically with limited network access. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID: This VLAN ID is functional only when Guest VLAN is enabled. This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. The range is 1–4095.

Max. Reauth. Count: The maximum number of times the switch transmits an EAPOL Request Identity frame without receiving a response before adding a port to the Guest VLAN. The value can only be changed when the Guest VLAN option is globally enabled. The range is 1–255.

Allow Guest VLAN if EAPOL Seen: The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration

Port: The port number. "Port *" rules apply to all ports.

Admin State: Select the authentication mode on a port. This setting works only when NAS is globally enabled. The following modes are available:

Force Authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

Force Unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-Based 802.1X: This mode requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.

Single 802.1X: In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the "Port Security" module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X: In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the "Port Security" module.

MAC-based Auth.: Unlike port-based 802.1X, MAC-based authentication do not transmit or receive EAPOL frames. In MAC-based authentication, the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

RADIUS-Assigned QoS Enabled: Select the checkbox to enable RADIUS-Assigned QoS on a port.

Radius-Assigned VLAN Enabled: Select the checkbox to enable RADIUS-Assigned VLAN on a port.

Guest VLAN Enabled: Select the checkbox to enable Guest VLAN on a port.

Port State: Display the current state of the port from 802.1X authentication point of view. The possible states are as follows:

Globally Disabled: 802.1X and MAC-based authentication are globally disabled.

Link Down: 802.1X and MAC-based authentication are enabled but there is no link on a port.

Authorized: The port is forced in authorized mode and the supplicant is successfully authorized.

Unauthorized: The port is forced in unauthorized mode and the supplicant is not successfully authorized by the RADIUS server.

X Auth/Y Unauth: The port is in a multi-supplicant mode. X clients are authorized and Y are unauthorized.

Restart: Restart client authentication using one of the methods described below. Note that the restart buttons are only enabled when the switch's authentication mode is globally enabled (under System Configuration) and the port's Admin State is an EAPOL-based or MACBased mode. Clicking these buttons will not cause settings changed on the page to take effect.

Reauthenticate: Schedules reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize: This forces the reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

4.3.5.2.3 ACL

ACL is a sequential list established to allow or deny users to access information or perform tasks on the network. In this switch, users can establish rules applied to port numbers to permit or deny actions or restrict rate limit.

4.3.5.2.3.1 Ports

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Port: The port number.

Policy Id: Assign an ACL policy ID to a particular port. A port can only use one policy ID; however, a policy ID can apply to many ports. The default ID is 0. The allowed range is 0–255.

Action: Permit or deny a frame based on whether it matches a rule defined in the assigned policy.

Rate Limiter ID: Select a rate limiter ID to apply to a port. Rate Limiter rule can be set up in “Rate Limiters” configuration page.

Port Redirect: Select a port to which matching frames are redirected.

Mirror: Enable or disable mirroring feature. When enabled, a copy of matched frames will be mirrored to the destination port specified in “Mirror” configuration page. ACL-based port mirroring set by this parameter and port mirroring set on the general Mirror Configuration page are implemented independently. To use ACL-based mirroring, enable the Mirror parameter on the ACL Ports Configuration page. Then open the Mirror Configuration page, set the “Port to mirror on” field to the required destination port, and leave the “Mode” field Disabled.

Logging: Enable logging of matched frames to the system log. To view log entries, go to System menu and then click the “System Log Information” option.

Shutdown: This field is to decide whether to shut down a port when matched frames are seen or not.

State: Select a port state.

Enabled: To re-open a port.

Disabled: To close a port.

Counters: The number of frames that have matched the rules defined in the selected policy.

4.3.5.2.3.2 Rate Limiters

ACL Rate Limiter Configuration	
Rate Limiter ID	Rate (pps)
*	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1

Save Reset

Rate Limiter ID: Display every rate limiter ID.

Rate: Specify the threshold above which packets are dropped. The allowed values are 0–3276700 pps or 1, 100, 200, 300...1000000 kbps.

Unit: Select the unit of measure used in rate.

4.3.5.2.3.3 Access Control List

Access Control List is to establish filtering rules for an ACL policy, for a particular port or for all ports. Rules applied to a port take effect immediately.

Access Control List Configuration								Auto-refresh ☐	Refresh	Clear	Remove All
Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter				
1	Any	Any	Permit	Disabled	Disabled	Disabled	0	+ + + + + + + + + + + + + + + + + + + +			

Ingress Port: The ingress port of the access control entry. Select “All” to apply to all ports or select a particular port.

Policy Bitmask: The policy number and bitmask of the ACE.

Frame Type: The type of frame that matches to this rule.

Action: Display the action type, either to permit or deny.

Rate Limiter: Display rate limiter is enabled or disabled when matched frames are found.

Port Redirect: Display port redirect is enabled or disabled.

Mirror: Display mirror function is enabled or disabled.

Counter: Display the number of frames that have matched any of the rules defined for this ACL.

Click the plus sign to add a new ACE entry.

ACE Configuration

Ingress Port

All

Policy Filter

Any

Frame Type

Any

Action

Permit

Rate Limiter

Disabled

Logging

Disabled

Shutdown

Disabled

Counter

0

MAC Parameters

DMAC Filter

Any

VLAN Parameters

VLAN ID Filter

Any

Tag Priority

Any

Save

Reset

Cancel

ACE Configuration

Ingress Port: Select the ingress port of the access control entry. Select “All” to apply an ACL rule to all ports or select a particular port.

Policy Filter: Select the policy filter type. “Any” means no policy filter is assigned to this rule (or don’t care). Select “Specific” to filter specific policy with this ACE.

Frame Type: Select a frame type to match. Available frame types include Any, Ethernet, ARP, IPv4. By default, any frame type is used.

Action: Select the action type, either to permit or deny.

Rate Limiter: Enable or disable the rate limiter when matched frames are found.

Logging: Enable or disable logging when a frame is matched.

Shutdown: Enable or disable shutdown a port when a frame is matched.

Counter: Display the number of frames that have matched any of the rules defined for this ACL.

MAC Parameter

SMAC Filter: The type of source MAC address. Select “Any” to allow all types of source MAC addresses or select “Specific” to define a source MAC address. This setting is only available when you select Ethernet and ARP frame type.

DMAC Filter: The type of destination MAC address.

Any: To allow all types of destination MAC addresses

MC: Multicast MAC address

BC: Broadcast MAC address

UC: Unicast MAC address

Specific: Use this to self-define a destination MAC address. This option is only available when you select Ethernet frame type.

VLAN Parameters

VLAN ID Filter: Select the VLAN ID filter for this ACE.

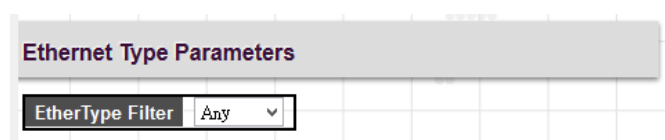
Any: No VLAN ID filter is specified. (Don’t care)

Specific: Specify a VLAN ID. A frame with the specified VLAN ID matches this ACE rule.

Tag Priority: Select the User Priority value found in the VLAN tag to match this rule.

Ethernet Type Parameter

Select “Ethernet” frame type, then Ethernet Type parameters appear.



Ether Type Filter: This option can only be used to filter Ethernet II formatted packets. Select “Specific” to define an Ether Type value.

ARP Parameter

Select “ARP” frame type, then Ethernet Type parameters appear.

ARP Parameters	
ARP/RARP	Any ▼
Request/Reply	Any ▼
Sender IP Filter	Any ▼
Target IP Filter	Any ▼
ARP Sender MAC Match	Any ▼
RARP Target MAC Match	Any ▼
IP/Ethernet Length	Any ▼
IP	Any ▼
Ethernet	Any ▼

ARP/RARP: Specify the type of ARP packet.

Any: No ARP/RARP opcode flag is specified

ARP: The frame must have ARP/RARP opcode set to ARP,

RARP: The frame must have ARP/RARP opcode set to RARP

Other: The frame has unknown ARP/RARP opcode flag

Request/Reply: Specify whether the packet is an ARP request, reply, or either type.

Any: No ARP/RARP opcode flag is specified

Request: The frame must have ARP Request or RARP Request opcode flag set.

Reply: The frame must have ARP Reply or RARP Reply opcode flag set.

Sender IP Filter: Specify the sender's IP address.

Any: No sender IP filter is specified.

Host: Specify the sender IP address.

Network: Specify the sender IP address and sender IP mask.

Target IP Filter: Specify the destination IP address.

Any: No target IP filter is specified.

Host: Specify the target IP address.

Network: Specify the target IP address and target IP mask.

ARP Sender SMAC Match: Select "0" to indicate that the SHA (Sender Hardware Address) field in the ARP/RARP frame is not equal to source MAC address. Select "1" to indicate that SHA field in the ARP/RARP frame is equal to source MAC address. Select "Any" to indicate a match and not a match.

RARP Target MAC Match: Select "0" to indicate that the THA (Target Hardware Address) field in the ARP/RARP frame is not equal to source MAC address. Select "1" to indicate that THA field in the ARP/RARP frame is equal to source MAC address. Select "Any" to indicate a match and not a match.

IP/Ethernet Length: Select "0" to indicate that HLN (Hardware Address Length) field in the ARP/RARP frame is not equal to Ethernet (0x6) and the Protocol Address Length field is not equal to IPv4 (0x4). Select "1" to indicate that HLN (Hardware Address Length) field in the ARP/RARP frame is equal to Ethernet (0x6) and the Protocol Address Length field is equal to IPv4 (0x4). Select "Any" to indicate a match and not a match.

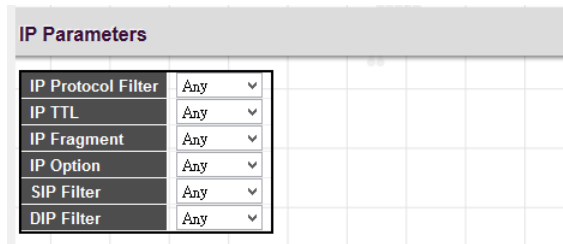
IP: Select "0" to indicate that Protocol Address Space field in ARP/RARP frame is not equal to IP (0x800). Select "1" to

indicate that Protocol Address Space is equal to IP (0x800). Select “Any” to indicate a match and not a match.

Ethernet: Select “0” to indicate that Hardware Address Space field in ARP/RARP frame is not equal to Ethernet (1). Select “1” to indicate that Hardware Address Space field is equal to Ethernet (1). Select “Any” to indicate a match and not a match.

IP Parameters

Select “IPv4” frame type, then the following IP parameters appear.



IP Parameters	
IP Protocol Filter	Any ▼
IP TTL	Any ▼
IP Fragment	Any ▼
IP Option	Any ▼
SIP Filter	Any ▼
DIP Filter	Any ▼

IP Protocol Filter: Select “Any”, “ICMP”, “UDP”, “TCP”, or “Other” protocol from the pull-down menu for IP Protocol filtering.

IP TTL: Select “Zero” to indicate that the TTL filed in IPv4 header is 0. If the value in TTL field is not 0, use “Non-Zero” to indicate that. You can also select “any” to denote the value which is either 0 or not 0.

IP Fragment: Select “Any” to allow any values. “Yes” denotes that IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must match this entry. “No” denotes that IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not match this entry.

IP Option: Specify the options flag setting for this rule. Select “Any” to allow any values. “Yes” denotes that IPv4 frames where the options flag is set must match this entry. “No” denotes that Pv4 frames where the options flag is set must not match this entry

SIP Filter: Select “Any”, “Host”, or “Network” for source IP filtering. If “Host” is selected, you need to indicate a specific host IP address. If “Network” is selected, you need to indicate both network address and subnet mask.

SIP Address: Specify a source IP address.

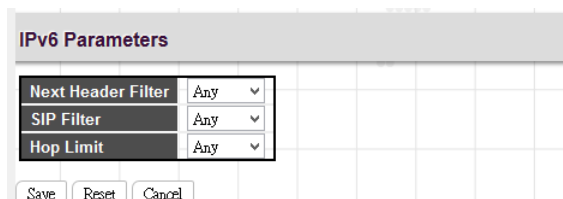
SIP Mask: Specify a source subnet mask.

DIP Filter: Select “Any”, “Host”, or “Network” for destination IP filtering. If “Host” is selected, you need to indicate a specific host IP address. If “Network” is selected, you need to indicate both network address and subnet mask.

DIP Address: Specify a destination IP address.

DIP Mask: Specify a destination subnet mask.

IPv6 Parameters



IPv6 Parameters	
Next Header Filter	Any ▼
SIP Filter	Any ▼
Hop Limit	Any ▼

Save Reset Cancel

Next Header Filter: Select next header filter option. Available options include ICMP, UDP, TCP, Other.

SIP Filter: Select a source IP filter. “Any” denotes that any SIP filter is allowed. Select “Specific” to enter self-define SIP filter.

Hop Limit: Select “Any” to allow any values in this field. Select “0” if IPv6 frames with a hop limit field greater than zero must not be able to match this entry. “1” denotes that IPv6 frames with a hop limit field greater than zero must be able to match this entry.

4.3.5.2.4 IP Source Guard

4.3.5.2.4.1 Configuration

Port	Mode	Max Dynamic Clients
*	Disabled	Unlimited
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited
11	Disabled	Unlimited
12	Disabled	Unlimited
13	Disabled	Unlimited
14	Disabled	Unlimited
15	Disabled	Unlimited
16	Disabled	Unlimited

IP Source Guard Configuration

Mode: Enable or disable IP source guard globally.

Translate dynamic to static: Click this button to translate dynamic entries to static ones.

Port Mode Configuration

Port: The port number. “Port *” rules apply to all ports.

Mode: Enable or disable IP source guard on a port. Please note that to make IP source guard work, both global mode and port mode must be enabled.

Max Dynamic Clients: Select the maximum number of dynamic clients that can be learned on a port. The available options are 0, 1, 2, unlimited. If the port mode is enabled and the maximum number of dynamic clients is equal 0, the switch will only forward IP packets that are matched in static entries for a given port.

4.3.5.2.4.2 Static Table

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
☐	1			

Add New Entry

Save Reset

Port: Select a port to which a static entry is bound.

VLAN ID: Enter VLAN ID that has been configured.

IP Address: Enter a valid IP address.

MAC Address: Enter a valid MAC address.

Click the “Add New Entry” button to insert an entry to the table.

Select the “Delete” checkbox to remove the entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore settings to default settings or previously configured settings.

4.3.5.2.5 ARP inspection

4.3.5.2.5.1 Port Configuration

ARP Inspection Configuration

Mode: Disabled

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None
8	Disabled	Disabled	None
9	Disabled	Disabled	None
10	Disabled	Disabled	None
11	Disabled	Disabled	None
12	Disabled	Disabled	None
13	Disabled	Disabled	None
14	Disabled	Disabled	None
15	Disabled	Disabled	None
16	Disabled	Disabled	None
17	Disabled	Disabled	None
18	Disabled	Disabled	None
19	Disabled	Disabled	None
20	Disabled	Disabled	None
21	Disabled	Disabled	None

ARP Inspection Configuration

Mode: Enable or disable ARP inspection function globally.

Port Mode Configuration

Port: The port number. "Port *" rules apply to all ports.

Mode: Enable or disable ARP Inspection on a port. Please note that to make ARP inspection work, both global mode and port mode must be enabled.

Check VLAN: Enable or disable check VLAN operation.

Log Type: There are four log types available.

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

All: Log all entries.

4.3.5.2.5.2 VLAN Configuration

VLAN Mode Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Log Type
☐		None

Add New Entry

Save Reset

VLAN ID: Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.

Log Type: There are four log types available.

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

All: Log all entries.

Click the "Add New Entry" button to insert an entry to the table.

Select the "Delete" checkbox to remove the entry during the next save.

Click the "Save" button to save newly-configured settings or changes.

Click the "Reset" button to restore settings to default settings or previously configured settings.

4.3.5.2.5.3 Static Table

Delete	Port	VLAN ID	MAC Address	IP Address
☐	1			

Port: Select a port to which a static entry is bound.

VLAN ID: Specify a configured VLAN ID.

MAC Address: Specify an allowed source MAC address in ARP request packets.

IP Address: Specify an allowed source IP address in ARP request packets.

Click the “Add New Entry” button to insert an entry to the table.

Select the “Delete” checkbox to remove the entry during the next save.

Click the “Save” button to save newly-configured settings or changes.

Click the “Reset” button to restore settings to default settings or previously configured settings.

4.3.5.2.5.4 Dynamic Table Configuration

Start from , VLAN , MAC address and IP address with entries per page.

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

Port: The port number of this entry.

VLAN ID: VLAN ID in which the ARP traffic is permitted.

MAC Address: User MAC address of this entry.

IP Address: User IP address of this entry.

Translate to static: Click the button to translate the dynamic entry to static one.

4.3.5.3 AAA

4.3.5.3.1 RADIUS Configuration

RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Add New Server						
Save	Reset					

Global Configuration

Timeout: The time the switch waits for a reply from an authentication server before it retransmits the request.

Retransmit: Specify the number of times to retransmit request packets to an authentication server that does not respond. If the server does not respond after the last retransmit is sent, the switch considers the authentication server is dead.

Deadtime: Deadtime is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. The allowed deadtime range is between 0 to 1440minutes.

Key: Specify the secret key up to 64 characters. This is shared between the RADIUS sever and the switch.

NAS-IP-Address: The IPv4 address is used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-IPv6-Address: The IPv6 address is used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS Identifier: The identifier, up to 256 characters long, is used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Sever Configuration

Hostname: The hostname or IP address for the RADIUS server.

Auth Port: The UDP port to be used on the RADIUS server for authentication.

Acct Port: The UDP port to be used on the RADIUS server for accounting.

Timeout: If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

Retransmit: If retransmit value is specified here, it will replace the global retransmit value. If you prefer to use the global value, leave this field blank.

Key: If secret key is specified here, it will replace the global secret key. If you prefer to use the global value, leave this field blank.

4.3.5.3.2 TACACS+

TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key		

Server Configuration

Delete	Hostname	Port	Timeout	Key
Delete		49		

Global Configuration

Timeout: The time the switch waits for a reply from a TACACS+ server before it retransmits the request.

Deadtime: Deadtime is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. The allowed deadtime range is between 0 to 1440minutes.

Key: Specify the secret key up to 63 characters. This is shared between a TACACS+ sever and the switch.

Server Configuration

Hostname: The hostname or IP address for a TACACS+ server.

Port: The TCP port number to be used on a TACACS+ server for authentication.

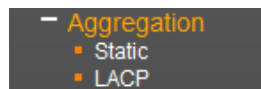
Timeout: If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

Key: If secret key is specified here, it will replace the global secret key. If you prefer to use the global value, leave this field blank.

4.3.6 Aggregation

Compared with adding cost to install extra cables to increase the redundancy and link speed, link aggregation is a relatively inexpensive way to set up a high-speed backbone network that transfers much more data than any one single port or device can deliver. Link aggregation uses multiple ports in parallel to increase the link speed. And there are two types of aggregation that are available, namely “Static” and “LACP”.

Under the Aggregation heading are two major icons, static and LACP.



4.3.6.1 Static

[illegible]

Aggregation Mode Configuration

Source MAC Address: All traffic from the same Source MAC address is output on the same link in a trunk.

Destination MAC Address: All traffic with the same Destination MAC address is output on the same link in a trunk.

IP Address: All traffic with the same source and destination IP address is output on the same link in a trunk.

TCP/UDP Port Number: All traffic with the same source and destination TCP/UDP port number is output on the same link in a trunk.

Aggregation Group Configuration

Group ID: Trunk ID number. "Normal" means that no aggregation is used. 16 aggregation groups are available for use. Each group contains at least 2 to 8 links (ports). Please note that each port can only be used once in Group ID 1~16.

Port Members: Select ports to belong to a certain trunk.

4.3.6.2 LACP

The Switch supports dynamic Link Aggregation Control Protocol (LACP) which is specified in IEEE 802.3ad. Static trunks have to be manually configured at both ends of the link. In other words, LACP configured ports can automatically negotiate a trunked link with LACP configured ports on another devices. You can configure any number of ports on the Switch as LACP, as long as they are not already configured as part of a static trunk. If ports on other devices are also configured as LACP, the Switch and the other devices will negotiate a trunk link between them.

LACP Port Configuration						
Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	 ▼		 ▼	 ▼	32768
1	☐	Auto ▼		Active ▼	Fast ▼	32768
2	☐	Auto ▼		Active ▼	Fast ▼	32768
3	☐	Auto ▼		Active ▼	Fast ▼	32768
4	☐	Auto ▼		Active ▼	Fast ▼	32768
5	☐	Auto ▼		Active ▼	Fast ▼	32768
6	☐	Auto ▼		Active ▼	Fast ▼	32768
7	☐	Auto ▼		Active ▼	Fast ▼	32768
8	☐	Auto ▼		Active ▼	Fast ▼	32768
9	☐	Auto ▼		Active ▼	Fast ▼	32768
10	☐	Auto ▼		Active ▼	Fast ▼	32768
11	☐	Auto ▼		Active ▼	Fast ▼	32768
12	☐	Auto ▼		Active ▼	Fast ▼	32768
13	☐	Auto ▼		Active ▼	Fast ▼	32768
14	☐	Auto ▼		Active ▼	Fast ▼	32768
15	☐	Auto ▼		Active ▼	Fast ▼	32768
16	☐	Auto ▼		Active ▼	Fast ▼	32768
17	☐	Auto ▼		Active ▼	Fast ▼	32768
18	☐	Auto ▼		Active ▼	Fast ▼	32768
19	☐	Auto ▼		Active ▼	Fast ▼	32768
20	☐	Auto ▼		Active ▼	Fast ▼	32768

Port: The port number.

