



CE Services Products

User Guide



21.4.2020
Version 1

Contents

1	Overview.....	19
1.1	Indicators	19
2	Command Line Interface	20
2.1	Command Line Overview.....	20
2.1.1	Context-Sensitive Help	20
2.1.2	Command Line Syntax	20
2.1.3	Output Modifiers.....	22
2.1.4	Ethernet Interface Reference	23
2.1.5	CLI Command Description	23
2.2	Clear Commands.....	23
2.2.1	Clear Access	24
2.2.2	Clear Access-List.....	24
2.2.3	Clear Dot1x.....	24
2.2.4	Clear EPS	24
2.2.5	Clear ERPS.....	24
2.2.6	Clear EVC	25
2.2.7	Clear IP.....	25
2.2.8	Clear IPV6.....	26
2.2.9	Clear LACP.....	27
2.2.10	Clear Link-OAM.....	27
2.2.11	Clear LLDP	27
2.2.12	Clear Logging.....	27
2.2.13	Clear MAC.....	27
2.2.14	Clear Mep	28
2.2.15	Clear MVR.....	28
2.2.16	Clear Network-clock	28
2.2.17	Clear sFLOW	28
2.2.18	Clear Spanning-Tree	28
2.2.19	Clear Statistics.....	29
2.3	Configuration Commands	29
2.3.1	AAA	29
2.3.2	Access.....	30
2.3.3	Access-List ACE.....	30
2.3.4	Access-List Rate-Limiter.....	36
2.3.5	Aggregation.....	36
2.3.6	Banner	36
2.3.7	Clock.....	36
2.3.8	Default.....	37
2.3.9	Do	37
2.3.10	Dot1x	37
2.3.11	Enable.....	38
2.3.12	End.....	39

2.3.13	EPS.....	39
2.3.14	ERPS.....	41
2.3.15	EVC.....	42
2.3.16	Exit.....	43
2.3.17	Firmware.....	43
2.3.18	Green-Ethernet.....	44
2.3.19	GVRP.....	44
2.3.20	Help.....	45
2.3.21	Hostname.....	45
2.3.22	Interface – Port Type.....	45
2.3.23	Interface – VLAN.....	70
2.3.24	IP.....	74
2.3.25	IPMC.....	77
2.3.26	IPV6.....	77
2.3.27	JSON.....	78
2.3.28	Lacp.....	78
2.3.29	Line.....	78
2.3.30	Lldp.....	79
2.3.31	Logging.....	81
2.3.32	Loop-Protect.....	81
2.3.33	Mac.....	82
2.3.34	Mep.....	83
2.3.35	Monitor.....	83
2.3.36	MVR.....	84
2.3.37	Network-clock.....	86
2.3.38	No.....	87
2.3.39	NTP.....	93
2.3.40	Port Security.....	93
2.3.41	Privilege.....	94
2.3.42	PTP.....	94
2.3.43	Qos.....	97
2.3.44	Radius-Server.....	99
2.3.45	Rmon.....	100
2.3.46	sFLOW.....	102
2.3.47	SNMP-Server.....	102
2.3.48	Spanning-tree.....	107
2.3.49	Switchport.....	108
2.3.50	Tacacs-server.....	108
2.3.51	thermal-protect.....	109
2.3.52	UDLD.....	109
2.3.53	UPnP.....	109
2.3.54	Username.....	110
2.3.55	Vlan.....	110
2.3.56	Voice.....	110
2.3.57	Web.....	111

2.4	Copy	111
2.5	Delete	112
2.6	Dir.....	112
2.7	Disable	112
2.8	Do	113
2.9	Dot1x	113
2.10	Enable.....	113
2.11	Erps.....	113
2.12	Exit.....	114
2.13	Firmware	114
2.14	Help.....	114
2.15	IP.....	114
2.16	Ipv6.....	115
2.17	Link-OAM	115
2.18	Logout.....	115
2.19	More	116
2.20	No	116
2.21	Ping.....	117
2.22	Platform	117
2.23	PTP	118
2.24	Reload	118
2.25	Send	118
2.26	Show.....	119
2.27	Terminal.....	123
2.28	Veriphy	124
2.29	Factory Default Configuration	124
3	Web Interface – Introduction.....	126
3.1	Web Interface – Configuration	126
3.2	Web Interface – Monitoring	126
3.3	Web Interface – Diagnostics.....	127
3.4	Web Interface – Maintenance.....	127
3.5	Web Interface – Getting Started	127
3.6	Web Interface – Login Window.....	128
4	Web Interface – Configuration.....	129
4.1	System Information Configuration	129
4.2	System – IP	130
4.2.1	IP Interfaces.....	131
4.2.2	IP Routes.....	133
4.2.3	IP Configuration Buttons.....	134
4.3	System – NTP.....	135
4.3.1	NTP Configuration.....	135
4.3.2	NTP Buttons	135
4.4	System - Time.....	136
4.4.1	Time Zone Configuration.....	136
4.4.2	Daylight Saving Time	136