LACP Enabled: Enable LACP on a switch port.

Key: The “Auto” setting sets the key as appropriate by the physical link speed. Select “Specific” if you want a user-defined key value. The allowed key value range is 1~65535. Ports in an aggregated link group must have the same LACP port Key. In order to allow a port to join an aggregated group, the port Key must be set to the same value.

Role: The user can select either “Active” or “Passive” role depending on the device’s capability of negotiating and sending LACP control packets.

Ports that are designated as “Active” are able to process and send LACP control frames. Hence, this allows LACP compliant devices to negotiate the aggregated link so that the group may be changed dynamically as required. In order to add or remove ports from the group, at least one of the participating devices must set to “Active” LACP ports.

On the other hand, LACP ports that are set to “Passive” cannot send LACP control frames. In order to allow LACP-enabled devices to form a LACP group, one end of the connection must designate as “Passive” LACP ports.

Timeout: The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

Prio: The priority of the port. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

4.3.7 Loop Protection

Loops sometimes occur in a network due to improper connecting, hardware problem or faulty protocol settings. When loops are seen in a switched network, they consume switch resources and thus downgrade switch performance. Loop Protection feature is provided in this switch and can be enabled globally or on a per port basis. Using loop protection enables the switch to automatically detect loops on a network. Once loops are detected, ports received the loop protection packet from the switch can be shut down or looped events can be logged.

Loop Protection Configuration

General Settings

Global Configuration	
Enable Loop Protection	Disable ▾
Transmission Time	5 seconds
Shutdown Time	180 seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	☒	◁ ▽	◁ ▽
1	☒	Shutdown Port ▽	Enable ▽
2	☒	Shutdown Port ▽	Enable ▽
3	☒	Shutdown Port ▽	Enable ▽
4	☒	Shutdown Port ▽	Enable ▽
5	☒	Shutdown Port ▽	Enable ▽
6	☒	Shutdown Port ▽	Enable ▽
7	☒	Shutdown Port ▽	Enable ▽
8	☒	Shutdown Port ▽	Enable ▽
9	☒	Shutdown Port ▽	Enable ▽
10	☒	Shutdown Port ▽	Enable ▽
11	☒	Shutdown Port ▽	Enable ▽
12	☒	Shutdown Port ▽	Enable ▽
13	☒	Shutdown Port ▽	Enable ▽
14	☒	Shutdown Port ▽	Enable ▽
15	☒	Shutdown Port ▽	Enable ▽

General Settings

Enable Loop Protection: Enable or disable loop protection function.

Transmission Time: The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.

Shutdown Time: The period for which a port will be kept disabled. Valid values are 0 to 604800 seconds. 0 means that a port is kept disabled until next device restart.

Port Configuration

Port: List the number of each port. "Port *" settings apply to all ports.

Enable: Enable or disable the selected ports' loop protection function.

Action: When a loop is detected on a port, the loop protection will immediately take appropriate actions. Actions will be taken include "Shutdown Port", "Shutdown Port and Log" or "Log Only".

Shutdown Port: A loop-detected port is shutdown for a period of time configured in "Shutdown Time".

Shutdown Port and Log: A loop-detected port is shutdown for a period of time configured in “Shutdown Time” and the event is logged.

Log Only: The event is logged and the port remains enable.

Tx Mode: Enable or disable a port to actively generate loop protection PDUs or to passively look for looped PDUs.

4.3.8 Spanning Tree

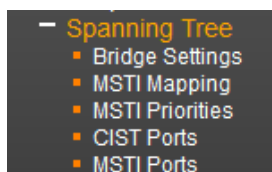
For some networking services, always-on connections are required to ensure that end users’ online related activities are not interrupted due to unexpected disconnections. In these circumstances, multiple active paths between network nodes are established to prevent disconnections from happening. However, multiple paths interconnected with each other have a high tendency to cause bridge loops that make networks unstable and in worst cases make networks unusable. For example, the MAC address table used by the switch or bridge can fail, since the same MAC addresses (and hence the same network hosts) are seen on multiple ports. Second, a broadcast storm occurs. This is caused by broadcast packets being forwarded in an endless loop between switches. A broadcast storm can consume all available CPU resources and bandwidth.

To solve problems causing by bridge loops, spanning tree allows a network design to include redundant links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manually enabling/disabling these backup links.

The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1s, can create a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches) and disable the links which are not part of that tree, leaving a single active path between any two network nodes.

To provide faster spanning tree convergence after a topology change, an evolution of the Spanning Tree Protocol “Rapid Spanning Tree Protocol (RSTP)”, is introduced by IEEE 802.1w. RSTP is a refinement of STP; therefore, it shares most of its basic operation characteristics. This essentially creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbors to determine if it can make a rapid transition. This is one of the major elements which allows RSTP to achieve faster convergence times than STP.

The other extension of RSTP is IEEE 802.1s Multiple Spanning Tree protocol (MSTP) that allows different VLANs to travel along separate instances of spanning tree. Unlike STP and RSTP, MSTP eliminates the needs for having different STP for each VLAN. Therefore, in a large networking environment that employs many VLANs, MSTP can be more useful than legacy STP.



4.3.8.1 Bridge Settings

STP Bridge Configuration	
Basic Settings	
Protocol Version	MSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6
Advanced Settings	
Edge Port BPDU Filtering	☐
Edge Port BPDU Guard	☐
Port Error Recovery	☐
Port Error Recovery Timeout	
Save Reset	

Basic Settings

Protocol Version: Select the appropriate spanning tree protocol. Protocol versions provided include “STP”, “RSTP”, and “MSTP”.

Bridge Priority: Each switch has a relative priority and cost that is used to decide what the shortest path is to forward a packet. The lowest cost path (lowest numeric value) has a higher priority and is always used unless it is down. If you have multiple bridges and interfaces then you need to adjust the priorities to achieve optimized performance. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay: For STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network. Valid values are 4-30 seconds.

Max Age: If another switch in the spanning tree does not send out a hello packet for a period of time, it is considered to be disconnected. Valid values are 6 to 40 seconds, and Max Age values must be smaller than or equal to (Forward Delay-1)*2.

Maximum Hop Count: The maximum number of hops allowed for MST region before a BPDU is discarded. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the BPDU is discarded. The default hop count is 20. The allowed range is 6-40.

Transmit Hold Count: The number of BPDU sent by a bridge port per second. When exceeded, transmission of the next BPDU will be delayed. By default, it is set to 6. The allowed transmit hold count is 1 to 10. Please note that increasing this value might have a significant impact on CPU utilization and decreasing this value might slow down convergence. It is recommended to remain Transmit Hold Count to the default setting.

Advanced Settings

Edge Port BPDU Filtering: The purpose of Port BPDU Filtering is to prevent the switch from sending BPDU frames on ports that are connected to end devices.

Edge Port BPDU Guard: Edge ports generally connect directly to PC, file servers or printers. Therefore, edge ports are configured to allow rapid transition. Under normal situations, edge ports should not receive configuration BPDUs. However, if they do, this probably is due to malicious attacks or mis-settings. When edge ports receive configuration BPDUs, they will be automatically set to non-edge ports and start a new spanning tree calculation process.

BPDU Guard is therefore used to prevent the device from suffering malicious attacks. With this function enabled, when edge ports receive configuration BPDUs, STP disables those affected edge ports. After a period of recovery time, those disabled ports are re-activated.

Port Error Recovery: When enabled, a port that is in the error-disabled state can automatically be enabled after a certain time.

Port Error Recovery Timeout: The time that has to pass before a port in the error-disabled state can be enabled. The allowed range is 30 – 86400 seconds.

4.3.8.2 MSTI Mapping

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification	
Configuration Name	00-01-c1-00-00-00
Configuration Revision	0

MSTI Mapping	
MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Configuration Identification

Configuration Name: The name for this MSTI. By default, the switch's MAC address is used. The maximum length is 32 characters. In order to share spanning trees for MSTI, bridges must have the same configuration name and revision value.

Configuration Revision: The revision number for this MSTI. The allowed range is 0 – 65535.

MSTI Mapping

MSTI: MSTI instance number.

VLAN Mapped: Specify VLANs mapped to a certain MSTI. Both a single VLAN and a range of VLANs are allowed. Separate VLANs with a comma and use hyphen to denote a range of VLANs. (Example: 2,5,20-40) Leave the field empty for unused MSTI.

4.3.8.3 MSTI Priorities

MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Save Reset

MSTI: Display MSTI instance number. “MSTI *” priority rule applies to all ports.

Priority: Select an appropriate priority for each MSTI instance. Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Note that lower numeric values indicate higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

4.3.8.4 CIST Ports

STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
*	☒	<>	<>	<>	☒	☐	☐	☐	<>
1	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
2	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
3	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
4	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
5	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
6	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
7	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
8	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
9	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
10	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
11	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
12	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
13	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
14	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto

CIST Aggregated Port Configuration

Port: The port number.

STP Enabled: Enable STP function

Path Cost: Path cost is used to determine the best path between devices. If “Auto” mode is selected, the system automatically detects the speed and duplex mode to decide the path cost. Select “Specific”, if you want to use user-defined value. Valid values are 1 to 200000000. Please note that path cost takes precedence over port priority.

Priority: Select port priority.

Admin Edge: If an interface is attached to end nodes, you can set it to “Edge”.

Auto Edge: Select the checkbox to enable this feature. When enabled, a port is automatically determined to be at the edge of the network when it receives no BPDUs.

Restricted Role: If enabled, this causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority.

Restricted TCN: If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

BPDU Guard: This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

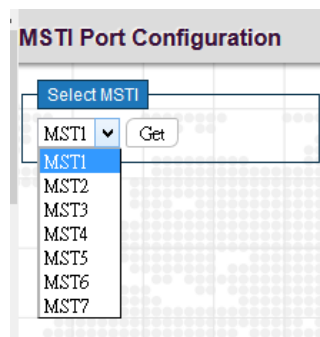
Point-to-Point: Select the link type attached to an interface.

Auto: The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

Forced True: It is a point-to-point connection.

Forced False: It is a shared medium connection.

4.3.8.5 MSTI Ports



Select a specific MSTI that you want to configure and then click the “Get” button.

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto	128

MSTI Normal Ports Configuration

Port	Path Cost	Priority
*	<	<
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128
5	Auto	128
6	Auto	128
7	Auto	128
8	Auto	128
9	Auto	128
10	Auto	128
11	Auto	128
12	Auto	128
13	Auto	128
14	Auto	128
15	Auto	128
16	Auto	128

Port: The port number.

Path Cost: Path cost is used to determine the best path between devices. If “Auto” mode is selected, the system automatically detects the speed and duplex mode to decide the path cost. Select “Specific”, if you want to use user-defined value. Valid values are 1 to 200000000. Please note that path cost take precedence over port priority.

Priority: Select port priority.

4.3.9 IPMC Profile

The "IPMC Profile" includes the following two sub menus.

- IPMC Profile
 - Profile Table
 - Address Entry

4.3.9.1 Profile Table

IPMC Profile Configurations

Global Profile Mode: Enabled

IPMC Profile Table Setting

Delete	Profile Name	Profile Description	Rule
☐	goldpass	for all channels	 

Add New IPMC Profile

Save Reset

IPMC Profile Configuration

Global Profile Mode: Enable or disable IPMC Profile feature globally.

IPMC Profile Table Setting

Profile Name: Enter a name for this profile.

Profile Description: Enter a brief description for this profile.

Click the "Add New IPMC Profile" to insert a new entry to the table.

Select the "Delete" checkbox to delete an entry.

Click the "e" button to edit this profile's detailed settings.

Profile Name & Index	Entry Name	Address Range	Action	Log
goldpass	1	-	Deny	Disable

Buttons: Add Last Rule, Commit, Reset

Icons: +, x, ↑, ↓

Profile Name & Index: Display the profile name and index.

Entry Name: The name used in specifying the address range. Only the existing profile address entries are selectable in the drop-down menu.

Address Range: Specify the multicast IP range. The available IP range is from 224.0.0.0~239.255.255.255

Action: Select the action taken upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Permit: Group address matches the range specified in the rule will be learned.

Deny: Group address matches the range specified in the rule will be dropped.

Log: Select the logging preference receiving the Join/Report frame that has the group address matches the address range of the rule.

Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.

Disable: Corresponding information of the group address, that matches the range specified in the rule, will not be logged.

You can manage rules and the corresponding precedence order by using the following buttons:

- : Insert a new rule before the current entry of rule.
- : Delete the current entry of rule.
- : Moves the current entry of rule up in the list.
- : Moves the current entry of rule down in the list.

4.3.9.2 Address Entry

IPMC Profile Address Configuration

Navigate Address Entry Setting in IPMC Profile by entries per page.

Delete	Entry Name	Start Address	End Address
☐	e1	224.0.0.1	239.0.0.1
Delete			

Entry Name: Enter a name which is used for indexing the address entry table.

Start Address: Enter the starting IPv4 or IPv6 multicast address used in this address range.

End Address: Enter the ending IPv4 or IPv6 multicast address used in this address range.

Click the "Add new Address (Range) Entry" button to insert a new entry.

Select the "Delete" checkbox to delete an entry during the next save.

4.3.10 MVR

Multicast VLAN Registration (MVR) protocol allows media servers to transmit multicast stream in a single multicast VLAN. Clients that receive multicast VLAN stream can reside in different VLANs. They can join or leave the multicast group simply by sending the IGMP Join or Leave message to a receiver port that belongs to one of the multicast groups can receive multicast stream from the media server.

MVR further isolates users who are not intended to receive multicast traffic and hence provide data security by VLAN segregation that allows only multicast traffic into other VLANs to which the subscribers belong. Even though common multicast streams are passed onto different VLAN groups from the MVR VLAN, users in different IEEE 802.1Q or private VLANs cannot exchange any information (except through upper-level routing services).

MVR Configurations

MVR Mode

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile																									
Delete	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
Role																																	

Immediate Leave Setting

Port	Immediate Leave
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled

MVR Configurations

MVR Mode: Enable or disable MVR feature globally on this device. Any multicast data from source ports will be sent to associated receiver ports registered in the table. By default, MVR feature is turned off.

VLAN Interface Setting

MVR ID: Specify multicast VLAN ID. Please note that MVR source ports are not recommended to be used as management VLAN ports. MVR source ports should be configured as members of the MVR VLAN, but MVR receiver ports should not be manually configured as members of this VLAN.

MVR Name: Optionally specify a user-defined name for this multicast VLAN. The maximum length of the MVR name string is 32. Both alphabets and numbers are allowed for use.

IGMP Address: Specify the IPv4 unicast address as source address used in IP header for IGMP control frames.

Mode: Two MVR operation modes are provided.

Dynamic: MVR allows dynamic MVR membership reports on source ports. (This is the default mode.)

Compatible: MVR membership reports are forbidden on source ports.

Tagging: Specify whether IGMP/MLD control frames will be sent tagged with MVR VID or untagged.

Priority: Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0 -7.

LLQI: LLQI stands for Last Listener Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. By default, LLQI is set to 5 tenths of a second (0.5 second). The allowed range is 0 – 31744 tenths of a second.

Interface Channel Profile: Select an IPMC profile from the drop-down menu. Click the  button to view a summary about the selected IPMC profile settings.

Port Role: Click the Port Role symbol to change the role status.

Inactive (I): By default, all ports are set to inactive. Inactive ports do not participate in MVR operations.

Source (S): Set a port (uplink ports) to source port. Source ports will receive and send multicast data. Subscribers can not directly be connected to source ports. Please also note that source ports cannot be management ports at the same time.

Receiver (R): Set a port to receiver port. Client or subscriber ports are configured to receiver ports so that they can issue IGMP/MLD messages to receive multicast data.

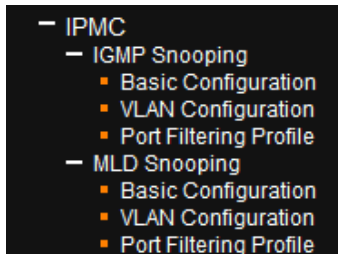
Immediate Leave Setting

Port: The port number. "Port *" rule applies to all ports.

Immediate Leave: Enable for disable immediate leave function. When enabled, the device immediately removes a port from a multicast stream as soon as it receives leave message for that group. This option only applies to an interface configured as MVR receivers.

4.3.11 IPMC

The “IPMC” menu includes IGMP Snooping and MLD Snooping sub menu. Select the appropriate menu to set up detailed configurations.



4.3.11.1 IGMP Snooping

The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used more efficiently when supporting activities, such as, online streaming video and gaming.

IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers by processing the layer 3 packets that IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch, it analyses all the IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch receives an IGMP report for a given multicast group from a host, the switch adds the host's port number to the multicast list for that group. When the switch hears an IGMP Leave, it removes the host's port from the table entry.

IGMP snooping can reduce multicast traffic from streaming and other bandwidth intensive IP applications more effectively. A switch using IGMP snooping will only forward multicast traffic to the hosts in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also decreases the workload at the end hosts since their network cards (or operating system) will not receive and filter all the multicast traffic generated in the network.

4.3.11.1.1 Basic Configuration

IGMP Snooping Configuration

Global Configuration

Snooping Enabled	☐
Unregistered IPMCv4 Flooding Enabled	☒
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	☐
Proxy Enabled	☐

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited
7	☐	☐	unlimited
8	☐	☐	unlimited
9	☐	☐	unlimited
10	☐	☐	unlimited
11	☐	☐	unlimited
12	☐	☐	unlimited
13	☐	☐	unlimited
14	☐	☐	unlimited
15	☐	☐	unlimited
16	☐	☐	unlimited

Global Configuration

Snooping Enabled: Select the checkbox to globally enable IGMP Snooping feature. When enabled, this device will monitor network traffic and determine which hosts will receive multicast traffic. The switch can passively monitor or snoop on IGMP Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

Unregistered IPMCv4 Flooding Enabled: Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

IGMP SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Leave Proxy Enabled: Suppresses leave messages unless received from the last member port in the group. IGMP leave proxy suppresses all unnecessary IGMP leave messages so that a non-querier switch forwards an IGMP leave packet only when the last dynamic member port leaves a multicast group.

Proxy Enabled: When enabled, the switch performs like “IGMP Snooping with Proxy Reporting” (as defined in DSL Forum TR-101, April 2006).

Port Related Configuration

Port: The port number.

Router Port: Tick the checkbox on a given port to assign it as a router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Fast Leave: Enable fast leave function if the checkbox is ticked. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

Throttling: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. Other allowed options are 1 – 10

4.3.11.1.2 VLAN Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Delete	1	☐	☒	0.0.0.0	IGMP-Auto	0	2	125	100	10	1

Add New IGMP VLAN

Save Reset

This page is used to configure IGMP Snooping for an interface.

Click the “Add New IGMP VLAN” button to add a new entry.

VLAN ID: Specify VLAN ID for IGMP snooping.

Snooping Enabled: Select the checkbox to enable snooping feature on an interface basis. When enabled, the switch will monitor network traffic on the specified interface to determine which hosts want to receive multicast services. If IGMP snooping is enabled globally and an interface’s IGMP snooping is enabled on an interface, IGMP snooping on an interface will take precedence. When disabled, snooping can still be configured on an interface. However, settings will only take effect until IGMP snooping is enabled globally.

Querier Election: Enable to join querier election in the VLAN. When disabled, it will act as an IGMP non-querier.

Querier Address: Specify the IPv4 unicast source address used in IP header for IGMP querier election. When the field is not specified, the switch uses the first available IPv4 management address of the IP interface associated with this VLAN.

Compatibility: This configures how hosts and routers take actions within a network depending on IGMP version selected. Available options are “IGMP-Auto”, “Forced IGMPv1”, “Forced IGMPv2”, “Forced IGMPv3”. By default, IGMP-Auto is used.

PRI: Select the priority of interface. This field indicates the IGMP control frame priority level generated by the system which is used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest). By default, interface priority value is set to 0.

RV: The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

QI (sec): The Query Interval is the interval between IGMP General Query messages sent by the Querier. The default Querier Interval is 125 seconds.

QRI: The Query Response Interval is the maximum amount of time that the IGMP router waits to receive a response to a General Query message. The QRI applies when the switch is acting as the querier and is used to inform other devices of the maximum time this system waits for a response to general queries. By default, RQI is set to 10 seconds. The allowed range is 10 – 31744 tenths of a second.

LLQI: The Last Listener Query Interval sets the interval that waits for a response to a group-specific or group-and-source specific query message.

URI: The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. By default, URI is set to 1 second. The allowed range for URI is 0 -31744 seconds.

4.3.11.1.3 Port Filtering Profile

The Port Filtering Configuration page is to filter specific multicast traffic on a per port basis. Before you select a filtering profile for filtering purposes, you must set up profiles in IPMC Profile page.

Port	Filtering Profile
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-
25	-

Port: The port number.

Filtering Profile: Select the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, IGMP join reports received on a port are dropped.

: Click the summary button to view details of the selected IPMC profile.

4.3.11.2 MLD Snooping

Multicast Listener Discovery (MLD) snooping, similar to IGMP snooping for IPv4, operates on IPv6 for multicast traffic. In other words, MLD snooping configures ports to limit or control IPv6 multicast traffic so that multicast traffic is forwarded to ports (or users) who want to receive it. In this way, MLD snooping can reduce the flooding of IPV6 multicast packets in the specified VLANs. Please note that IGMP Snooping and MLD Snooping are independent of each other. They can both be enabled and function at the same time.

4.3.11.2.1 Basic Configuration

MLD Snooping Configuration			
Global Configuration			
Snooping Enabled	☐		
Unregistered IPMCv6 Flooding Enabled	☒		
MLD SSM Range	ff3e:: / 96		
Leave Proxy Enabled	☐		
Proxy Enabled	☐		
Port Related Configuration			
Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited
7	☐	☐	unlimited
8	☐	☐	unlimited
9	☐	☐	unlimited
10	☐	☐	unlimited
11	☐	☐	unlimited
12	☐	☐	unlimited
13	☐	☐	unlimited
14	☐	☐	unlimited
15	☐	☐	unlimited
16	☐	☐	unlimited

Global Configuration

Snooping Enabled: Select the checkbox to globally enable MLD Snooping feature. When enabled, this device will monitor network traffic and determine which hosts would like to receive multicast traffic. The switch can passively monitor or snoop on MLD Listener Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

Unregistered IPMCv6 Flooding Enabled: Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

MLD SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Leave Proxy Enabled: To prevent multicast router from becoming overloaded with leave messages, MLD snooping suppresses leave messages unless received from the last member port in the group. When the switch acts as the querier, the leave proxy feature will not function.

Proxy Enabled: When MLD proxy is enabled, the switch exchanges MLD messages with the router on its upstream interface, and performs the host portion of the MLD task on the upstream interface as follows:

- When queried, it sends multicast listener reports to the group.
- When a host joins a multicast group to which no other host belongs, it sends unsolicited multicast listener reports to that group.
- When the last host in a particular multicast group leaves, it sends an unsolicited multicast listener done report to the all-routers address (FF02::2) for MLDv1.

Port Related Configuration

Port: The port number.

Router Port: Tick the checkbox on a given port to assign it as a router port. If MLD snooping cannot locate the MLD querier, you can manually designate a port which is connected to a known MLD querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch

to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Fast Leave: Enable fast leave function if the checkbox is ticked. When a leave packet is received, the switch immediately removes it from a multicast service without sending a MLD group-specific (GS) query to that interface.

Throttling: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new MLD join reports will be dropped. By default, unlimited is selected. Other allowed options are 1 – 10.

4.3.11.2.2 VLAN Configuration

MLD Snooping VLAN Configuration

Start from VLAN with entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Delete		☐	☒	MLD-Auto	0	2	125	100	10	1

This page is used to configure MLD Snooping for an interface.

VLAN ID: Specify VLAN ID for MLD snooping.

Snooping Enabled: Select the checkbox to enable snooping feature on an interface basis. When enabled, the switch will monitor network traffic on the specified interface to determine which hosts want to receive multicast services.

Querier Election: Enable to join querier election in the VLAN. When enabled, the switch can serve as the MLDv2 querier in the bidding process with other competing multicast routers or switches. Once it becomes querier, it will be responsible for asking hosts periodically if they want to receive multicast traffic. When disabled, it will act as an IGMP non-querier.

Compatibility: This configures how hosts and routers take actions within a network depending on MLD version selected. Available options are “MLD-Auto”, “Forced MLDv1” and “Forced MLDv2”. By default, MLD-Auto is used.

PRI: Select the priority of interface. This field indicates the MLD control frame priority level generated by the system which is used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest). By default, interface priority value is set to 0.

RV: The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2. The allowed range is 1 -255.

QI (sec): The Query Interval is the interval between IGMP General Query messages sent by the Querier. The default Querier Interval is 125 seconds. The allowed interval range is 1 – 255 seconds.

QRI: The Query Response Interval is the maximum amount of time that the IGMP router waits to receive a response to a General Query message. The QRI applies when the switch is acting as the querier and is used to inform other devices of the maximum time this system waits for a response to general queries. By default, RQI is set to 10 seconds. The allowed range is 10 – 31744 tenths of a second.

LLQI: The Last Listener Query Interval sets the interval that waits for a response to a group-specific or group-and-source specific query message.

URI: The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. By default, URI is set to 1 second. The allowed range for URI is 0 -31744 seconds.

Click the “Add New MLD VLAN” button to add a new entry.

4.3.11.2.3 Port Filtering Profile

The Port Filtering Configuration page is to filter specific multicast traffic on a per port basis. Before you select a filtering profile for filtering purposes, you must set up profiles in IPMC Profile page.

MLD Snooping Port Filtering Profile Configuration		
Port		Filtering Profile
1		-
2		-
3		-
4		-
5		-
6		-
7		-
8		-
9		-
10		-
11		-
12		-
13		-
14		-
15		-
16		-
17		-
18		-
19		-
20		-
21		-
22		-
23		-
24		-
25		-

Port: List the number of each port.

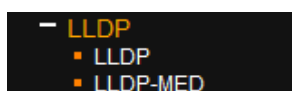
Filtering Profile: Select the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, MLD join reports received on a port are dropped.

: Click the summary button to view details of the selected IPMC profile.

4.3.12 LLDP

LLDP (Link Layer Discovery Protocol) runs over data link layer which is used for network devices to send information about themselves to other directly connected devices on the network. By using LLDP, two devices running different network layer protocols can learn information about each other. A set of attributes referred to TLVs are used to discover neighbour devices. Details such as port description, system name, system description, system capabilities, management address can be sent and received on this device.

The “LLDP” menu contains the following sub menus. Select the appropriate menu to set up detailed configurations.



4.3.12.1 LLDP Configuration

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Interface Configuration

Interface	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
GigabitEthernet 1/1	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/2	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/3	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/4	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/5	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/6	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/7	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/8	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/9	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/10	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/11	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/12	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/13	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/14	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/15	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/16	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/17	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/18	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/19	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/20	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/21	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/22	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/23	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/24	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/25	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/26	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/27	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/28	Enabled	☐	☒	☒	☒	☒	☒
10GigabitEthernet 1/1	Enabled	☐	☒	☒	☒	☒	☒
10GigabitEthernet 1/2	Enabled	☐	☒	☒	☒	☒	☒
10GigabitEthernet 1/3	Enabled	☐	☒	☒	☒	☒	☒
10GigabitEthernet 1/4	Enabled	☐	☒	☒	☒	☒	☒
GigabitEthernet 1/29	Enabled	☐	☒	☒	☒	☒	☒

Save Reset

LLDP Parameters

Tx Interval: Specify the interval between LLDP frames are sent to its neighbors for updated discovery information. The valid values are 5 - 32768 seconds. The default is 30 seconds.

Tx Hold: This setting defines how long LLDP frames are considered valid and is used to compute the TTL. Valid range is 2~10 times. The default is 4.

Tx Delay: Specify a delay between the LLDP frames that contain changed configurations. Tx Delay cannot be larger than 1/4 of the Tx interval value. The valid values are 1 - 8192 seconds.

Tx Reinit: Specify a delay between the shutdown frame and a new LLDP initialization. The valid values are 1 - 10 seconds.

LLDP Port Configuration

Interface: This shows the "interface name" of each port. "*" settings apply to all ports. The Interface/Port mapping table for firmware version 1.007 or newer is as follows:

** If your firmware version is below 1.007, please contact your sales representatives for firmware updates.

Panel Mylar Port No. Printing	Interface (CLI)	Port No. (WEB)
1	GigabitEthernet 1/1	1
2	GigabitEthernet 1/2	2
3	GigabitEthernet 1/3	3
4	GigabitEthernet 1/4	4
5	GigabitEthernet 1/5	5
6	GigabitEthernet 1/6	6
7	GigabitEthernet 1/7	7
8	GigabitEthernet 1/8	8
9	GigabitEthernet 1/9	9
10	GigabitEthernet 1/10	10
11	GigabitEthernet 1/11	11
12	GigabitEthernet 1/12	12
13	GigabitEthernet 1/13	13
14	GigabitEthernet 1/14	14
15	GigabitEthernet 1/15	15
16	GigabitEthernet 1/16	16
17	GigabitEthernet 1/17	17
18	GigabitEthernet 1/18	18
19	GigabitEthernet 1/19	19
20	GigabitEthernet 1/20	20
21	GigabitEthernet 1/21	21
22	GigabitEthernet 1/22	22
23	GigabitEthernet 1/23	23
24	GigabitEthernet 1/24	24
25	GigabitEthernet 1/25	25
26	GigabitEthernet 1/26	26
27	GigabitEthernet 1/27	27
28	GigabitEthernet 1/28	28
1 29	10GigabitEthernet 1/1	29
2 30	10GigabitEthernet 1/2	30
3 31	10GigabitEthernet 1/3	31
4 32	10GigabitEthernet 1/4	32
MGMT	GigabitEthernet 1/29	33

Mode: Select the appropriate LLDP mode.

Disabled: LLDP information will not be sent and LLDP information received from neighbours will be dropped.

Enabled: LLDP information will be sent and LLDP information received from neighbours will be analyzed.

Rx Only: The switch will analyze LLDP information received from neighbours.

Tx Only: The switch will send out LLDP information but will drop LLDP information received from neighbours.

CDP Aware: CDP aware operation is used to decode incoming CDP (Cisco Discovery Protocol) frames. If enabled, CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded, all others are discarded. CDP TLVs are mapped into LLDP neighbors table as shown below:

Optional TLVs: LLDP uses several attributes to discover neighbour devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent from this device. Uncheck the boxes if they are not appropriate to be known by other neighbour devices.

4.3.12.2 LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, inventory management and location information. (See above for the interface/port mapping table.)

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count:

Transmit TLVs

Interface	Capabilities	Policies	Location
GigabitEthernet 1/1	☒	☒	☒
GigabitEthernet 1/2	☒	☒	☒
GigabitEthernet 1/3	☒	☒	☒
GigabitEthernet 1/4	☒	☒	☒
GigabitEthernet 1/5	☒	☒	☒
GigabitEthernet 1/6	☒	☒	☒
GigabitEthernet 1/7	☒	☒	☒
GigabitEthernet 1/8	☒	☒	☒
GigabitEthernet 1/9	☒	☒	☒
GigabitEthernet 1/10	☒	☒	☒
GigabitEthernet 1/11	☒	☒	☒
GigabitEthernet 1/12	☒	☒	☒
GigabitEthernet 1/13	☒	☒	☒
GigabitEthernet 1/14	☒	☒	☒
GigabitEthernet 1/15	☒	☒	☒
GigabitEthernet 1/16	☒	☒	☒

2.5GigabitEthernet 1/1	☒	☒	☒
2.5GigabitEthernet 1/2	☒	☒	☒
2.5GigabitEthernet 1/3	☒	☒	☒
2.5GigabitEthernet 1/4	☒	☒	☒
2.5GigabitEthernet 1/5	☒	☒	☒
2.5GigabitEthernet 1/6	☒	☒	☒
2.5GigabitEthernet 1/7	☒	☒	☒
2.5GigabitEthernet 1/8	☒	☒	☒
GigabitEthernet 1/17	☒	☒	☒
GigabitEthernet 1/18	☒	☒	☒
GigabitEthernet 1/19	☒	☒	☒
GigabitEthernet 1/20	☒	☒	☒
10GigabitEthernet 1/1	☒	☒	☒
10GigabitEthernet 1/2	☒	☒	☒
10GigabitEthernet 1/3	☒	☒	☒
10GigabitEthernet 1/4	☒	☒	☒
GigabitEthernet 1/21	☒	☒	☒

Coordinates Location

Latitude 0 ° North Longitude 0 ° East Altitude 0 Meters Map Datum WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

Add New Policy

Fast Start Repeat Count

Fast Start Repeat Count: Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDP space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind, LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. With Fast start repeat count it is possible to specify the number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including between Network Connectivity Devices, or to other types of links.

Transmit TLVs

Select which LLDP-MED information that shall be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.

Coordinates Location

Latitude: Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.

Longitude: Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude: Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters).

Meters: Representing meters of Altitude defined by the vertical datum specified.

Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum: The Map Datum is used for the coordinates given in these options:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Country Code: The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

State: National subdivisions (state, canton, region, province, prefecture).

County: County, parish, gun (Japan), district.

City: City, township, shi (Japan) - Example: Copenhagen.

City District: City division, borough, city district, ward, chou (Japan).

Block (Neighbourhood): Neighbourhood, block.

Street: Street - Example: Poppelvej.

Leading street direction: Example: N.

Trailing street suffix: Example: SW.

Street suffix: Example: Ave, Platz.

House no.: Example: 21.

House no. suffix: Example: A, 1/2.

Landmark: Landmark or vanity address - Example: Columbia University.

Additional location info: Example: South Wing.

Name: Name (residence and office occupant): Example: Flemming Jahn.

Zip code: Postal/zip code - Example: 2791.

Building: Building (structure). Example: Low Library.

Apartment: Unit (Apartment, suite). Example: Apt 42.

Floor: Example: 4.

Room no.: Room number - Example: 450F.

Place type: Example: Office.

Postal community name: Example: Leonia.

P.O. Box: Example: 12345.

Additional code: Example: 1320300003.

Emergency Call Service

Emergency Call Service: Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Policies

Policy ID: Specify the ID for this policy.

Application Type: The application types include “Voice”, “Voice Signalling”, “Guest Voice”, “Guest Voice Signalling”, “Softphone Voice”, “Video Conferencing”, “Streaming”, “Video Signalling”.

Tag: Tag indicating whether the specified application type is using a “tagged” or an “untagged” VLAN.

VLAN ID: Specify the VLAN ID for the port.

L2 Priority: Specify one of eight priority levels (0-7) as defined by 802.1D-2004.

DSCP: Specify one of 64 code point values (0-63) as defined in IETF RFC 2474.

4.3.13 MAC Table

Aging Configuration

Disable Automatic Aging: Learned MAC addresses will appear in the table permanently.

Aging Time: Set up the aging time for a learned MAC to be appeared in MAC learning table. The allowed range is 10 to 1000000 seconds.

MAC Learning Table

MAC Learning Table: Three options are available on each port.

Auto: On a given port, learning is automatically done once unknown SMAC is received.

Disable: Disable MAC learning function.

Secure: Only static MAC entries listed in “Static MAC Table Configuration” are learned. Others will be dropped.

NOTE: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

Static MAC Table Configuration: This table is used to manually set up static MAC entries. The total entries that can be entered are 64.

Delete: Delete this MAC address entry.

VLAN ID: Specify the VLAN ID for this entry.

Port Members: Check or uncheck the ports. If the incoming packet has the same destination MAC address as the one specified in VID, it will be forwarded to the checked port directly.

4.3.14 VLANs

IEEE 802.1Q VLAN (Virtual Local Area Network) is a popular and cost-effectively way to segment your networking deployment by logically grouping devices with similar attributes irrespective of their physical connections. VLANs also segment the network into different broadcast domains so that packets are forwarded to ports within the VLAN that they belong. Using VLANs provides the following main benefits:

VLANs provide extra security: Devices that frequently communicate with each other are grouped into the same VLAN. If devices in a VLAN want to communicate with devices in a different VLAN, the traffic must go through a routing device or Layer 3 switching device.

VLANs help control traffic: Traditionally, when networks are not segmented into VLANs, congestion can be easily caused by broadcast traffic that is directed to all devices. To minimize the possibility of broadcast traffic damaging the entire network, VLANs can help group devices that communicate frequently with other in the same VLAN so as to divide the entire network into several broadcast domains.

VLANs make changes of devices or relocation more easily: In traditional networks, when moving a device geographically to a new location (for example, move a device in floor 2 to floor 4), the network administrator may need to change the IP or even subnet of the network or require re-cabling. However, by using VLANs, the original IP settings can remain the same and re-cabling can be reduced to minimal.

Global VLAN Configuration								
Allowed Access VLANs		1						
Ethertype for Custom S-ports		88A8						
Port VLAN Configuration								
Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
1	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
2	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
7	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
11	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
12	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
13	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
14	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
15	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
16	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
17	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	

Global VLAN Configuration

Allowed Access VLANs: This shows the allowed access VLANs. This setting only affects ports set in “Access” mode. Ports in other modes are members of all VLANs specified in “Allowed VLANs” field. By default, only VLAN 1 is specified. More allowed access VLANs can be entered by specifying the individual VLAN ID separated by comma. If you want to specify a range, separate it by a dash. For example, 1, 5, 10, 12-15, 100

Ethertype for Custom S-ports: Specify ether type used for customer s-ports.

Port VLAN Configuration

Port: List the number of each port. “Port *” settings apply to all ports.

Mode: The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied.

Access: Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:

- Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1.
- Accepts untagged and C-tagged frames.
- Discards all frames that are not classified to the Access VLAN.
- On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged.

Trunk: Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:

- By default, a trunk port is member of all VLANs (1-4095).
- The VLANs that a trunk port is member of may be limited by the use of “Allowed VLANs”.

- Frames classified to a VLAN that the port is not a member of are discarded.
- By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress.
- Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress.

Hybrid: Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware.
- Ingress filtering can be controlled.
- Ingress acceptance of frames and configuration of egress tagging can be configured independently.

Port VLAN: Configures the VLAN identifier for the port. The allowed values are from 1 through 4095. The default value is 1.

The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

Port Type: When you select "Hybrid" mode, the Port Type field becomes selectable. There are four port types available. Each port type's ingress and egress action is described in the following table.

Action Port Type	Ingress Action	Egress Action
Unaware	When a tagged frame is received on a port, 3. If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded. 4. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing are also affected by egress rule.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
C-port	When a tagged frame is received on a port, 3. If a tagged frame with TPID=0x8100, it is forwarded. 4. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by C-port will be set to 0x8100.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-port	When a tagged frame is received on a port, 3. If a tagged frame with TPID=0x88A8, it is forwarded. 4. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TPID of frame transmitted by S-port will be set to 0x88A8
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-custom port	When a tagged frame is received on a port, 3. If a tagged frame with TPID=0x88A8, it is forwarded. 4. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TPID of frame transmitted by S-custom-port will be set to an self-customized value, which can be set by the user using the column of Ethertype for Custom S-ports.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	

Ingress Filtering: If Ingress Filtering is enabled and the ingress port is not a member of a VLAN, the frame from the ingress port is discarded. By default, ingress filtering is disabled.

Ingress Acceptance: Select the acceptable ingress traffic type on a port.

Tagged and Untagged: Both tagged and untagged ingress packets are acceptable on a port.

Tagged Only: Only tagged ingress packets are acceptable on a port. Untagged packets will be dropped.

Untagged Only: Only untagged ingress packets are acceptable on a port. Tagged packets will be dropped.

Egress Tagging: The action taken when packets are sent out from a port.

Untag Port VLAN: Frames that carry PVID will be removed when leaving from a port. Frames with tags other than PVID will be transmitted with the carried tags.

Tag All: Frames are transmitted with a tag.

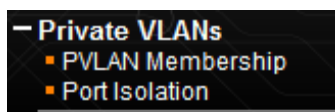
Untag All: Frames are transmitted without a tag. This option is only available for ports in Hybrid mode.

Allowed VLAN: Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095.

Forbidden VLAN: A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

4.3.15 Private VLANs

The “Private VLANs” menu contains the following sub menus. Select the appropriate one to configure its detailed settings.



4.3.15.1 PVLAN Membership

The screenshot shows the "Private VLAN Membership Configuration" page. At the top right, there are "Auto-refresh" and "Refresh" buttons. Below is a table with columns for "Delete", "PVLAN ID", and "Port Members" (ports 1 through 33). The first row shows PVLAN ID 1 with checkboxes for all ports. Below the table, there is an "Add New Private VLAN" button, and "Save" and "Reset" buttons.

This page is used to configure private VLANs. New Private VLANs can be added here and existing VLANs can be modified. Private VLANs are based on the source port mask and there are no connections to VLANs which means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

PVLAN ID: Specify the PVLAN ID. Valid values are 1 to 11.

Port Members: Select the checkbox, if you would like a port to belong to a certain Private VLAN. Uncheck the checkbox to remove a port from a Private VLAN.

Delete: Delete this VLAN membership entry.

Add New VLAN: Click the button once to add a new VLAN entry.