4.4.3	Time Buttons	137
4.5	System - Log	138
4.5.1	System Log Configuration	138
4.5.2	Log Buttons	139
4.6	Green Ethernet – LED	140
4.6.1	Status LED	140
4.6.2	Front Ethernet Port LEDs	140
4.6.3	LEDs Intensity	141
4.6.4	Maintenance	141
4.6.5	Buttons	142
4.7	Green Ethernet - Port Power Savings	143
4.7.1	Port Configuration	144
4.7.2	Port Power Savings Buttons	144
4.8	Thermal Protection Configuration	145
4.8.1	Temperature Settings for Priority Groups	145
4.8.2	Port Priorities	145
4.8.3	Thermal Protection Configuration Buttons	145
4.9	Ports	146
4.9.1	Port Configuration	146
4.9.2	Port Configuration Buttons	148
4.10	DHCP	149
4.10.1	DHCP Server Mode Configuration	149
4.10.2	DHCP Server Excluded IP Configuration	150
4.10.3	DHCP Server Pool Configuration	151
4.11	Security – Switch - Users Configurations	156
4.12	Security – Switch – Privilege Levels	157
4.12.1	Group name	157
4.12.2	Privilege Level	158
4.12.3	Privilege Levels Buttons	158
4.13	Security – Switch – Auth Method	159
4.13.1	Authentication Method Configuration	159
4.13.2	Command Authorization Method Configuration	160
4.13.3	Accounting Method Configuration	160
4.13.4	Authentication Method Buttons	161
4.14	Security – Switch – SSH	162
4.14.1	SSH Configuration	162
4.14.2	SSH Buttons	162
4.15	Security – Switch – HTTPS	163
4.15.1	HTTPS Configuration	163
4.15.2	HTTPS Buttons	164
4.16	Security – Switch – Access Management	165
4.16.1	Access Management Configuration	165
4.16.2	Access Management Buttons	166
4.17	Security – Switch – SNMP– System	167
4.17.1	System	167

4.17.2	SNMP System Configuration Buttons	168
4.18	Security – Switch – SNMP – Trap.....	169
4.18.1	Global Settings	169
4.18.2	Trap Destination Configurations	169
4.18.3	Trap Configuration Buttons	170
4.19	Security – Switch – SNMP – Communities	171
4.19.1	SNMPv3 Community Configuration.....	171
4.19.2	Community Configuration Buttons.....	172
4.20	Security – Switch – SNMP – Users	173
4.20.1	SNMPv3 User Configuration	173
4.20.2	User Configuration Buttons	175
4.21	Security – Switch – SNMP – Groups.....	176
4.21.1	SNMPv3 Group Configuration.....	176
4.21.2	Group Configuration Buttons.....	177
4.22	Security – Switch – SNMP – Views	178
4.22.1	SNMPv3 View Configuration	178
4.22.2	View Configuration Buttons	179
4.23	Security – Switch – SNMP – Access	180
4.23.1	SNMPv3 Access Configuration	180
4.23.2	Access Configuration Buttons	181
4.24	Security – Switch – SNMP – RMON	182
4.24.1	RMON Statistics Configuration.....	182
4.24.2	RMON Statistics Configuration Buttons	182
4.25	Security – Switch – RMON – History	183
4.25.1	SNMPv3 Access Configuration	183
4.25.2	RMON History Configuration Buttons	184
4.26	Security – Switch – RMON – Alarm	185
4.26.1	Alarm Configuration.....	185
4.26.2	RMON Alarm Configuration Buttons	187
4.27	Security – Switch – RMON – Event	188
4.27.1	RMON Event Configuration.....	188
4.27.2	RMON Event Configuration Buttons	189
4.28	Security – Network – Limit Control.....	190
4.28.1	System Configuration	190
4.28.2	Port Configuration	191
4.28.3	Limit Control Configuration Buttons	193
4.29	Security – Network – NAS	194
4.29.1	System Configuration	195
4.29.2	Port Configuration	197
4.29.3	NAS Configuration Buttons	202
4.30	Security – Network – ACL – Ports	203
4.30.1	ACL Ports Configuration	203
4.30.2	ACL Ports Configuration Buttons	205
4.31	Security – Network – ACL – Rate Limiters.....	206
4.31.1	ACL Rate Limiter Configuration.....	206