Save: VLAN membership changes will be saved and new VLANs are enabled after clicking “Save” button.

Reset: Click “Reset” button to clear all unsaved VLAN settings and changes.

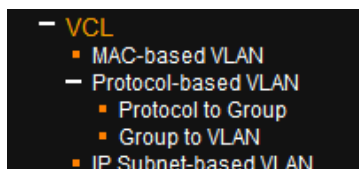
4.3.15.2 Port Isolation

Private VLAN is used to group ports together so as to prevent communications within PVLAN. Port Isolation is used to prevent communications between customer ports in a same Private VLAN. The port that is isolated from others cannot forward any unicast, multicast or broadcast traffic to any other ports in the same PVLAN.

Port Number: Select the checkbox if you want a port or ports to be isolated from other ports.

4.3.16 VCL

The “VCL” menu contains the following sub menus.



4.3.16.1 MAC-based VLAN

MAC-based VLAN configuration page is to set up VLANs based on source MAC addresses. When ingress untagged frames are received by a port, source MAC address is processed to decide which VLAN these untagged frames belong. When source MAC addresses does not match the rules created, untagged frames are assigned to the receiving port’s native VLAN ID (PVID).

MAC Address: Indicate the source MAC address. Please note that the source MAC address can only map to one VLAN ID.

VLAN ID: Map this MAC address to the associated VLAN ID.

Port Members: Ports that belong to this VLAN.

Save: Changes will be saved and newly entered rules are enabled after clicking “Save” button.

Click “Add New Entry” to create a new rule.

Delete: Click “Delete” to remove this entry.

4.3.16.2 Protocol-based VLAN

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including

security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

4.3.16.2.1 Protocol to Group

The figure shows three sequential screenshots of a web-based configuration interface titled "Protocol to Group Mapping Table". Each screenshot displays a table with four columns: "Delete", "Frame Type", "Value", and "Group Name".

- Top Screenshot:** The "Frame Type" is set to "Ethernet". The "Value" field contains "Etype: 0x0800".
- Middle Screenshot:** The "Frame Type" is set to "SNAP". The "Value" field contains "OUI: 0x00-B0-2E PID: 0x0000".
- Bottom Screenshot:** The "Frame Type" is set to "LLC". The "Value" field contains "DSAP: 0xFF SSAP: 0xFF".

Below each table, there are three buttons: "Add New Entry", "Save", and "Reset".

Frame Type: There are three frame types available for selection; these are "Ethernet", "SNAP", and "LLC". The value field will change accordingly.

Value: This field specifically indicates the protocol type. This value field varies depending on the frame type you selected.

Ethernet: Ether Type (etype) value. By default, it is set to 0x0800. The range allowed is 0x0600 to 0xffff.

SNAP: This includes OUI (Organizationally Unique Identifier) and PID (Protocol ID) values.

OUI: A value in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value in the ranges of 0x00-0xff.

PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

LLC (Logical Link Control): This includes DSAP (Destination Service Access Point) and SSAP (Source Service Access Point) values. By default, the value is 0xff. Valid range is 0x00 to 0xff.

Group Name: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

4.3.16.2.2 Group to VLAN

Group Name to VLAN mapping Table																																			
Auto-refresh ☐ Refresh																																			
Delete	Group Name	VLAN ID	Port Members																																
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
Currently no entries present in the switch																																			
Add New Entry Save Reset																																			

Group Name: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

VLAN ID: Indicate the VLAN ID.

Port Members: Assign ports to this rule.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

4.3.16.3 IP Subnet-based VLAN

IP Subnet-based VLAN configuration is to map untagged ingress frames to a specific VLAN if the source address is found in the IP subnet-to-VLAN mapping table. When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port’s VLAN ID (PVID).

IP Subnet-based VLAN Membership Configuration																																				
Auto-refresh ☐ Refresh																																				
Delete	IP Address	Mask Length	VLAN ID	Port Members																																
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
Currently no entries present																																				
Add New Entry Save Reset																																				

VCE ID: Index of the entry. Valid range is 0-256.

IP Address: Indicate the IP address for this rule.

Mask Length: Indicate the network mask length.

VLAN ID: Indicate the VLAN ID

Port Members: Assign ports to this rule.

Click the “Add New Entry” button to insert a new entry to the list.

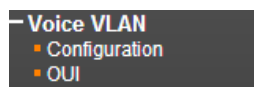
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

4.3.17 Voice VLAN

Nowadays, in the enterprise network, VoIP devices are commonly deployed to save operational cost due to its easy-to-setup feature and convenience. However, while deploying VoIP devices, it is recommended that VoIP traffic is separated from data traffic. By isolating traffic, VoIP traffic can be assigned to have the highest priority while forwarding so that higher voice quality can be achieved without encountering situations like excessive packet delays, packet loss, and jitters. Moreover,

This switch provides Voice VLAN feature that enables voice traffic to be forwarded on the voice VLAN. The user can also overwrite traffic priority by assigning higher traffic class value to voice traffic. Voice traffic can be detected on a port by using LLDP (IEEE 802.1ab) to discover VoIP devices attached to the switch or from devices' OUI (Organizationally Unique Identifier). When voice packets are detected on a port, the switch automatically assigns the port as a tagged member of the Voice VLAN and forward packets based on configurations set in Voice VLAN configuration page.

The Voice VLAN section provides that following two sub menus:



4.3.17.1 Configuration

Voice VLAN Configuration

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
*	Disabled	Disabled	OUI
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI
11	Disabled	Disabled	OUI
12	Disabled	Disabled	OUI
13	Disabled	Disabled	OUI
14	Disabled	Disabled	OUI

Voice VLAN Configuration

Mode: Enable or disable Voice VLAN function on this switch.

VLAN ID: Assign a VLAN ID to this Voice VLAN. Only one Voice VLAN is supported on the switch. By default, VLAN 1000 is set. The allowed range is 1 - 4095.

Note:

1. The Voice VLAN cannot be the same as management VLAN, MVR VLAN, or the native VLAN assigned to any port.
2. MSTP must be disabled before the Voice VLAN is enabled or the Voice VLAN port mode is set to Auto or Forced. This prevents the spanning tree's ingress filter from dropping VoIP traffic tagged for the Voice VLAN.

Aging Time: The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. By default, the aging time is set to 86400 seconds. The allowed aging time is 10 – 10,000,000 seconds.

Traffic Class: Select the traffic class value which defines a service priority for traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new traffic class when the Voice VLAN feature is active on a port. By default, 7 (Highest priority) is used. The allowed range is 0 (Lowest) ~ 7 (Highest).

Port Configuration

Port: The port number. “All” rules apply to all ports.

Mode: Select whether a particular is enabled with Voice VLAN feature or not. There are three options available:

Disabled: Disable Voice VLAN feature on a particular port.

Auto: Enable the Voice VLAN auto detection mode. When voice (VoIP) traffic is detected on a port, the port will be added as a tagged member to the Voice VLAN. When Auto mode is selected, you need to further decide a method for detecting voice traffic in “Discovery Protocol” field, either OUI or LLDP (802.1ab).

Forced: Enable Voice VLAN feature on a particular port.

Security: Enable or disable security filtering feature on a per port basis. When enabled, any non-VoIP packets received on a port with Voice VLAN ID will be discarded. VoIP traffic is identified by source MAC addresses configured in the telephony OUI list or through LLDP which is used to discover VoIP devices attached to the switch.

Discovery Protocol: Select a method for detecting VoIP traffic. By default, OUI is used.

OUI: Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to manufacturers and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.

LLDP: Use LLDP (IEEE 802.1ab) to discover VoIP devices attached to a port. LLDP checks that the “telephone bit” in the system capability TLV is turned on or not.

Both: Use both OUI table and LLDP to detect VoIP traffic on a port.

4.3.17.2 OUI

Voice VLAN OUI Table		
Delete	Telephony OUI	Description
☐	00-01-e3	Siemens AG phones
☐	00-03-6b	Cisco phones
☐	00-0f-e2	H3C phones
☐	00-60-b9	Philips and NEC AG phones
☐	00-d0-1e	Pingtel phones
☐	00-e0-75	Polycom phones
☐	00-e0-bb	3Com phones

Telephony OUI: Specify your VoIP device’s OUI. It must be 6 characters long and the input format is “xx-xx-xx” (x is hexadecimal digit)

Description: Specify a descriptive comments or information to this entry.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

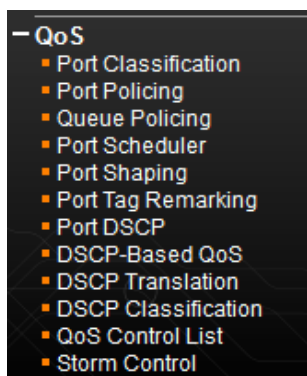
Click the “Reset” button to restore changed settings to the default settings.

4.3.18 QoS

Network traffic is always unpredictable and the only basic assurance that can be offered is the best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria and receives preferential treatments.

QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic. To set up the priority of packets in this switch, go to “Port Classification” page.

The “QoS” menu contains the following sub menus.



4.3.18.1 Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	WRED Group
1	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
2	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
3	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
4	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
5	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
6	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
7	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
8	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
9	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
10	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
11	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
12	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
13	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
14	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
15	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
16	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
17	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
18	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
19	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
20	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
21	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
22	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
23	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
24	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
25	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
26	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
27	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
28	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼
29	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	1 ▼

Port: List of the number of each port. "Port *" rules will apply to all ports.

CoS: Indicate the Class of Service level. A CoS class of 0 has the lowest priority. By Default, 0 is used.

DPL: Select the default Drop Precedence Level.

PCP: Select the appropriate value for the default Priority Code Point (or User Priority) for untagged frames.

DEI: Select the appropriate value for the default Drop Eligible Indicator for untagged frames.

Tag Class: This field displays classification mode for tagged frames on this port:

Disabled: Use the default QoS class and DP level for tagged frames.

Enabled: Use the mapped versions of PCP and DEI for tagged frames.

DSCP Based: Select the checkbox to enable DSCP based QoS (Ingress Port).

WRED Group: This setting controls WRED group membership.

4.3.18.2 Port Policing

Port	Enable	Rate	Unit	Flow Control
*	☐	500	<>	☐
1	☐	500	kbps	☐
2	☐	500	kbps	☐
3	☐	500	kbps	☐
4	☐	500	kbps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐
7	☐	500	kbps	☐
8	☐	500	kbps	☐
9	☐	500	kbps	☐
10	☐	500	kbps	☐
11	☐	500	kbps	☐
12	☐	500	kbps	☐
13	☐	500	kbps	☐
14	☐	500	kbps	☐
15	☐	500	kbps	☐
16	☐	500	kbps	☐
17	☐	500	kbps	☐
18	☐	500	kbps	☐
19	☐	500	kbps	☐
20	☐	500	kbps	☐
21	☐	500	kbps	☐
22	☐	500	kbps	☐
23	☐	500	kbps	☐
24	☐	500	kbps	☐
25	☐	500	kbps	☐
26	☐	500	kbps	☐
27	☐	500	kbps	☐
28	☐	500	kbps	☐

This page allows users to set each port's allowed bandwidth.

Port: The port number. "Port *" settings apply to all ports.

Enabled: Select the checkbox to enable port policing function on a port.

Rate: Indicate the rate for the policer. By default, 500kbps is used. The allowed range for kbps and fps is 100 to 1000000. The allowed range for Mbps and kfps is 1 to 3300Mbps.

Unit: Select the unit of measure for the policer.

Flow Control: If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

4.3.18.3 Queue Policing

QoS Ingress Queue Policers									
Port	Queue 0 Enable	Queue 1 Enable	Queue 2 Enable	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable	Queue 7 Enable	
*	☐	☐	☐	☐	☐	☐	☐	☐	
1	☐	☐	☐	☐	☐	☐	☐	☐	
2	☐	☐	☐	☐	☐	☐	☐	☐	
3	☐	☐	☐	☐	☐	☐	☐	☐	
4	☐	☐	☐	☐	☐	☐	☐	☐	
5	☐	☐	☐	☐	☐	☐	☐	☐	
6	☐	☐	☐	☐	☐	☐	☐	☐	
7	☐	☐	☐	☐	☐	☐	☐	☐	
8	☐	☐	☐	☐	☐	☐	☐	☐	
9	☐	☐	☐	☐	☐	☐	☐	☐	
10	☐	☐	☐	☐	☐	☐	☐	☐	
11	☐	☐	☐	☐	☐	☐	☐	☐	
12	☐	☐	☐	☐	☐	☐	☐	☐	
13	☐	☐	☐	☐	☐	☐	☐	☐	
14	☐	☐	☐	☐	☐	☐	☐	☐	
15	☐	☐	☐	☐	☐	☐	☐	☐	
16	☐	☐	☐	☐	☐	☐	☐	☐	
17	☐	☐	☐	☐	☐	☐	☐	☐	
18	☐	☐	☐	☐	☐	☐	☐	☐	
19	☐	☐	☐	☐	☐	☐	☐	☐	
20	☐	☐	☐	☐	☐	☐	☐	☐	
21	☐	☐	☐	☐	☐	☐	☐	☐	
22	☐	☐	☐	☐	☐	☐	☐	☐	
23	☐	☐	☐	☐	☐	☐	☐	☐	
24	☐	☐	☐	☐	☐	☐	☐	☐	
25	☐	☐	☐	☐	☐	☐	☐	☐	
26	☐	☐	☐	☐	☐	☐	☐	☐	
27	☐	☐	☐	☐	☐	☐	☐	☐	
28	☐	☐	☐	☐	☐	☐	☐	☐	
29	☐	☐	☐	☐	☐	☐	☐	☐	

Port: The port number. "Port *" settings apply to all ports.

Queue 0~7 Enable: Select the appropriate checkboxes to enable queue policing function on switch ports. When enabled, the following image will appear:

QoS Ingress Queue Policers										
Port	E	Rate	Unit	Queue 0 Enable	Queue 1 Enable	Queue 2 Enable	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable
*	☒	500	<>	☐	☐	☐	☐	☐	☐	☐
1	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
2	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
3	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
4	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
5	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
6	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
7	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
8	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
9	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
10	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
11	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
12	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
13	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
14	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
15	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
16	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
17	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
18	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
19	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
20	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
21	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
22	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
23	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
24	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
25	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐
26	☒	500	kbps	☐	☐	☐	☐	☐	☐	☐

Rate: Indicate the rate for the ingress queue policer. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 3300Mbps.

Unit: Select the unit of measure for the ingress queue policer.

Save: Save the current running configurations to memory.

Reset: Clear all selected settings.

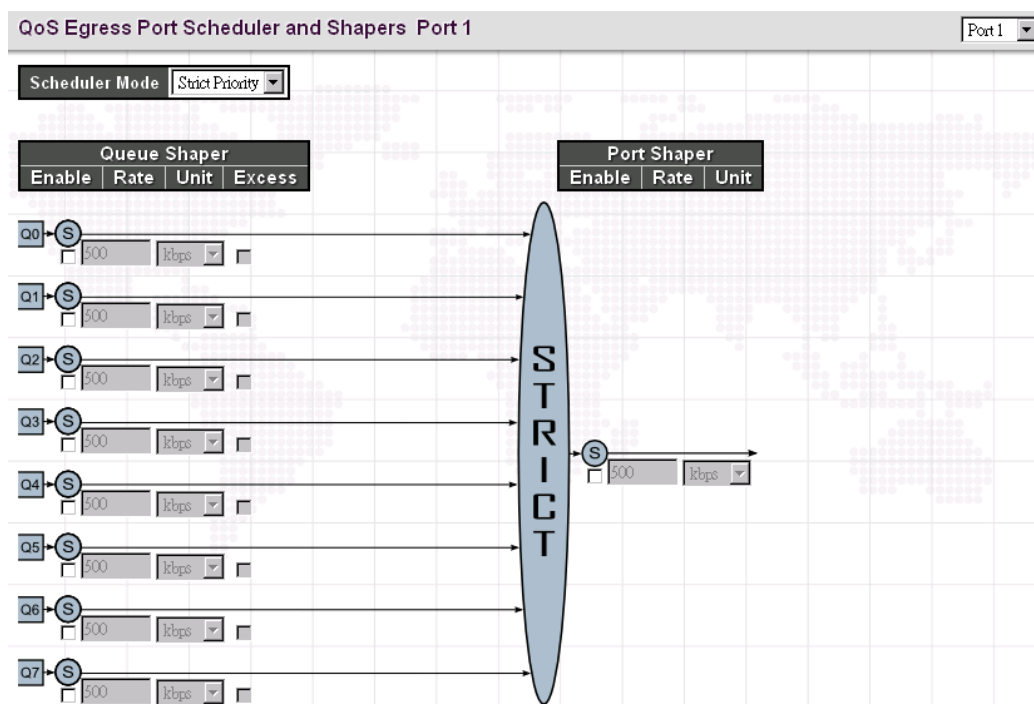
4.3.18.4 Port Scheduler

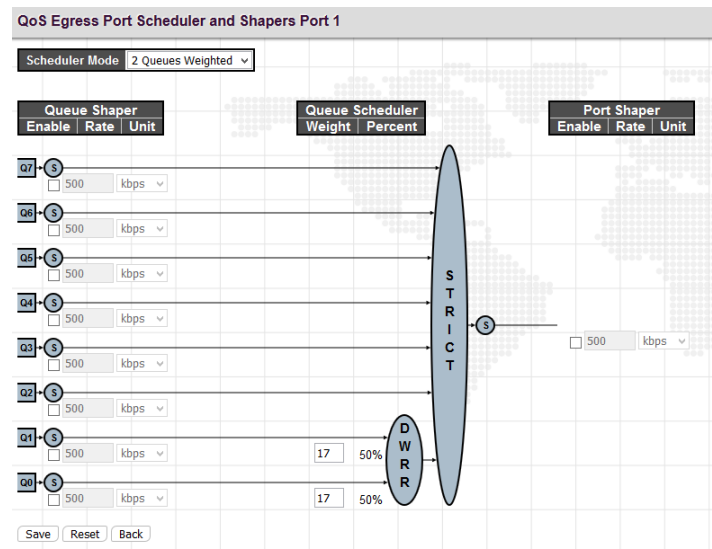
Port	Mode	Weight						
		Q0	Q1	Q2	Q3	Q4	Q5	Q6
1	Strict Priority	-	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-	-
15	Strict Priority	-	-	-	-	-	-	-
16	Strict Priority	-	-	-	-	-	-	-
17	Strict Priority	-	-	-	-	-	-	-
18	Strict Priority	-	-	-	-	-	-	-
19	Strict Priority	-	-	-	-	-	-	-
20	Strict Priority	-	-	-	-	-	-	-
21	Strict Priority	-	-	-	-	-	-	-
22	Strict Priority	-	-	-	-	-	-	-
23	Strict Priority	-	-	-	-	-	-	-
24	Strict Priority	-	-	-	-	-	-	-
25	Strict Priority	-	-	-	-	-	-	-
26	Strict Priority	-	-	-	-	-	-	-
27	Strict Priority	-	-	-	-	-	-	-
28	Strict Priority	-	-	-	-	-	-	-
29	Strict Priority	-	-	-	-	-	-	-
30	Strict Priority	-	-	-	-	-	-	-
31	Strict Priority	-	-	-	-	-	-	-
32	Strict Priority	-	-	-	-	-	-	-
33	Strict Priority	-	-	-	-	-	-	-

Port: Click the port to set up detailed settings for port scheduler.

Mode: Display scheduler mode selected.

Weight: Display the weight in percentage assigned to Q0 – Q5.





This page allows you to set up the Schedulers and Shapers for a specific port.

Scheduler Mode: The device offers two modes to handle queues.

Strict mode: This gives egress queues with higher priority to be transmitted first before lower priority queues are serviced.

(2~8 Queues) Weight mode: Deficit Weighted Round-Robin (DWRR) queuing which specifies a scheduling weight for each queue. (Options: Strict, Weighted; Default: Strict) DWRR services the queues in a manner similar to WRR, but the next queue is serviced only when the queue's Deficit Counter becomes smaller than the packet size to be transmitted.

Queue Shaper/Port Shaper/Queue Shaper

Enable: Select the checkbox to enable queue shaper on a certain queue for this selected port.

Rate: Indicate the rate for the queue shaper. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 13200Mbps.

Unit: Select the unit of measure for the queue shaper.

Excess: Select the checkbox to allow excess bandwidth.

Queue Schedule

Queue Scheduler: When Scheduler Mode is set to Weighted, the user needs to indicate a relative weight for each queue. DWRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Weight: Assign a weight to each queue. This weight sets the frequency at which each queue is polled for service and subsequently affects the response time software applications assigned a specific priority value.

Percent: The weight as a percentage for this queue.

Port Shaper

Enable: Select the checkbox to enable Port shaper.

Rate: Indicate the rate for Port Shaper. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 13200Mbps.

Unit: Select the rate of measure

4.3.18.5 Port Shaping

QoS Egress Port Shapers									
Port	Shapers							Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6		
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-	-
15	-	-	-	-	-	-	-	-	-
16	-	-	-	-	-	-	-	-	-
17	-	-	-	-	-	-	-	-	-
18	-	-	-	-	-	-	-	-	-
19	-	-	-	-	-	-	-	-	-
20	-	-	-	-	-	-	-	-	-
21	-	-	-	-	-	-	-	-	-
22	-	-	-	-	-	-	-	-	-
23	-	-	-	-	-	-	-	-	-
24	-	-	-	-	-	-	-	-	-
25	-	-	-	-	-	-	-	-	-
26	-	-	-	-	-	-	-	-	-
27	-	-	-	-	-	-	-	-	-
28	-	-	-	-	-	-	-	-	-
29	-	-	-	-	-	-	-	-	-
30	-	-	-	-	-	-	-	-	-
31	-	-	-	-	-	-	-	-	-
32	-	-	-	-	-	-	-	-	-
33	-	-	-	-	-	-	-	-	-

This displays each port's queue shaper and port shaper's rate.

Click the port number to modify or reset queue shaper and port shaper's rates. See "Port Scheduler" for detailed explanation on each configuration option.

4.3.18.6 Port Tag Remarking

QoS Egress Port Tag Remarking Port 2

Tag Remarking Mode

Classified

Save

Reset

Cancel

QoS Egress Port Tag Remarking Port 2

Tag Remarking Mode

Default

PCP/DEI Configuration

Default PCP

0

Default DEI

0

Save

Reset

Cancel

QoS Egress Port Tag Remarking Port 2

Tag Remarking Mode Mapped

(QoS class, DP level) to (PCP, DEI) Mapping

QoS class	DP level	PCP	DEI
*	*		
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Tag Remarking Mode: Select the appropriate remarking mode used by this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values (Default PCP:0; Default DEI:0).

Mapped: Use the mapping of the classified QoS class values and DP levels to PCP/DEI values.

QoS class/DP level: Show the mapping options for QoS class values and DP levels (drop precedence).

PCP: Remarks matching egress frames with the specified Priority Code Point (or User Priority) value. (Range: 0-7; Default: 0)

DEI: Remarks matching egress frames with the specified Drop Eligible Indicator. (Range: 0-1; Default: 0)

4.3.18.7 Port DSCP

QoS Port DSCP Configuration			
Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☐	Disable	Disable
3	☐	Disable	Disable
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable
7	☐	Disable	Disable
8	☐	Disable	Disable
9	☐	Disable	Disable
10	☐	Disable	Disable
11	☐	Disable	Disable
12	☐	Disable	Disable
13	☐	Disable	Disable
14	☐	Disable	Disable
15	☐	Disable	Disable
16	☐	Disable	Disable
17	☐	Disable	Disable
18	☐	Disable	Disable
19	☐	Disable	Disable
20	☐	Disable	Disable
21	☐	Disable	Disable
22	☐	Disable	Disable
23	☐	Disable	Disable
24	☐	Disable	Disable
25	☐	Disable	Disable
26	☐	Disable	Disable
27	☐	Disable	Disable
28	☐	Disable	Disable

Port: The port number. "Port *" settings apply to all ports.

Ingress Translate: Select the checkbox to enable ingress translation of DSCP values based on the selected classification method.

Ingress Classify: Select the appropriate classification method:

Disable: No ingress DSCP classification is performed.

DSCP=0: Classify if incoming DSCP is 0.

Selected: Classify only selected DSCP for which classification is enabled in DSCP Translation table

All: Classify all DSCP.

Egress Rewrite: Configure port egress rewriting of DSCP values.

Disable: Egress rewriting is disabled.

Enable: Enable egress rewriting is enabled but with remapping.

Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

4.3.18.8 DSCP-Based QoS Ingress Classification

DSCP-Based QoS Ingress Classification			
DSCP	Trust	QoS Class	DPL
*	☐	< ▾	< ▾
0 (BE)	☐	0 ▾	0 ▾
1	☐	0 ▾	0 ▾
2	☐	0 ▾	0 ▾
3	☐	0 ▾	0 ▾
4	☐	0 ▾	0 ▾
5	☐	0 ▾	0 ▾
6	☐	0 ▾	0 ▾
7	☐	0 ▾	0 ▾
8 (CS1)	☐	0 ▾	0 ▾
9	☐	0 ▾	0 ▾
10 (AF11)	☐	0 ▾	0 ▾
11	☐	0 ▾	0 ▾
12 (AF12)	☐	0 ▾	0 ▾
13	☐	0 ▾	0 ▾
14 (AF13)	☐	0 ▾	0 ▾
15	☐	0 ▾	0 ▾
16 (CS2)	☐	0 ▾	0 ▾
17	☐	0 ▾	0 ▾
18 (AF21)	☐	0 ▾	0 ▾
19	☐	0 ▾	0 ▾
20 (AF22)	☐	0 ▾	0 ▾
21	☐	0 ▾	0 ▾
22 (AF23)	☐	0 ▾	0 ▾
23	☐	0 ▾	0 ▾
24 (CS3)	☐	0 ▾	0 ▾
25	☐	0 ▾	0 ▾
26 (AF31)	☐	0 ▾	0 ▾
27	☐	0 ▾	0 ▾

DSCP: DSCP value in ingress packet. DSCP range is from 0 to 63.

Trust: Select the checkbox to indicate that DSCP value is trusted. Only trusted DSCP values are mapped to a specific QoS class and drop precedence level (DPL). Frames with untrusted DSCP values are treated as non-IP frames.

QoS Class: Select the QoS class to the corresponding DSCP value for ingress processing. By default, 0 is used. Allowed range is 0 to 7.

DPL: Select the drop precedence level to the corresponding DSCP value for ingress processing. By default, 0 is used. The value "1" has the higher drop priority.

4.3.18.9 DSCP Translation

DSCP Translation			
DSCP	Ingress		Egress
	Translate	Classify	Remap
*	<>	☐	<>
0 (BE)	0 (BE)	☐	0 (BE)
1	1	☐	1
2	2	☐	2
3	3	☐	3
4	4	☐	4
5	5	☐	5
6	6	☐	6
7	7	☐	7
8 (CS1)	8 (CS1)	☐	8 (CS1)
9	9	☐	9
10 (AF11)	10 (AF11)	☐	10 (AF11)
11	11	☐	11
12 (AF12)	12 (AF12)	☐	12 (AF12)
13	13	☐	13
14 (AF13)	14 (AF13)	☐	14 (AF13)
15	15	☐	15
16 (CS2)	16 (CS2)	☐	16 (CS2)
17	17	☐	17
18 (AF21)	18 (AF21)	☐	18 (AF21)
19	19	☐	19
20 (AF22)	20 (AF22)	☐	20 (AF22)
21	21	☐	21
22 (AF23)	22 (AF23)	☐	22 (AF23)

DSCP: DSCP value in ingress packet. DSCP range is from 0 to 63.

Ingress Translate: Enable Ingress Translation of DSCP values based on the specified classification method.

Ingress Classify: Enable classification at ingress side as defined in the QoS port DSCP Configuration Table.

Egress Remap: Enable egress remap based on the specified classification method.

4.3.18.10 DSCP Classification

DSCP Classification				
QoS Class	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<>	<>	<>	<>
0	0 (BE)	0 (BE)	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)	0 (BE)	0 (BE)

Map DSCP values to QoS class and DPL value.

QoS Class: List of actual QoS class values.

DSCP: Select the DSCP value to map QoS class and DPL value. DSCP value selected for “*” will map to all QoS class and DPL value.

4.3.18.11 QoS Control List

Quality of Service control list is used to establish policies for handling ingress packets based on frame type, MAC address, VID, PCP, DEI values. Once a QCE is mapped to a port, traffic matching the first entry in the QoS Control List is assigned to the QoS class, drop precedence level, and DSCP value defined by that entry. Traffic not matching any of the QCEs are classified to the default QoS Class for the port.

QoS Control List Configuration														
QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action					
									CoS	DPL	DSCP	PCP	DEI	Policy

This page displays rules created in QoS control list (QCL) only. The maximum number of QCL is 256 on this device. Click the plus sign  to insert a new QCL to the list.

QCE#: Display Quality Control Entry index.

Port: Display the port number that uses this QCL.

DMAC: Destination MAC address. Possible values are Any, Broadcast, Multicast, Unicast.

SMAC: Source MAC address.

Tag Type: The value of tag field can be "Untagged", "Tagged" or "Any".

VID: Display VLAN ID (1-4095)

PCP: Display PCP value.

DEI: Display DEI value.

Frame Type: Display the frame type to look for in incoming frames. Possible frame types are Any, Ethernet, LLC SNAP, IPv4, IPv6.

Action: Display the classification action taken on ingress frames when the configured parameters are matched in the frame's content. If a frame matches the QCL, the following actions will be taken.

CoS: If a frame matches the QCL, it will be put in the queue corresponding to the specified QoS class.

DPL: The drop precedence level will be set to the specified value.

DSCP: The DSCP value will be set to the specified value.

PCP: The PCP value will be set to the specified value.

DEI: The DEI value will be set to the sepecified value.

Policy: The policy will be set to the specified one.

You can modify each QCE (QoS Control Entry) in the table using the following buttons:

: Insert a new QCE before the current row.

: Edit the QCE entry.

: Move the QCE up the list.

: Move the QCE down the list.

: Delete the QCE.

: The lowest plus sign add a new entry at the bottom of the QCE listings.

Once  is clicked in display page, the following page will appear.

QCE Configuration

Port Members: Select ports that use this rule.

Key Parameters

SMAC: Select source MAC address type. By default, any is used. Select “Specific” to specify a source MAC (first three bytes of the MAC address or OUI).

DMAC Type: Select destination MAC address type. By default, any is used. Other options available are “UC” for unicast, “MC” for multicast, and “BC” for broadcast.

Tag: Select VLAN tag type (Tag or Untag). By default, any type is used.

VID: Select VID preference. By default, any VID is used. Select “Specific”, if you would like to designate a VID to this QCL entry. Or Select “Range”, if you would like to map a range of VIDs to this QCL entry.

PCP: Select a PCP value (either specific value or a range of values are provided). By default, any is used.

DEI: Select a DEI value. By default, any is used.

Inner Tag: Select a Inner Tag value. By default, any is used.

Inner VID: Select a Inner VID (VLAN ID) value. By default, any is used.

Inner PCP: Select a Inner PCP (802.1p priority level) value. By default, any is used.

Inner DEI: Select a Inner DEI (Drop Eligible Indicator) value. By default, any is used.

Frame Type: The frame types can be selected are listed below.

Any: By default, any is used which means that all types of frames are allowed.

Ethernet: This option can only be used to filter Ethernet II formatted packets (Options: Any, Specific – 600-ffff hex; Default: ffff). Note that 800 (IPv4) and 86DD (IPv6) are excluded. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

LLC: LLC refers to Link Logical Control and further provides three options.

SSAP: SSAP stands for Source Service Access Point address. By default, any is used. Select specific to indicate a value (0x00 - 0xFF).

DSAP: DSAP stands for Destination Service Access Point address. By default, any is used. Select specific to indicate a value (0x00 to 0xFF).

Control: Control field may contain command, response, or sequence information depending on whether the LLC frame type is Unnumbered, Supervisory, or Information. By default, any is used. Select specific to indicate a value (0x00 to 0xFF).

SNAP: SubNetwork Access Protocol can be distinguished by an OUI and a Protocol ID. (Options for PID: Any, Specific (0x00-0xffff); Default: Any) If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

IPv4:

Protocol: IPv4 frame type includes Any, TCP, UDP, Other. If “TCP” or “UDP” is selected, you might further define Sport (Source port number) and Dport (Destination port number).

Source IP: Select source IP type. By default, any is used. Select “Specific” to indicate self-defined source IP and submask format. The address and mask must be in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero

IP Fragment: By default, any is used. Datagrams sometimes may be fragmented to ensure they can pass through a network device that uses a maximum transfer unit smaller than the original packet’s size.

DSCP: By default, any is used. Select “Specific” to indicate a DSCP value. Select “Range” to indicate a range of DSCP value.

IPv6:

Protocol: IPv6 protocol includes Any, TCP, UDP, Other. If “TCP” or “UDP” is selected, you may need to further define Sport (Source port number) and Dport (Destination port number).

SIP (32 LSB): Select source IP type. By default, any is used. Select “Specific” to indicate self-defined source IP and submask format.

DSCP: By default, any is used. Select “Specific” to indicate a DSCP value. Select “Range” to indicate a range of DSCP value.

Action Parameters

Specify the classification action taken on ingress frame if the parameters match the frame’s content. The actions taken include the following:

CoS: If a frame matches the QCE, it will be put in the queue corresponding to the specified CoS class.

DPL: If a frame matches the QCE, the drop precedence level will be set to the selected value or left unchanged.

DSCP: If a frame matches the QCE, the DSCP value will be set to the selected one.

4.3.18.12 Storm Policing

Storm Control is used to keep a network from downgraded performance or a complete halt by setting up a threshold for traffic like broadcast, unicast and multicast. When a device on the network is malfunctioning or application programs are not well designed or properly configured, storms may occur and will degrade network performance or even cause a complete halt. The network can be protected from storms by setting a threshold for specified traffic on the device. Any specified packets exceeding the specified threshold will then be dropped.

Global Storm Policer Configuration			
Frame Type	Enable	Rate	Unit
Unicast	☐	10	fps
Multicast	☐	10	fps
Broadcast	☐	10	fps

Enable: Enable Unicast storm, Multicast storm or Broadcast storm protection.

Rate (pps): Select the packet threshold. The packets received exceed the selected value will be dropped.

Unit: Select the unit for each frame type.

Port Storm Policer Configuration											
Port	Unicast Frames			Broadcast Frames			Unknown Frames				
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit		
1	☐	500	kbps	☐	500	kbps	☐	500	kbps		
2	☐	500	kbps	☐	500	kbps	☐	500	kbps		
3	☐	500	kbps	☐	500	kbps	☐	500	kbps		
4	☐	500	kbps	☐	500	kbps	☐	500	kbps		
5	☐	500	kbps	☐	500	kbps	☐	500	kbps		
6	☐	500	kbps	☐	500	kbps	☐	500	kbps		
7	☐	500	kbps	☐	500	kbps	☐	500	kbps		
8	☐	500	kbps	☐	500	kbps	☐	500	kbps		
9	☐	500	kbps	☐	500	kbps	☐	500	kbps		
10	☐	500	kbps	☐	500	kbps	☐	500	kbps		
11	☐	500	kbps	☐	500	kbps	☐	500	kbps		
12	☐	500	kbps	☐	500	kbps	☐	500	kbps		
13	☐	500	kbps	☐	500	kbps	☐	500	kbps		
14	☐	500	kbps	☐	500	kbps	☐	500	kbps		
15	☐	500	kbps	☐	500	kbps	☐	500	kbps		
16	☐	500	kbps	☐	500	kbps	☐	500	kbps		
17	☐	500	kbps	☐	500	kbps	☐	500	kbps		
18	☐	500	kbps	☐	500	kbps	☐	500	kbps		
19	☐	500	kbps	☐	500	kbps	☐	500	kbps		
20	☐	500	kbps	☐	500	kbps	☐	500	kbps		
21	☐	500	kbps	☐	500	kbps	☐	500	kbps		

Enable: Enable Unicast storm, Multicast storm or Broadcast storm protection.

Rate (pps): Select the packet threshold. The packets received exceed the selected value will be dropped.

4.3.18.13 WRED

Weighted Random Early Detection Configuration						
Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	☐	0	50	Drop Probability ▼
1	0	2	☐	0	50	Drop Probability ▼
1	0	3	☐	0	50	Drop Probability ▼
1	1	1	☐	0	50	Drop Probability ▼
1	1	2	☐	0	50	Drop Probability ▼
1	1	3	☐	0	50	Drop Probability ▼
1	2	1	☐	0	50	Drop Probability ▼
1	2	2	☐	0	50	Drop Probability ▼
1	2	3	☐	0	50	Drop Probability ▼
1	3	1	☐	0	50	Drop Probability ▼
1	3	2	☐	0	50	Drop Probability ▼
1	3	3	☐	0	50	Drop Probability ▼
1	4	1	☐	0	50	Drop Probability ▼
1	4	2	☐	0	50	Drop Probability ▼
1	4	3	☐	0	50	Drop Probability ▼
1	5	1	☐	0	50	Drop Probability ▼
1	5	2	☐	0	50	Drop Probability ▼
1	5	3	☐	0	50	Drop Probability ▼
1	6	1	☐	0	50	Drop Probability ▼
1	6	2	☐	0	50	Drop Probability ▼
1	6	3	☐	0	50	Drop Probability ▼
1	7	1	☐	0	50	Drop Probability ▼
1	7	2	☐	0	50	Drop Probability ▼
1	7	3	☐	0	50	Drop Probability ▼
2	0	1	☐	0	50	Drop Probability ▼
2	0	2	☐	0	50	Drop Probability ▼
2	0	3	☐	0	50	Drop Probability ▼
2	1	1	☐	0	50	Drop Probability ▼
2	1	2	☐	0	50	Drop Probability ▼
2	1	3	☐	0	50	Drop Probability ▼

Enable: Select the checkbox to enable RED on a particular queue.

Min. threshold: Specify the lowest RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This valid value for this field is 0~100.

Max. DP 1: Controls the drop probability for the frames marked in drop precedence level 1 when the average queue filling level is 100%. The valid value is 0~100.

Max. DP 2: Controls the drop probability for the frames marked in drop precedence level 2 when the average queue filling level is 100%. The valid value is 0~100.

Max. DP 3: Controls the drop probability for the frames marked in drop precedence level 3 when the average queue filling level is 100%. The valid value is 0~100.

4.3.19 Mirroring

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extend function of Mirroring. It can extend the destination port in other switch. So the administrator can analyze the network traffic on the other switches.

If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you have to set VLAN egress tagging as "Untag ALL" on the reflector port.

Mirroring & Remote Mirroring Configuration

Mode: Disabled
 Type: Mirror
 VLAN ID: 200
 Reflector Port: Port 25

Source VLAN(s) Configuration

Source VLANs:

Port Configuration

Port	Source	Intermediate	Destination
1	Disabled	☐	☐
2	Disabled	☐	☐
3	Disabled	☐	☐
4	Disabled	☐	☐
5	Disabled	☐	☐
6	Disabled	☐	☐
7	Disabled	☐	☐
8	Disabled	☐	☐
9	Disabled	☐	☐
10	Disabled	☐	☐
11	Disabled	☐	☐
12	Disabled	☐	☐
13	Disabled	☐	☐
14	Disabled	☐	☐
15	Disabled	☐	☐
16	Disabled	☐	☐
17	Disabled	☐	☐
18	Disabled	☐	☐
19	Disabled	☐	☐
20	Disabled	☐	☐

Mode: Enable or disable the mirror or Remote Mirroring function.

Type: Select switch type.

Mirror: The switch is running on mirror mode. The source port(s) and destination port are located on this switch.

RMirror source: The switch is a source node for monitor flow. The source port(s), reflector port are located on this switch.

RMirror destination: The switch is an end node for monitor flow. The destination port(s) is located on this switch.

VLAN ID: The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.

Reflector Port: The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled.

If you shut down a port, it cannot be a candidate for reflector port.

If you shut down the port which is a reflector port, the remote mirror function cannot work.

Note1: The reflector port needs to select only on Source switch type.

Note2: The reflector port needs to disable MAC Table learning and STP.

Note3: The reflector port only supports on pure copper ports.

Source VLAN(s) Configuration

Source VLANs: The device supports VLAN-based mirroring. If you want to monitor some VLANs on the switch, you can input VLAN IDs in this field.

Port Configuration

Port: The logical port for the settings contained in the same row.

Source: Select mirror mode.

Disabled: Neither frames transmitted nor frames received are mirrored.

Both: Frames received and frames transmitted are mirrored on the Destination port.

Rx only: Frames received on this port are mirrored on the Destination port. Frames transmitted are not mirrored.

Tx only: Frames transmitted on this port are mirrored on the Destination port. Frames received are not mirrored.

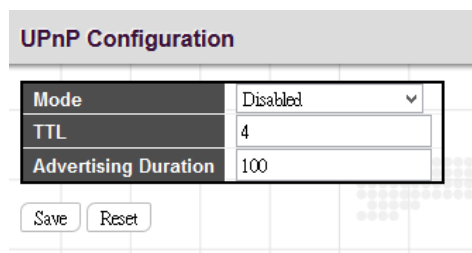
Intermediate: Select the checkbox if it is the intermediate port. The intermediate port is a switched port to connect to the other switch. Note: The intermediate port needs to disable MAC Table learning.

Destination: Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port.

Note1: On mirror mode, the device only supports one destination port.

Note2: The destination port needs to disable MAC Table learning.

4.3.20 UPnP



UPnP Configuration	
Mode	Disabled ▼
TTL	4
Advertising Duration	100
Save Reset	

Mode: Enable or disable UPnP operation.

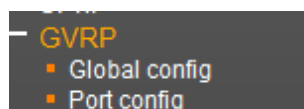
TTL: TTL (Time to live) is used to configure how many steps an UPnP advertisement can travel before it disappears.