4.31.2	ACL Rate Limiter Configuration Buttons	206
4.32	Security – Network – ACL – Access Control List	208
4.32.1	Access Control List Configuration	208
4.32.2	Access Control List Configuration Buttons	210
4.33	Security – Network – IP Source Guard.....	227
4.33.1	IP Source Guard Configuration.....	227
4.33.2	Port Mode Configuration	227
4.33.3	IP Source Buttons.....	227
4.33.4	Static Table Buttons	228
4.34	Security – Network – ARP Inspection – Port.....	229
4.34.1	Mode of ARP Inspection Configuration.....	229
4.34.2	Port Mode Configuration	229
4.34.3	ARP Inspection Port Buttons	230
4.35	Security – Network – ARP Inspection – VLAN	231
4.35.1	VLAN Mode Configuration	231
4.35.2	ARP Inspection VLAN Buttons	232
4.36	Security – Network – ARP Inspection – Static Table	233
	Static Table Buttons	233
4.37	Security – Network – ARP Inspection – Dynamic Table.....	234
	Dynamic Table Buttons	235
4.38	Security – AAA – Radius.....	236
4.38.1	Global Configuration	236
4.38.2	Server Configuration.....	237
4.38.3	RADIUS Server Configuration Buttons.....	238
4.39	Security – AAA – TACACS+.....	239
4.39.1	Global Configuration	239
4.39.2	Server Configuration.....	240
4.39.3	TACACS+ Server Configuration Buttons.....	240
4.40	Aggregation – Static.....	241
4.40.1	Aggregation Mode Configuration.....	241
4.40.2	Aggregation Group Configuration	242
4.40.3	Aggregation Configuration Buttons	242
4.41	Aggregation – LACP	243
4.41.1	LACP Port Configuration.....	243
4.41.2	LACP Port Configuration Buttons	244
4.42	Link OAM – Port	245
4.42.1	Link OAM Port Configuration	245
4.42.2	Link OAM Port Configuration Buttons	246
4.43	Link OAM – Event	247
4.43.1	Link Event Configuration.....	247
4.43.2	Link Event Configuration Buttons	248
4.44	Loop Protection (Configuration)	249
4.44.1	General Settings.....	249
4.44.2	Port Configuration	250
4.44.3	Loop Protection Configuration Buttons	250

4.45	Spanning Tree – Bridge Settings	251
4.45.1	STP Bridge Configuration – Basic Settings	251
4.45.2	STP Bridge Configuration – Advanced Settings	252
4.45.3	STP Bridge Configuration Buttons.....	253
4.46	Spanning Tree – MSTI Mapping	254
4.46.1	MSTI Configuration Identification.....	254
4.46.2	MSTI Mapping	254
4.46.3	MSTI Configuration Buttons.....	255
4.47	Spanning Tree – MSTI Priorities	256
4.47.1	STP MSTI Priority Configuration.....	256
4.47.2	STP MSTI Priority Buttons	256
4.48	Spanning Tree – Bridge CIST Ports.....	257
4.48.1	STP CIST Port Configuration	257
4.48.2	STP CIST Port Configuration Buttons	259
4.49	Spanning Tree – MSTI Ports	260
4.49.1	STP MSTI Port Configuration	261
4.49.2	STP MSTI Port Buttons	261
4.49.3	MSTI Port Configuration - Get	261
4.50	IPMC – Profile Table	262
4.50.1	IPMC Profile Configurations	262
4.50.2	IPMC Profile Buttons	263
4.51	IPMC – Address Entry	264
4.51.1	IPMC Profile Address Entry Table.....	264
4.51.2	IPMC Profile Buttons	265
4.52	MVR	266
4.52.1	MVR Configurations	266
4.52.2	MVR Buttons	269
4.53	IPMC – IGMP Snooping - Basic Configuration.....	270
4.53.1	IGMP Snooping Configuration.....	270
4.53.2	IGMP Buttons.....	271
4.54	IPMC – IGMP Snooping - VLAN Configuration	272
4.54.1	IGMP Snooping VLAN Configuration	272
4.54.2	IGMP Snooping VLAN Configuration Buttons	274
4.55	IPMC – IGMP Snooping - Port Filtering Profile.....	275
4.55.1	Port Filtering Profile Configuration.....	275
4.55.2	Port Filtering Profile Buttons	275
4.56	IPMC – MLD Snooping - Basic Configuration	277
4.56.1	MLD Snooping Configuration.....	277
4.56.2	MLD Buttons.....	278
4.57	IPMC – MLD Snooping - VLAN Configuration	279
4.57.1	MLD Snooping VLAN Configuration	279
4.57.2	MLD Snooping VLAN Configuration Buttons.....	281
4.58	IPMC – MLD Snooping - Port Filtering Profile.....	282
4.58.1	Port Filtering Profile Configuration.....	282
4.58.2	Port Filtering Profile Buttons	282