Advertising Duration: This defines how often an UPnP advertisement is sent. The duration is carried in Simple Service Discover Protocol (SSDP) packets which informs a control point how often it should receive a SSDP advertisement message from the switch. By default, the advertising duration is set to 100 seconds. However, due to the unreliable nature of UDP, it is recommended to set to the shorter duration since the shorter the duration, the fresher is UPnP status.

4.3.21 GVRP

GVRP (GVRP VLAN Registration Protocol) is defined in the IEEE 802.1Q standard and enables the switch to dynamically create IEEE 802.1Q compliant VLANs between GVRP-enabled devices. With GVRP, VLAN information can be automatically propagated from device to device so as to reduce errors when creating VLANs manually and provide VLANs consistency across network.

This section provides configuration pages for users to set up GVRP timers and enable GVRP on a per-port basis.



4.3.21.1 Global Config

GVRP Configuration

☐ Enable GVRP

Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

Enable GVRP: Select the checkbox to globally enable GVRP function.

Join-time: Specify the amount of time in units of centi-seconds that PDUs are transmitted. The default value is 20 centi-seconds. The valid value is 1~20.

Note: The "Leave-time" parameter must be three times greater than or equal to Join time.

Leave-time: Specify the amount of time in units of centi-seconds that the device waits before deleting the associated entry. The leave time is activated by a "Leave All-time" message sent/received and cancelled by the Join message. The default value is 60 centi-seconds.

LeaveAll-time: Specify the amount of time that "LeaveAll" PDUs are created. A LeaveAll PDU indicates that all registrations are shortly de-registered. Participants will need to rejoin in order to maintain registration. The valid value is 1000 to 5000 centi-seconds. The factory default 1000 centi-seconds.

NOTE: The "LeaveAll-time" parameter must be greater than the "Leave-time" parameter.

Max VLANs: The maximum number of VLANs can be learned via GVRP.

4.3.21.2 Port Config

GVRP Port Configuration		
Port	Mode	
*	 ▼	
1	Disabled ▼	
2	Disabled ▼	
3	Disabled ▼	
4	Disabled ▼	
5	Disabled ▼	
6	Disabled ▼	
7	Disabled ▼	
8	Disabled ▼	
9	Disabled ▼	
10	Disabled ▼	
11	Disabled ▼	
12	Disabled ▼	
13	Disabled ▼	
14	Disabled ▼	
15	Disabled ▼	
16	Disabled ▼	
17	Disabled ▼	
18	Disabled ▼	
19	Disabled ▼	
20	Disabled ▼	
21	Disabled ▼	
22	Disabled ▼	
23	Disabled ▼	
24	Disabled ▼	

Port: The port number.

Mode: Enable GVRP on a per port basis.

4.3.22 sFlow

4.3.22.1 Configuration

sFlow Configuration

Agent Configuration

IP Address:

Receiver Configuration

Owner	<none>	Release
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	seconds
Max. Datagram Size	1400	bytes

Port Configuration

Port	Flow Sampler		Counter Poller	
	Enabled	Sampling Rate	Enabled	Interval
*	☐	0	☐	0
1	☐	0	☐	0
2	☐	0	☐	0
3	☐	0	☐	0
4	☐	0	☐	0
5	☐	0	☐	0
6	☐	0	☐	0
7	☐	0	☐	0
8	☐	0	☐	0
9	☐	0	☐	0
10	☐	0	☐	0
11	☐	0	☐	0
12	☐	0	☐	0
13	☐	0	☐	0
14	☐	0	☐	0
15	☐	0	☐	0
16	☐	0	☐	0
17	☐	0	☐	0

Agent Configuration

IP Address: Specify an valid IPv4 or IPv6 address for sFlow agent.

Receiver Configuration

Owner: Basically, sFlow can be configured in two ways. One is through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

The button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

IP Address Hostname: Specify the IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port: The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

Timeout: The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.

Max. Datagram Size: The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

Port: The port number for which the configuration below applies.

Flow Sampler Enabled: Enables flow sampling on this port. Uncheck the box will disable flow sampling on the this specific port.

Flow Sampler Sampling Rate: The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 to 4294967295.

Flow Sampler Max. Header: The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

Counter Poller Enabled: Enable counter polling on this port. Uncheck the box to disable Counter Poller function on this port.

Counter Poller Interval: With counter polling enabled, this specifies the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.

Save Button: Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.

4.3.23 UDLD

UDLD Port Configuration		
Port	UDLD mode	Message Interval
1	Disable	7
2	Disable	7
3	Disable	7
4	Disable	7
5	Disable	7
6	Disable	7
7	Disable	7
8	Disable	7
9	Disable	7
10	Disable	7
11	Disable	7
12	Disable	7
13	Disable	7
14	Disable	7
15	Disable	7
16	Disable	7
17	Disable	7
18	Disable	7
19	Disable	7
20	Disable	7
21	Disable	7
22	Disable	7
23	Disable	7
24	Disable	7
25	Disable	7
26	Disable	7
27	Disable	7
28	Disable	7
29	Disable	7

UDLD Mode: Configures the UDLD mode on a port. Valid values are Disable, Normal and Aggressive. Default mode is Disable.

Disable: In disabled mode, UDLD functionality doesn't exists on port.

Normal: In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state.

Aggressive: In aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, need to disable UDLD on that port.

Message Interval: Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds(Default value is 7 seconds)(Currently default time interval is supported, due to lack of detailed information in RFC 5171).

Detailed UDLD Status for Port 1
Port 1 ☐ Auto-refresh

UDLD status	
UDLD Admin state	Disable
Device ID(local)	00-02-AB-06-20-20
Device Name(local)	-
Bidirectional State	Indeterminant

Neighbour Status

Port	Device Id	Link Status	Device Name
No Neighbour ports enabled or no existing partners			

UDLD Status

UDLD Admin State: The current port state of the logical port, Enabled if any of state(Normal,Aggressive) is Enabled.

Device ID (local): The ID of Device.

Device Name (local): Name of the Device.

Bidirectional State: The current state of the port.

Neighbour Status

Port: The current port of neighbour device.

Device ID: The current ID of neighbour device.

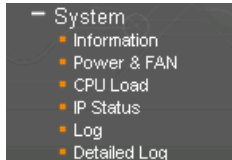
Link Status: The current link status of neighbour port.

Device Name: Name of the Neighbour Device.

4.4 Monitor

This part provides monitoring statistics or data on configured functions. The user can use sub-sections of this part to view System information, configured IP address, MAC addresses learned, etc.

4.4.1 System



4.4.1.1 System Information

The system information screen will display the configuration information, the hardware MAC address and version, the system time, the system "uptime" and the software version and build date.

System Information	
System	
Contact	techsupport@ctcu.com
Name	GSW3424FM-218
Location	Demo Room 9F
Hardware	
MAC Address	00-01-c1-00-00-00
Hardware Version	V1.100
Time	
System Date	2020-05-29T11:02:10+08:00
System Uptime	0d 18:06:59
Software	
Software Version	"V1.007"
Software Date	2019-07-12T11:53:10+08:00

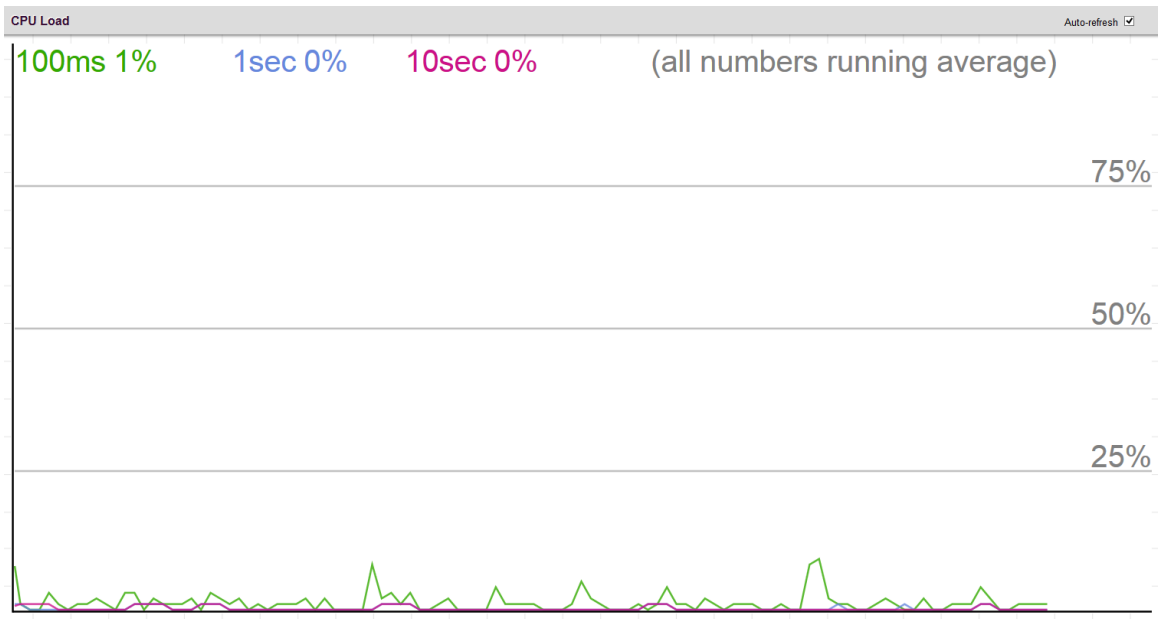
4.4.1.2 Power & Fan

This screen page displays the current state of the built-in power and fan. If there is something wrong with fan modules, error messages will be displayed here. (If there is something wrong with fan modules, FAN LED indicators on the front panel will also be lit in red.)

Power and FAN	
Power	
Power 1	AC
Power 2	DC48V
FAN	
Fan 1	10624 rpm
Fan 2	10368 rpm
Fan 3	10563 rpm
Temperature	
Temp 0	28°C
Temp 1	33°C
Temp 2	20°C
Temp 3	20°C
Refresh	

4.4.1.3 System CPU Load

This page displays the CPU load, using an SVG graph.



The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Automatic refresh occurs every 3 seconds.

4.4.1.4 System IP Status

Display the status of IP interfaces and routes.

IP Interfaces

Auto-refresh ☐ Refresh

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80:1::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-02-ab-d6-68-b0	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.250/24	
VLAN1	IPv6	fe80:2::202:abff:fed6:68b0/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	OS:lo:127.0.0.1	<UP HOST>
192.168.0.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	OS:lo:127.0.0.1	<UP>
::1/128	OS:lo:::1	<UP HOST>
fe80:1::/128	OS:lo:fe80:1::1	<UP>
fe80:1::1/128	OS:lo	<UP HOST>
fe80:2::/128	VLAN1	<UP>
fe80:2::202:abff:fed6:68b0/128	OS:lo:2:abd6:68b0::	<UP HOST>
ff01:1::/128	OS:lo:::1	<UP>
ff01:2::/128	VLAN1	<UP>
ff02:1::/128	OS:lo:::1	<UP>
ff02:2::/128	VLAN1	<UP>

Neighbour cache

IP Address	Link Address
192.168.0.145	VLAN1:74-d0-2b-8f-ad-24
fe80:2::202:abff:fed6:68b0	VLAN1:00-02-ab-d6-68-b0

Please refer to “System IP” for the configuration of the interfaces and routes. This page is informational only.

4.4.1.5 System Log Information

Displays the collected log information.

System Log Information Auto-refresh ☐ Refresh Clear << << >> >>

Level: All Clear Level: All

The total number of entries is 2 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Info	2012-12-31T23:59:59+00:00	Switch just made a cool boot.
2	Info	2013-01-01T00:00:01+00:00	Link up on port 5

Level: Use this pull down to display all messages or messages of type info, warning or error.

Clear Level: Use this pull down to clear selected message types from the log.

Browsing buttons: Use these buttons to quickly go to the beginning or end of the log or to page through the log.

4.4.1.6 System Detailed Log

Displays individual log records.

Detailed System Log Information Refresh << << >> >>

ID: 1

Message

Level	Info
Time	2012-12-31T23:59:59+00:00
Message	Switch just made a cool boot.

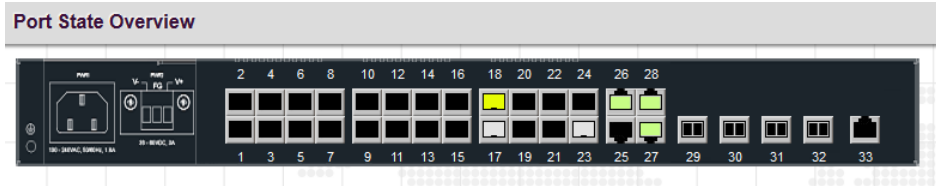
View each log, by ID number.

4.4.2 Ports

- Ports
 - State
 - SFP
 - Traffic Overview
 - QoS Statistics
 - QCL Status
 - Detailed Statistics

4.4.2.1 State

Display an overview graphic of the switch.



This is the same graphic overview shown when first logging into the switch for management. The link status display can be updated by clicking the "Refresh" button. When "Auto-refresh" is checked, the display will be updated every 3 seconds.

4.4.2.2 SFP

SFP monitoring page displays the selected port's slide-in SFP transceiver information. If your SFP transceivers support DDMI, SFP information about optical input power, optical output power, sensitivity and temperature in real time will also be displayed.

SFP and D/D Information	
Port 14	
Vendor Name	CTC UNION
Vendor Part Number	SFS-7020-WA-DDI V1.
Fiber Type	Single
Wave Length	1310 nm
Wave Length 2	1550 nm
Link Length	20 km
TX Power	-6 dBm
RX Power	-37 dBm
RX Sensitivity	-23 dBm
Temperature	12°C

4.4.2.3 Traffic Overview

Port Statistics Overview										
Port	Description	Packets		Bytes		Errors		Drops		Filtered
		Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	
1		0	0	0	0	0	0	0	0	0
2		0	0	0	0	0	0	0	0	0
3		0	0	0	0	0	0	0	0	0
4		0	0	0	0	0	0	0	0	0
5		0	0	0	0	0	0	0	0	0
6		0	0	0	0	0	0	0	0	0
7		0	0	0	0	0	0	0	0	0
8		0	0	0	0	0	0	0	0	0
9		0	0	0	0	0	0	0	0	0
10		0	0	0	0	0	0	0	0	0
11		0	0	0	0	0	0	0	0	0
12		0	0	0	0	0	0	0	0	0
13		0	0	0	0	0	0	0	0	0
14		0	0	0	0	0	0	0	0	0
15		0	0	0	0	0	0	0	0	0
16		0	0	0	0	0	0	0	0	0
17		0	0	0	0	0	0	0	0	0
18		12759	416109	983270	26942813	0	0	0	0	1
19		0	0	0	0	0	0	0	0	0
20		0	0	0	0	0	0	0	0	0
21		0	0	0	0	0	0	0	0	0
22		0	0	0	0	0	0	0	0	0
23		0	0	0	0	0	0	0	0	0
24		0	0	0	0	0	0	0	0	0
25		0	0	0	0	0	0	0	0	0
26		4759063	5136058	1614174467	489289040	0	0	0	0	12
27		15536741	15228869	1491779407	4704001168	0	0	0	0	323
28		5765575	6168930	1302094836	568857166	0	0	0	0	1
29		0	0	0	0	0	0	0	0	0
30		0	0	0	0	0	0	0	0	0
31		0	0	0	0	0	0	0	0	0
32		0	0	0	0	0	0	0	0	0
33		0	0	0	0	0	0	0	0	0

Packets Received & Transmitted: The number of received and transmitted packets per port.

Bytes Received & Transmitted: The number of received and transmitted bytes per port.

Errors Received & Transmitted: The number of frames received in error and the number of incomplete transmissions per port.

Drops Received & Transmitted: The number of frames discarded due to ingress or egress congestion.

Filtered Received: The number of received frames filtered by the forwarding process.

The counter display can be updated by clicking the "Refresh" button. When "Auto-refresh" is checked, the display will be updated every 3 seconds. Clicking the "Clear" button will zero all counters and start counting again.

4.4.2.4 QoS Statistics

Queuing Counters																
Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	12808	415475	0	0	0	0	0	0	0	0	0	0	0	0	0	2236
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	4776879	5153073	0	0	0	0	0	0	0	0	0	0	0	0	0	2243
27	15595282	10577049	0	0	0	0	0	0	0	0	0	0	0	0	0	4709187
28	5787381	6190038	0	0	0	0	0	0	0	0	0	0	0	0	0	2242
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

The displayed counters are:

Port: The logical port for the settings contained in the same row.

Qn: There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx: The number of received and transmitted packets per queue.

4.4.2.5 QCL Status

This page shows the QCL status by different QCL users.

QoS Control List Status									
User	QCE	Port	Frame Type	CoS	DPL	DSCP	PCP	DEI	Policy
No entries									

Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

User: Indicates the QCL user.

QCE#: Indicates the index of QCE.

Port: Indicates the list of ports configured with the QCE.

Frame Type: Indicates the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed.

SNAP: Only (SNAP) frames are allowed.

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

Action: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP.

CoS: Classified QoS class; if a frame matches the QCE it will be put in the queue.

DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.

DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

Conflict: Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications, it may happen that resources required to add a QCE may not be available. In that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

4.4.2.6 Ports Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit. Use the port select pull down to select which switch port details to display.

Detailed Port Statistics Port 1			
Port 1		Auto-refresh ☐	Refresh Clear
Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Receive Total and Transmit Total

Rx and Tx Packets: The number of received and transmitted (good and bad) packets.

Rx and Tx Octets: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast: The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast: The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast: The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause: A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE.

Receive and Transmit Size Counters

Rx 64~1527 Bytes & Tx 64~1527 Bytes: Displays the number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

Rx Q0~Q7 & Tx Q0~Q7: Displays the number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops: The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment: The number of frames received with CRC or alignment errors.

Rx Undersize: The number of short¹ frames received with valid CRC.

Rx Oversize: The number of long² frames received with valid CRC.

Rx Fragments: The number of short¹ frames received with invalid CRC.

Rx Jabber: The number of long² frames received with invalid CRC.

Rx Filtered: The number of received frames filtered by the forwarding process.

¹ Short frames are frames that are smaller than 64 bytes.

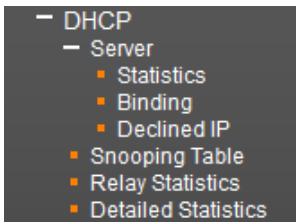
² Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Tx Drops: The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.: The number of frames dropped due to excessive or late collisions.

4.4.3 DHCP



4.4.3.1 Server

4.4.3.1.1 Statistics

DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Declined IP Address
0	0	0

Binding Counters

Automatic Binding	Manual Binding	Expired Binding
0	0	0

DHCP Message Received Counters

DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
0	0	0	0	0

DHCP Message Sent Counters

OFFER	ACK	NAK
0	0	0

Database Counters

Pool: The number of pool that has been configured.

Excluded IP Address: The number of excluded IP address.

Declined IP Address: The number of declined IP address.

Binding Counters

Automatic Binding: The number of bindings with network-type pools.

Manual Binding: The number of bindings that the network engineer assigns an IP address to a client. In other words, the pool is of host type.

Expired Binding: The number of bindings that their lease time expired or they are cleared from Automatic or Manual type bindings.

DHCP Message Received Counters

Discover: The number of DHCP DISCOVER messages received.

Request: The number of DHCP REQUEST messages received.

Decline: The number of DHCP DECLINE messages received.

Release: The number of DHCP RELEASE messages received.

Inform: The number of DHCP INFORM messages received.

DHCP Message Sent Counters

OFFER: The number of DHCP OFFER messages sent.

ACK: The number of DHCP ACK messages sent.

NAK: The number of DHCP NAK messages sent.

4.4.3.1.2 Binding

DHCP Server Binding IP						
Auto-refresh ☐ Refresh Clear Selected Clear Automatic Clear Manual Clear Expired						
Binding IP Address						
Delete	IP	Type	State	Pool Name	Server ID	

IP: The IP address allocated to DHCP client.

Type: The type of binding method. This field can be “Automatic”, “Manual” or “Expired”.

State: The state of binding. Possible states are “Committed”, “Allocated”, or “Expired”.

Pool Name: The pool that generates the binding.

Server ID: The server IP address to create the binding.

4.4.3.1.3 Declined IP

DHCP Server Declined IP	
Declined IP Address	
Declined IP	

Declined IP: Displays a list of declined IP addresses.

4.4.3.2 Snooping Table

Dynamic DHCP Snooping Table

Start from MAC address 00-00-00-00-00-00, VLAN 0 with 20 entries per page.

MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
No more entries					

4.4.3.2.1 Relay Statistics

DHCP Relay Statistics							
Auto-refresh ☐ Refresh Clear							
Server Statistics							
Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0
Client Statistics							
Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option	
0	0	0	0	0	0	0	

DHCP Relay Statistics

Transmit to Server: The number of packets that are relayed from client to server.

Transmit Error: The number of packets that resulted in errors while being sent to clients.

Receive from Client: The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID: The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID: The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID: The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client: The number of relayed packets from server to client.

Transmit Error: The number of packets that resulted in error while being sent to servers.

Receive from Client: The number of received packets from server.

Receive Agent Option: The number of received packets with relay agent information option.

Replace Agent Option: The number of packets which were replaced with relay agent information option.

Keep Agent Option: The number of packets whose relay agent information was retained.

Drop Agent Option: The number of packets that were dropped which were received with relay agent information.

4.4.3.2.2 Detailed Statistics

DHCP Detailed Statistics Port 1			
Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Rx and Tx Discover: The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer: The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request: The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

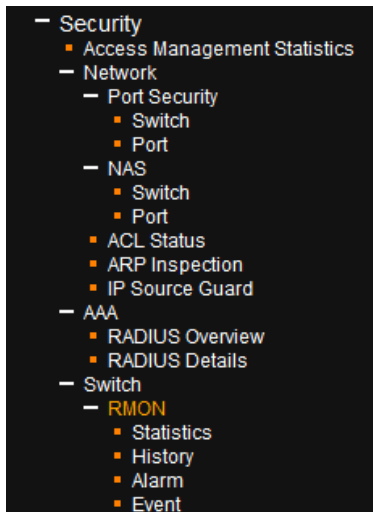
Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Rx and Tx Discarded from Untrusted: The number of discarded packet that are coming from untrusted port.

4.4.4 Security



4.4.4.1 Access Management Statistics

This page provides statistics for access management.

Access Management Statistics				Auto-refresh ☐	Refresh	Clear
Interface	Received Packets	Allowed Packets	Discarded Packets			
HTTP	0	0	0			
HTTPS	0	0	0			
SNMP	0	0	0			
TELNET	0	0	0			
SSH	0	0	0			

Interface: The interface type through which any remote host can access the switch.

Received Packets: The number of received packets from the interface when access management mode is enabled.

Allowed Packets: The number of allowed packets from the interface when access management mode is enabled.

Discarded Packets: The number of discarded packets from the interface when access management mode is enabled.

4.4.4.2 Network

4.4.4.2.1 Port Security

4.4.4.2.1.1 Switch

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-
9	---	Disabled	-	-
10	---	Disabled	-	-
11	---	Disabled	-	-
12	---	Disabled	-	-
13	---	Disabled	-	-
14	---	Disabled	-	-
15	---	Disabled	-	-
16	---	Disabled	-	-
17	---	Disabled	-	-
18	---	Disabled	-	-
19	---	Disabled	-	-
20	---	Disabled	-	-
21	---	Disabled	-	-
22	---	Disabled	-	-
23	---	Disabled	-	-
24	---	Disabled	-	-
25	---	Disabled	-	-
26	---	Disabled	-	-
27	---	Disabled	-	-
28	---	Disabled	-	-
29	---	Disabled	-	-
30	---	Disabled	-	-
31	---	Disabled	-	-
32	---	Disabled	-	-
33	---	Disabled	-	-

User Module Legend

User Module Name: The full name of a module that may request Port Security services.

Abbr: This column is the abbreviation for the user module used in the “Users” column in the “Port Status”.

Port Status

Port: Port number. Click a particular port number to see its port status.

Users: Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter has enabled port security.

State: This shows the current status of a port. It can be one of the following states:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

Shutdown: The Port Security service is enabled by at least the Limit Control user module and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration page.

MAC Count (Current/Limit): The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

4.4.4.2.1.2 Port Status

Port Security Port Status Port 1				
Port 1		Auto-refresh	Refresh	
MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

This page shows MAC addresses learned on a particular port.

MAC Address: When “Port Security Limit Control” is enabled globally and on a port, MAC addresses learned on a port show in here.

VLAN ID: Display VLAN ID that is seen on this port.

State: Display whether the corresponding MAC address is forwarding or blocked. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition: Display the date and time when this MAC address was seen on the port.

Age/Hold: If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address is still forwarding traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

4.4.4.2.2 NAS

4.4.4.2.2.1 Switch

Network Access Server Switch Status						
Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled	-	-	-	-
2	Force Authorized	Globally Disabled	-	-	-	-
3	Force Authorized	Globally Disabled	-	-	-	-
4	Force Authorized	Globally Disabled	-	-	-	-
5	Force Authorized	Globally Disabled	-	-	-	-
6	Force Authorized	Globally Disabled	-	-	-	-
7	Force Authorized	Globally Disabled	-	-	-	-
8	Force Authorized	Globally Disabled	-	-	-	-
9	Force Authorized	Globally Disabled	-	-	-	-
10	Force Authorized	Globally Disabled	-	-	-	-
11	Force Authorized	Globally Disabled	-	-	-	-
12	Force Authorized	Globally Disabled	-	-	-	-
13	Force Authorized	Globally Disabled	-	-	-	-
14	Force Authorized	Globally Disabled	-	-	-	-
15	Force Authorized	Globally Disabled	-	-	-	-
16	Force Authorized	Globally Disabled	-	-	-	-
17	Force Authorized	Globally Disabled	-	-	-	-
18	Force Authorized	Globally Disabled	-	-	-	-
19	Force Authorized	Globally Disabled	-	-	-	-
20	Force Authorized	Globally Disabled	-	-	-	-
21	Force Authorized	Globally Disabled	-	-	-	-
22	Force Authorized	Globally Disabled	-	-	-	-
23	Force Authorized	Globally Disabled	-	-	-	-
24	Force Authorized	Globally Disabled	-	-	-	-
25	Force Authorized	Globally Disabled	-	-	-	-
26	Force Authorized	Globally Disabled	-	-	-	-
27	Force Authorized	Globally Disabled	-	-	-	-
28	Force Authorized	Globally Disabled	-	-	-	-
29	Force Authorized	Globally Disabled	-	-	-	-
30	Force Authorized	Globally Disabled	-	-	-	-
31	Force Authorized	Globally Disabled	-	-	-	-
32	Force Authorized	Globally Disabled	-	-	-	-
33	Force Authorized	Globally Disabled	-	-	-	-

Port: The port number. Click a port to view the detailed NAS statistics.

Admin State: Display the port's current administrative state.

Port Status: Display the port state.

Last Source: The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication.

Last ID: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication.

QoS Class: Display the QoS class that NAS assigns to the port. This field is left blank if QoS is not set by NAS.

Port VLAN ID: The VLAN ID of the port assigned by NAS. This field is left blank if VLAN ID is not set by NAS.

4.4.4.2.2 Port

NAS Statistics Port 16	
Port State	
Admin State	Force Authorized
Port State	Globally Disabled

Admin State: Display the port's current administrative state.

Port Status: Display the port state.

4.4.4.2.3 ACL Status

ACL Status

combinedAuto-refreshRefresh

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
No entries								

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 on each switch.

User: Display the ACL user.

ACE: Display the ingress port of the ACE. This field could be all ports, a specific port or a range of ports.

Frame Type: Display the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

IPv6: The ACE will match all IPv6 standard frames.

Action: Display the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE may be forwarded and learned.

Filtered: Frames matching the ACE are filtered.

Rate Limiter: Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect: Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

Mirror: Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

CPU: Forward packet that matched the specific ACE to CPU.

CPU Once: Forward first packet that matched the specific ACE to CPU.

Counter: The counter indicates the number of times the ACE was hit by a frame.

Conflict: Indicate the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

4.4.4.2.4 Dynamic ARP Inspection Table

Dynamic ARP Inspection Table

Auto-refresh☐ Refresh << >>

Start from Port1, VLAN 1, MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

Port: The port number of this entry.

VLAN ID: VLAN ID in which the ARP traffic is permitted.

MAC Address: User MAC address of this entry.

4.4.4.2.5 Dynamic IP Source Guard Table

The Dynamic IP Source Guard table shows entries sorted by port, VLAN ID, IP address and MAC address. By default, each page displays 20 entries. However, it can display 999 entries by entering the number in “entries per page” input field.

Dynamic IP Source Guard Table
Auto-refresh ☐ Refresh << >>

Start from Port 1 , VLAN 1 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

4.4.4.3 AAA

4.4.4.3.1 RADIUS Overview

RADIUS Server Status Overview					
#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1			Disabled		Disabled
2			Disabled		Disabled
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

IP Address: The configured IP address and UDP port number.

Status: The current state of RADIUS authentication & Accounting server. Displayed states include the following:

Disabled: This server is disabled.

Not Ready: The server is ready but IP communication is not yet up and running.

Ready: The server is ready and IP communication is not yet up and running. The RADIUS server is ready to accept access attempts.

4.4.4.3.2 RADIUS Details

RADIUS Authentication Statistics for Server #1			
Server #1		Auto-refresh	☐
		Refresh	Clear
Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address		0.0.0.0	
State		Disabled	
Round-Trip Time		0 ms	
RADIUS Accounting Statistics for Server #1			
Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address		0.0.0.0	
State		Disabled	
Round-Trip Time		0 ms	

RADIUS Authentication Statistics for Server

Access Accepts: The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

Access Rejects: The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

Access Challenges: The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

Malformed Access Responses: The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

Bad Authenticators: The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

Unknown Types: The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

Packets Dropped: The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

Access Requests: The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

Access Retransmissions: The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

Pending Requests: The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

Timeouts: The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address: IP address and UDP port for the authentication server in question.

State: Shows the state of the server. It takes one of the following values:

Disabled: The selected server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time: The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics for Server

Responses: The number of RADIUS packets (valid or invalid) received from the server.

Malformed Responses: The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

Bad Authenticators: The number of RADIUS packets containing invalid authenticators received from the server.

Unknown Types: The number of RADIUS packets of unknown types that were received from the server on the accounting port.

Packets Dropped: The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

Requests: The number of RADIUS packets sent to the server. This does not include retransmissions.

Retransmissions: The number of RADIUS packets retransmitted to the RADIUS accounting server.

Pending Requests: The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

Timeouts: The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address: IP address and UDP port for the accounting server in question.

State: Shows the state of the server. It takes one of the following values:

Disabled: The selected server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time: The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

4.4.4.4 Switch

4.4.4.4.1 RMON

4.4.4.4.1.1 RMON Statistics Overview

This RMON statistics overview page shows interface statistics. All values displayed have been accumulated since the last system reboot and are shown as counts per second. The system will automatically refresh every 60 seconds by default.

RMON Statistics Status Overview

Auto-refresh☐ Refresh << >>

Start from Control Index with entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

ID: Display an ID index.

Data Source: Port ID to Monitor.

Drop: The total number of dropped packets due to lack of resources.

Octets: The total number of octets of data received.

Pkts: The total number of packets (including bad packets, broadcast packets) received.

Broadcast: The total number of good packets received that were directed to the broadcast address.

Multicast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.

Undersize: The total number of packets received that were less than 64 octets.

Oversize: The total number of packets received that were longer than 64 octets.

Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.: The best estimate of the total number of collisions on this Ethernet segment.

64 Bytes: The total number of packets (including bad packets) received that were 64 octets in length.

X~Y (65~127, 128~255, 256~511, 512~1023, 1024~1588): The total number packets received between X and Y octets in length.

4.4.4.4.1.2 RMON History Overview

RMON History Overview

Auto-refresh☐ Refresh<<>>

Start from Control Index and Sample Index with entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

History Index: Display Index of History control entry.

Sample Index: Display Index of the data entry associated with the control entry.

Sample Start: The time at which this sample started, expressed in seconds since the switch booted up.

Drop: The total number of dropped packets due to lack of resources.

Octets: The total number of octets of data received.

Pkts: The total number of packets (including bad packets, broadcast packets) received.

Broadcast: The total number of good packets received that were directed to the broadcast address.

Multicast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.

Undersize: The total number of packets received that were less than 64 octets.

Oversize: The total number of packets received that were longer than 64 octets.

Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.: The best estimate of the total number of collisions on this Ethernet segment.

Utilization: The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

4.4.4.4.1.3 RMON Alarm Overview

RMON Alarm Overview									
Auto-refresh ☐ Refresh << >>									
Start from Control Index 0 with 20 entries per page.									
ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

ID: Display an alarm control index.

Interval: Interval in seconds for sampling and comparing the rising and falling threshold.

Variable: MIB object that is used to be sampled.

Sample Type: The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value: The value of the statistic during the last sampling period.

Startup Alarm: The alarm that may be triggered when this entry is first set to valid.

Rising Threshold: If the current value is greater than the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated.

Rising Index: The index of the event to use if an alarm is triggered by monitored variables crossing above the rising threshold.

Falling Threshold: If the current value is less than the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated.

Falling Index: The index of the event to use if an alarm is triggered by monitored variables crossing below the falling threshold.

4.4.4.4.1.4 RMON Event Overview

RMON Event Overview			
Start from Control Index 0 and Sample Index 0 with 20 entries per page.			
Event Index	LogIndex	LogTime	LogDescription
No more entries			

Event Index: Display the event entry index.

Log Index: Display the log entry index.

Log Time: Display Event log time.

Log Description: Display Event description.

4.4.5 Aggregation

4.4.5.1 Static

Aggregation Status					
Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
No aggregation groups					

Aggr ID: Display the aggregation ID associated with the Link Aggregation Group (LAG).

Name: Display the name of the Aggregation group ID.

Type: Display the type of Aggregation group (either Static or LACP).

Speed: Display the speed of the aggregation group.

Configured Ports: Display the configured ports of Aggregation group.

Aggregated Ports: Display aggregated member ports of the Aggregation group.

4.4.6 LACP

— LACP - System Status - Port Status - Port Statistics

4.4.6.1 System Status

LACP System Status					
Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

Aggr ID: Display the aggregation ID associated with the Link Aggregation Group (LAG).

Partner System ID: LAG's partner system ID (MAC address).

Partner Key: The partner key assigned to this LAG.

Partner Prio: The priority value of the partner.

Last Changed: The time since this LAG changed.

Local Ports: The local ports that are a port of this LAG.

4.4.6.2 Port Status

LACP Status						
Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-
13	No	-	-	-	-	-
14	No	-	-	-	-	-
15	No	-	-	-	-	-
16	No	-	-	-	-	-
17	No	-	-	-	-	-
18	No	-	-	-	-	-
19	No	-	-	-	-	-
20	No	-	-	-	-	-
21	No	-	-	-	-	-
22	No	-	-	-	-	-
23	No	-	-	-	-	-
24	No	-	-	-	-	-
25	No	-	-	-	-	-
26	No	-	-	-	-	-
27	No	-	-	-	-	-
28	No	-	-	-	-	-
29	No	-	-	-	-	-
30	No	-	-	-	-	-
31	No	-	-	-	-	-
32	No	-	-	-	-	-
33	No	-	-	-	-	-

Port: The port number.

LACP: Show LACP status on a port.

Yes: LACP is enabled and the port link is up.

No: LACP is not enabled or the port link is down.

Backup: The port is in a backup role. When other ports leave LAG group, this port will join LAG.

Key: The aggregation key value on a port.

Aggr ID: Display the aggregation ID active on a port.

Partner System ID: LAG partner's system ID.

Partner Port: The partner port connected to this local port.

Partner Prio: The priority value of the partner.

4.4.6.3 Port Statistics

LACP Statistics					
Port	LACP Received	LACP Transmitted	Discarded		
			Unknown	Illegal	
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	0
9	0	0	0	0	0
10	0	0	0	0	0
11	0	0	0	0	0
12	0	0	0	0	0
13	0	0	0	0	0
14	0	0	0	0	0
15	0	0	0	0	0
16	0	0	0	0	0
17	0	0	0	0	0
18	0	0	0	0	0
19	0	0	0	0	0
20	0	0	0	0	0
21	0	0	0	0	0
22	0	0	0	0	0
23	0	0	0	0	0
24	0	0	0	0	0
25	0	0	0	0	0
26	0	0	0	0	0
27	0	0	0	0	0
28	0	0	0	0	0
29	0	0	0	0	0
30	0	0	0	0	0
31	0	0	0	0	0
32	0	0	0	0	0
33	0	0	0	0	0

Port: The port number.

LACP Received: The number of LACP packets received on a port.

LACP Transmitted: The number of LACP packets transmitted by a port

Discarded: The number of unknown and illegal packets that have been discarded on a port.

4.4.7 Loop Protection

Loop Protection Status						
Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-
13	Shutdown	Enabled	0	Down	-	-
14	Shutdown	Enabled	0	Down	-	-
15	Shutdown	Enabled	0	Down	-	-
16	Shutdown	Enabled	0	Down	-	-
17	Shutdown	Enabled	0	Down	-	-
18	Shutdown	Enabled	0	Down	-	-
19	Shutdown	Enabled	0	Down	-	-
20	Shutdown	Enabled	0	Down	-	-
21	Shutdown	Enabled	0	Down	-	-
22	Shutdown	Enabled	0	Down	-	-
23	Shutdown	Enabled	0	Down	-	-
24	Shutdown	Enabled	0	Down	-	-
25	Shutdown	Enabled	0	Down	-	-
26	Shutdown	Enabled	0	Down	-	-
27	Shutdown	Enabled	0	Down	-	-
28	Shutdown	Enabled	0	Down	-	-
29	Shutdown	Enabled	0	Down	-	-
30	Shutdown	Enabled	0	Down	-	-
31	Shutdown	Enabled	0	Down	-	-
32	Shutdown	Enabled	0	Down	-	-
33	Shutdown	Enabled	0	Up	-	-

Port: The port number.

Action: Display the configured action that the switch will react when loops occur.

Transmit: Display the configured transmit (Tx) mode.

Loops: The number of loops detected on a port.

Status: The current loop status detected on a port.

Loop: Loops detected on a port or not.

Time of Last Loop: The time of the last loop event detected.

4.4.8 Spanning Tree

4.4.8.1 Bridge Status

STP Bridges Auto-refresh ☐ Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-02-AB-D6-68-B0	32768.00-02-AB-D6-68-B0	-	0	Steady	-

MSTI: The bridge instance. Click this instance to view STP detailed bridge status.

Bridge ID: The unique bridge ID for this instance consisting a priority value and MAC address of the bridge switch.

Root ID: Display the root device's priority value and MAC address.

Root Port: The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

Root Cost: The path cost from the root port on the switch to the root device. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.

Topology Flag: The current state of the Topology Change Notification flag for this bridge instance.

Topology Change Last: The time since this spanning tree was last configured.

Click the MSTI instance to view STP detailed bridge status.

STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-02-AB-D6-68-B0
Root ID	32768.00-02-AB-D6-68-B0
Root Cost	0
Root Port	-
Regional Root	32768.00-02-AB-D6-68-B0
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
1	128:001	DesignatedPort	Forwarding	20000	Yes	Yes	0d 00:01:18
3	128:003	BackupPort	Discarding	20000	No	Yes	0d 00:01:18
5	128:005	DesignatedPort	Forwarding	200000	Yes	Yes	0d 00:01:39

STP Detailed Bridge Status

Bridge Instance: The bridge instance.

Bridge ID: The unique bridge ID for this instance consisting a priority value and MAC address of the bridge switch.

Root ID: Display the root device's priority value and MAC address.

Root Cost: The path cost from the root port on the switch to the root device. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.

Root Port: The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

Regional Root: The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (This parameter only applies to the CIST instance.)

Internal Root Cost: The Regional Root Path Cost. For the Regional Root Bridge the cost is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (This parameter only applies to the CIST instance.)

Topology Flag: The current state of the Topology Change Notification flag for this bridge instance.

Topology Change Last: The time since this spanning tree was last configured.

CIST Ports & Aggregations State

Port: Display the port number.

Port ID: The port identifier used by the RSTP protocol. This port ID contains the priority and the port number.

Role: The role assigned by Spanning Tree Algorithm. Roles can be "Designated Port", "Backup Port", "Root Port".

State: Display the current state of a port.

Blocking: Ports only receive BPDU messages but do not forward them.

Learning: Port has transmitted configuration messages for an interval set by the Forward Delay parameter

without receiving contradictory information. Port address table is cleared, and the port begins learning addresses

Forwarding: Ports forward packets and continue to learn addresses.

Edge: Display whether this port is an edge port or not.

Point-to-Point: Display whether this point is in point-to-point connection or not. This can be both automatically and manually configured.

Uptime: The time since the bridge port was last initialized.

4.4.8.2 Port Status

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	Non-STP	Forwarding	-
25	Non-STP	Forwarding	-
26	Non-STP	Forwarding	-
27	Non-STP	Forwarding	-
28	Non-STP	Forwarding	-
29	Non-STP	Forwarding	-
30	Non-STP	Forwarding	-
31	Non-STP	Forwarding	-
32	Non-STP	Forwarding	-
33	Non-STP	Forwarding	-

Port: The port number.

CIST Role: The role assigned by Spanning Tree Algorithm. Roles can be “Designated Port”, “Backup Port”, “Root Port” or “Non-STP”.

CIST State: Display the current state of a port. The CIST state must be one of the following:

Blocking: Ports only receive BPDU messages but do not forward them.

Learning: Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses

Forwarding: Ports forward packets and continue to learn addresses.

Uptime: The time since the bridge port was last initialized.

4.4.8.3 Port Statistics

STP Statistics										
Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	0	103	0	0	0	3	0	0	0	0
3	0	3	0	0	0	103	0	0	0	0
5	2228	114	0	0	0	0	0	0	0	0

Port: Display the port number.

Transmitted & Received MSTP/RSTP/STP: The number of MSTP/RSTP/STP configuration BPDU messages transmitted and received on a port.

Transmitted & Received TCN: The number of TCN messages transmitted and received on a port.

Discarded Unknown/Illegal: The number of unknown and illegal packets discarded on a port.

4.4.9 MVR

- MVR
 - Statistics
 - MVR Channel Groups
 - MVR SFM Information

4.4.9.1 MVR Statistics

MVR Statistics						
VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
200	0 / 0	0 / 0	0	0 / 0	0 / 0	0 / 0

This page displays MVR statistics information on queries, joins, reports and leaves messages.

VLAN ID: Display VLAN ID that is used for processing multicast traffic.

IGMP/MLD Queries Received: The number of received queries for IGMP and MLD.

IGMP/MLD Queries Transmitted: The number of transmitted queries for IGMP/MLD.

IGMPv1 Joins Received: The number of IGMPv1 received joins

IGMPv2/MLDv1 Reports Received: The number of IGMPv2 and MLDv1 received reports.

IGMPv3/MLDv2 Reports Received: The number of IGMPv3 and MLDv2 received reports.

IGMPv2/MLDv1 Leaves Received: The number of IGMPv2 and MLDv1 received leaves.

4.4.9.2 MVR Channel Groups

MVR Channels (Groups) Information

Auto-refresh☐ Refresh << >>

Start from VLAN and Group Address with entries per page.

		Port Members																																
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
No more entries																																		

Start from VLAN ____ and Group Address _____ with 20 entries per page.

This table displays MVR channels (groups) information and is sorted by VLAN ID.

VLAN ID: VLAN ID of the group.

Groups: Group ID

Port Members: Ports that belong to this group.

4.4.9.3 MVR SFM Information

MVR SFM Information						
Start from VLAN 1 and Group Address :: with 20 entries per page.						
VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

VLAN ID: VLAN ID of the group.

Group: The group address.

Port: Switch port number.

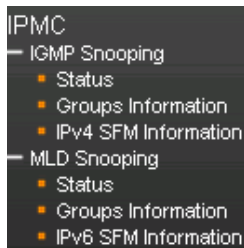
Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address: The source IP Address. Currently, the system limits the total number of source IP addresses for filtering to be 128. When there is no source filtering address, "None" is shown in the Source Address field.

Type: Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch: Indicate whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

4.4.10 IPMC



4.4.10.1 IGMP Snooping

4.4.10.1.1 Status

IGMP Snooping Status									
Statistics									
VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
Router Port									
Port	Status								
1	-								
2	-								
3	-								
4	-								
5	-								
6	-								
7	-								
8	-								
9	-								
10	-								
11	-								
12	-								
13	-								
14	-								
15	-								
16	-								
17	-								
18	-								
19	-								
20	-								
21	-								
22	-								
23	-								
24	-								
25	-								
26	-								
27	-								
28	-								
29	-								
30	-								
31	-								
32	-								
33	-								

Statistics

VLAN ID: The VLAN ID of this entry.

Querier Version: The current working Querier version.

Host Version: The current host version.

Querier Status: Show the Querier status that is either "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted: The number of queries transmitted.

Queries Received: The number of queries received.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V3 Reports Received: The number of Received V3 Reports.

V2 Leaves Received: The number of Received V2 Leaves.

Router Port

Port: The port number.

Status: Indicate whether a specific port is a router port or not.

4.4.10.1.2 Groups Information

IGMP Snooping Group Information																																		Auto-refresh ☐ Refresh << >>			
Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.																																					
																Port Members																					
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33			
No more entries																																					

VLAN ID: Display the VLAN ID of the group.

Groups: Display the group address.

Port Members: Ports that belong to this group.

4.4.10.1.3 IPv4 SFM Information

IGMP SFM Information

Start from VLAN and Group with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

VLAN ID: Display the VLAN ID of the group.

Groups: Display the IP address of a multicast group.

Port: The switch port number.

Mode: The filtering mode maintained per VLAN ID, port number and group address.

Source Address: The source IP address available for filtering.

Type: Display either Allow or Deny type.

Hardware Filter/Switch: Indicates whether the data plane destined to the specific group address from the source IPv4 address can be handled by the chip or not.

4.4.10.2 MLD Snooping

4.4.10.2.1 Status

MLD Snooping Status									
Statistics									
VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received	
Router Port									
Port	Status								
1	-								
2	-								
3	-								
4	-								
5	-								
6	-								
7	-								
8	-								
9	-								
10	-								
11	-								
12	-								
13	-								
14	-								
15	-								
16	-								
17	-								
18	-								
19	-								
20	-								
21	-								
22	-								
23	-								
24	-								
25	-								
26	-								
27	-								
28	-								
29	-								
30	-								
31	-								
32	-								
33	-								

Statistics

VLAN ID: The VLAN ID of this entry.

Querier Version: The current working Querier version.

Host Version: The current host version.

Querier Status: Show the Querier status that is either "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted: The number of queries transmitted.

Queries Received: The number of queries received.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V2 Leaves Received: The number of Received V2 Leaves.

Router Port

Port: The port number.

Status: Indicate whether a specific port is a router port or not.

4.4.10.2.2 Groups Information

MLD Snooping Group Information

Auto-refresh ☐ Refresh |<< >>

Start from VLAN 1 and group address ff00:: with 20 entries per page.

VLAN ID	Groups	Port Members																															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
No more entries																																	

VLAN ID: Display the VLAN ID of the group.

Groups: Display the group address.

Port Members: Ports that belong to this group.

4.4.10.2.3 IPv6 SFM Information

MLD SFM Information

Start from VLAN 1 and Group ff00:: with 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

VLAN ID: Display the VLAN ID of the group.

Group: Display the IP address of a multicast group.

Port: The switch port number.

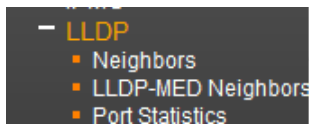
Mode: The filtering mode maintained per VLAN ID, port number and group address.

Source Address: The source IP address available for filtering.

Type: Display either Allow or Deny type.

Hardware Filter/Switch: Indicates whether the data plane destined to the specific group address from the source IPv4 address can be handled by the chip or not.

4.4.11 LLDP



4.4.11.1 Neighbors

LLDP Neighbor Information						
LLDP Remote Device Summary						
Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbor information found						

Local Port: The local port that a remote LLDP-capable device is attached.

Chassis ID: An ID indicating the particular chassis in this system.

Port ID: A remote port ID that LDPDU's were transmitted.

Port Description: A remote port's description.

System Name: The system name assigned to the remote system.

System Capabilities: This shows the neighbour unit's capabilities. When a capability is enabled, the capability is followed by (+). If disabled, the capability is followed by (-).

Management Address: The IPv4 address of the remote device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. If the neighbor device allows management access, clicking on an entry in this field will re-direct the web browser to the neighbor's management interface.

4.4.11.2 LLDP-MED Neighbors

LLDP-MED Neighbour Information	
Local Port	
No LLDP-MED neighbour information found	

This page displays information about LLDP-MED neighbours detected on the network.

4.4.11.3 Port Statistics

LLDP Statistics Local Counters									
Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/2	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/4	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/5	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/6	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/7	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/8	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/9	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/10	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/11	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/12	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/13	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/14	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/15	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/16	0	0	0	0	0	0	0	0	✓
2.5GigabitEthernet 1/1	0	0	0	0	0	0	0	0	✓
2.5GigabitEthernet 1/2	0	0	0	0	0	0	0	0	✓
2.5GigabitEthernet 1/3	0	0	0	0	0	0	0	0	✓
2.5GigabitEthernet 1/4	0	0	0	0	0	0	0	0	✓
2.5GigabitEthernet 1/5	0	0	0	0	0	0	0	0	✓
2.5GigabitEthernet 1/6	0	0	0	0	0	0	0	0	✓
2.5GigabitEthernet 1/7	0	0	0	0	0	0	0	0	✓
2.5GigabitEthernet 1/8	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/17	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/18	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/19	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/20	0	0	0	0	0	0	0	0	✓
10GigabitEthernet 1/1	0	0	0	0	0	0	0	0	✓
10GigabitEthernet 1/2	0	0	0	0	0	0	0	0	✓
10GigabitEthernet 1/3	0	0	0	0	0	0	0	0	✓
10GigabitEthernet 1/4	0	0	0	0	0	0	0	0	✓
GigabitEthernet 1/21	0	0	0	0	0	0	0	0	✓

LLDP Global Counters

Total Neighbours Entries Added: Shows the number of new entries added since the switch was rebooted, and for which the remote TTL has not yet expired.

Total Neighbors Entries Deleted: The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.

Total Neighbors Entries Dropped: The number of times which the remote database on this switch dropped an LLDPDU because the entry table was full.

Total Neighbors Entries Aged Out: The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

LLDP Statistics Local Counters

Local Port: The port number.

Tx Frames: The number of LLDP PDUs transmitted.

Rx Frames: The number of LLDP PDUs received.

Rx Errors: The number of received LLDP frames with some kind of error.

Frames Discarded: The number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular Type Length Value (TLV).

TLVs Discarded: Each LLDP frame can contain multiple pieces of information, known as TLVs. If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized: The number of well-formed TLVs, but with an unknown type value.

Org. Discarded: The number of organizational TLVs discarded.

Age-Outs: Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age-out time, the LLDP information is removed, and the Age-Out counter is incremented.

4.4.12 MAC Table

The MAC Address Table shows both static and dynamic MAC addresses learned from CPU or switch ports. You can enter the starting VLAN ID and MAC addresses to view the desired entries.

MAC Address Table

Auto-refresh ☐ Refresh Clear << >>

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
Static	1	01-00-5E-7F-FF-FA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-11-22-33	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	F0-DE-F1-0B-65-9D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Type: This field displays whether the learned MAC address is static or dynamic.

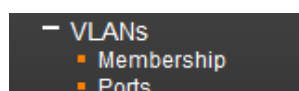
VLAN ID: The VLAN ID associated with this entry.

MAC Address: The MAC address learned on CPU or certain ports.

Port Members: Ports associated with this entry.

Flush Dynamic Entries: Refresh all MAC addresses or refresh MAC addresses on a per port or per VLAN basis.

4.4.13 VLANs



4.4.13.1 Membership

VLAN Membership Status for Combined users

Start from VLAN 1 with 20 entries per page. << >>

	Port Members																																
VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

This page shows the current VLAN membership saved on the Switch.

VLAN ID: VLANs that are already created.

Port members: Display member ports on the configured VLANs.

4.4.13.2 Ports

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☒	All	1	Untag All		No
2	C-Port	☒	All	1	Untag All		No
3	C-Port	☒	All	1	Untag All		No
4	C-Port	☒	All	1	Untag All		No
5	C-Port	☒	All	1	Untag All		No
6	C-Port	☒	All	1	Untag All		No
7	C-Port	☒	All	1	Untag All		No
8	C-Port	☒	All	1	Untag All		No
9	C-Port	☒	All	1	Untag All		No
10	C-Port	☒	All	1	Untag All		No
11	C-Port	☒	All	1	Untag All		No
12	C-Port	☒	All	1	Untag All		No
13	C-Port	☒	All	1	Untag All		No
14	C-Port	☒	All	1	Untag All		No
15	C-Port	☒	All	1	Untag All		No
16	C-Port	☒	All	1	Untag All		No
17	C-Port	☒	All	1	Untag All		No
18	C-Port	☒	All	1	Untag All		No
19	C-Port	☒	All	1	Untag All		No
20	C-Port	☒	All	1	Untag All		No
21	C-Port	☒	All	1	Untag All		No
22	C-Port	☒	All	1	Untag All		No
23	C-Port	☒	All	1	Untag All		No
24	C-Port	☒	All	1	Untag All		No
25	C-Port	☒	All	1	Untag All		No
26	C-Port	☒	All	1	Untag All		No
27	C-Port	☒	All	1	Untag All		No
28	C-Port	☒	All	1	Untag All		No
29	C-Port	☒	All	1	Untag All		No
30	C-Port	☒	All	1	Untag All		No
31	C-Port	☒	All	1	Untag All		No
32	C-Port	☒	All	1	Untag All		No
33	C-Port	☒	All	1	Untag All		No

Port: The port number.

Port Type: Displays the selected port type of each port.

Ingress Filtering: Displays whether Ingress Filtering function of each port is enabled or not. When the checkbox is selected, it indicates that Ingress Filtering is enabled.

Frame Type: Displays the accepted Ingress frame type.

Port VLAN ID: Display the Port VLAN ID (PVID).

Tx Tag: Displays the Egress action on a port.

Untagged VLAN ID: Display the untagged VLAN ID. A port's UVID determines the packet's behavior at the egress side. If the VID of Ethernet frames leaving a port match the UVID, these frames will be sent untagged.

Conflicts: Display whether conflicts exist or not. When a software module requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

- *Functional conflicts between features.
- *Conflicts due to hardware limitations.
- *Direct conflicts between user modules.

4.4.14 sFlow

sFlow Statistics

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

Port	Flow Samples	Counter Samples
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0
29	0	0
30	0	0
31	0	0
32	0	0
33	0	0

This page shows receiver and per-port sFlow statistics.

Receiver Statistics

Owner: This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

IP Address/Hostname: This field shows the IP address or hostname of the sFlow receiver.

Timeout: This shows the number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes: The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors: The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).

Flow Samples: The total number of flow samples sent to the sFlow receiver.

Counter Samples: The total number of counter samples sent to the sFlow receiver.

Port Statistics

Port: The port number for which the following statistics applies.

Rx and Tx Flow Samples: The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

Counter Samples: The total number of counter samples sent to the sFlow receiver originating from this port.

4.4.15 UDLD

Detailed UDLD Status for Port 1
Port 1

UDLD status	
UDLD Admin state	Disable
Device ID(local)	00-02-AB-06-20-20
Device Name(local)	-
Bidirectional State	Indeterminant

Neighbour Status

Port	Device Id	Link Status	Device Name
No Neighbour ports enabled or no existing partners			

UDLD Status

UDLD Admin State: The current port state of the logical port, Enabled if any of state(Normal,Aggressive) is Enabled.

Device ID (local): The ID of Device.

Device Name (local): Name of the Device.

Bidirectional State: The current state of the port.

Neighbour Status

Port: The current port of neighbour device.

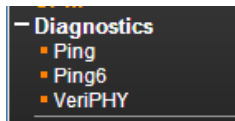
Device ID: The current ID of neighbour device.

Link Status: The current link status of neighbour port.

Device Name: Name of the Neighbour Device.

4.5 Diagnostics

The “Diagnostics” menu provides ping function to test the connectivity of a certain IP.



4.5.1 Ping

This Ping function is for ICMPv4 packets.

A screenshot of the 'ICMP Ping' configuration form. It features four input fields: 'IP Address' with the value '0.0.0.0', 'Ping Length' with '56', 'Ping Count' with '5', and 'Ping Interval' with '1'. Below these fields is a 'Start' button.

IP Address: Enter the IP address that you wish to ping.

Ping Length: The size or length of echo packets.

Ping Count: The number of echo packets will be sent.

Ping Interval: The time interval between each ping request.

4.5.3 Ping6

This Ping function is for ICMPv6 packets.

A screenshot of the 'ICMPv6 Ping' configuration form. It features five input fields: 'IP Address' with the value '0:0:0:0:0:0:0:0', 'Ping Length' with '56', 'Ping Count' with '5', 'Ping Interval' with '1', and 'Egress Interface' which is empty. Below these fields is a 'Start' button.

IP Address: Enter the IP address that you wish to ping.

Ping Length: The size or length of echo packets.

Ping Count: The number of echo packets will be sent.

Ping Interval: The time interval between each ping request.

Egress Interface: The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When this field is not specified, Ping6 will find the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.

4.27.3 VeriPHY

The VeriPHY Cable Diagnostics page is used to perform cable diagnostics for all ports or selected ports to diagnose any cable faults (short, open, etc.) and report the cable length.

VeriPHY Cable Diagnostics								
Port: All ▼								
Start								
Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
25	--	--	--	--	--	--	--	--
26	--	--	--	--	--	--	--	--
27	--	--	--	--	--	--	--	--
28	--	--	--	--	--	--	--	--
33	--	--	--	--	--	--	--	--

Port: Select All (all ports) or a port to perform cable diagnostics.

Start: Click the “Start” button to begin the diagnostics.

Cable Status

Port: The port number.

Pair A/B/C/D: The status of cable pair.

OK: Correctly terminated pair
 Open: Open pair
 Short: Shorted pair
 Short A: Cross-pair short to pair A
 Short B: Cross-pair short to pair B
 Short C: Cross-pair short to pair C
 Short D: Cross-pair short to pair D
 Cross A: Abnormal cross-pair coupling with pair A
 Cross B: Abnormal cross-pair coupling with pair B
 Cross C: Abnormal cross-pair coupling with pair C
 Cross D: Abnormal cross-pair coupling with pair D

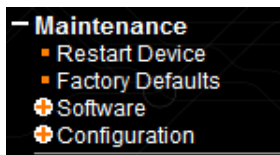
Length A/B/C/D: The length (in meters) of the cable pair.

Note:

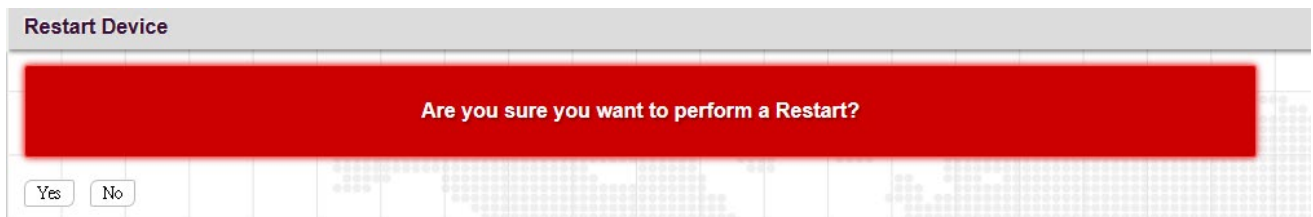
1. If a specific port is selected, the test will take approximately 5 seconds. If all ports are selected, it can run approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.
 2. VeriPHY is only accurate for cables of length 7 - 140 meters.
 3. 10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.
 4. The EEE must be disabled at link partner.
-

4.6 Maintenance

The “Maintenance” menu contains several sub menus. Select the appropriate sub menu to restart the device, set the device to the factory default or upgrade firmware image.



4.6.1 Restart Device



Click “Yes” button to reboot the switch.

4.6.2 Factory Defaults



Click “Yes” button to reset your device to factory defaults settings. Please note that all changed settings will be lost. It is recommended that a copy of the current configuration is saved to your local device.

4.6.3 Software

4.6.3.1 Upload



Update the latest Firmware file.

Select a Firmware file from your local device and then click “Upload” to start updating.

4.6.3.2 Image Select

Software Image Selection	
Active Image	
Image	GSW-3424FM1007.dat
Version	"V1.007"
Date	2019-07-12T11:53:10+08:00
Alternate Image	
Image	GSW-3424FM1005.dat
Version	"V1.005"
Date	2019-04-09T16:18:27+08:00
Activate Alternate Image Cancel	

Select the image file to be used in this device.

4.6.4 Configuration

4.6.4.1 Save

Save Running Configuration to startup-config
Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.
Save Configuration

Click on the "Save Configuration" button to save current running configurations to startup configurations.

4.6.4.2 Download

Download Configuration				
Select configuration file to save.				
Please note: running-config may take a while to prepare for download.				
<table border="1"> <thead> <tr> <th>File Name</th> </tr> </thead> <tbody> <tr> <td>☐ running-config</td> </tr> <tr> <td>☐ default-config</td> </tr> <tr> <td>☐ startup-config</td> </tr> </tbody> </table>	File Name	☐ running-config	☐ default-config	☐ startup-config
File Name				
☐ running-config				
☐ default-config				
☐ startup-config				
Download Configuration				

running-config: Download a copy of the current running configurations to your local device.

default-config: Download a copy of the factory default configurations to your local device.

startup-config: Download a copy of startup configurations to your local device.

4.6.4.3 Upload

Upload Configuration

File To Upload

Browse... No file selected.

Destination File

File Name	Parameters
☒ running-config	☒ Replace ☐ Merge
☐ startup-config	
☐ Create new file	

Upload Configuration

Select a file and then click “Upload Configuration” to start uploading the file.

4.6.4.4 Activate

Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

File Name

☐ default-config
☐ startup-config

Activate Configuration

Select the file that you would like to use. Click on the “Activate Configuration” to replace configurations to the selected one.

4.6.4.5 Delete

Delete Configuration File

Select configuration file to delete.

File Name

☐ startup-config

Delete Configuration File

Select the file that you would like to delete. Click on the “Delete Configuration File” to remove the file from the device.

This page is intentionally left blank.