4.59	LLDP – LLDP Configuration	283
4.59.1	LLDP Parameters.....	283
4.59.2	LLDP Port Configuration	284
4.59.3	LLDP Configuration Buttons	286
4.60	LLDP – LLDP-MED	287
4.60.1	Fast start repeat count.....	287
4.60.2	Transmit TLVs	288
4.60.3	Coordinates Location.....	288
4.60.4	Civic Address Location.....	289
4.60.5	Emergency Call Service	291
4.60.6	Policies	291
4.60.7	Policies Interface Configuration	294
4.60.8	LLDP-MED Configuration Buttons	294
4.61	SyncE.....	295
4.61.1	Clock Source Nomination and State	295
4.61.2	Clock Selection Mode and State	297
4.61.3	Station Clock Configuration	298
4.61.4	SyncE Ports.....	298
4.61.5	SyncE Buttons	299
4.62	EPS.....	300
4.62.1	Ethernet Protection Switching	300
4.62.2	EPS Buttons	301
4.63	MEP	302
4.63.1	Maintenance Entity Point	302
4.63.2	MEP Buttons.....	303
4.64	ERPS	304
4.64.1	ERPS Configuration	304
4.64.2	ERPS Buttons.....	305
4.65	MAC Table – MAC Address Table Configuration	306
4.65.1	Aging Configuration	306
4.65.2	MAC Table Learning.....	307
4.65.3	Static MAC Table Configuration	307
4.65.4	MAC Configuration Buttons.....	308
4.66	VLANs –VLAN Configuration.....	309
4.66.1	Global VLAN Configuration.....	309
4.66.2	Port VLAN Configuration.....	309
4.66.3	Global VLAN Configuration Buttons	313
4.67	Private VLANs – Membership	314
4.67.1	Private VLAN Membership Configuration	314
4.67.2	Private VLAN Membership Configuration Buttons.....	315
4.68	Private VLANs – Port Isolation	316
4.68.1	Port Isolation Configuration	316
4.68.2	Port Isolation Configuration Buttons.....	316
4.69	VCL – Mac-Based VLAN.....	317
4.69.1	VCL Mac-Based VLAN Configuration.....	317

4.69.2	VCL Mac-Based VLAN Configuration Buttons	317
4.70	VCL – Protocol-Based VLAN – Protocol to Group Mapping.....	319
4.70.1	Protocol to Group Mapping Configuration	319
4.70.2	VCL Group Mapping Configuration Buttons.....	320
4.71	VCL – Protocol-Based VLAN – Group to VLAN.....	321
4.71.1	Group Name to VLAN Mapping Configuration	321
4.71.2	Group Name to VLAN Mapping Buttons.....	322
4.72	VCL – IP Subnet-based VLAN Membership	323
4.72.1	IP Subnet-based VLAN Membership Configuration	323
4.72.2	VCL IP Subnet-Based VLAN Configuration Buttons	324
4.73	Voice VLAN - Configuration.....	325
4.73.1	Voice VLAN Configuration	325
4.73.2	Voice VLAN Configuration Buttons.....	326
4.74	Voice VLAN - OUI	327
4.74.1	Voice VLAN OUI Configuration.....	327
4.74.2	Voice VLAN OUI Buttons	327
4.75	Ethernet Services - Ports.....	328
4.75.1	EVC Port Configuration	328
4.75.2	EVC Port Buttons.....	329
4.76	Ethernet Services – L2CP.....	330
4.76.1	L2CP Configuration	331
4.76.2	L2CP Buttons.....	331
4.77	Ethernet Services – Bandwidth Profiles	332
4.77.1	Bandwidth Profiles Configuration.....	332
4.77.2	Bandwidth Profile Buttons.....	333
4.78	Ethernet Services – EVC Control List	334
4.78.1	EVC Control List Configuration.....	334
4.78.2	Modification Buttons.....	335
4.78.3	Buttons	335
4.79	Ethernet Services – EVC Control Entries	336
4.79.1	Ingress Matching	337
4.79.2	Actions	337
4.79.3	Egress Outer Tag	338
4.79.4	Modification Buttons.....	338
4.79.5	Buttons	339
4.80	QoS – Port Classification	340
4.80.1	QoS Ingress Port Classification.....	340
4.80.2	QoS Ingress Port Classification Buttons	342
4.81	QoS – Port Policing.....	343
4.81.1	QoS Ingress Port Policers	343
4.81.2	QoS Ingress Port Policers Buttons	344
4.82	QoS – Queue Policing	345
4.82.1	Queue Port Policers	345
4.82.2	QoS Queue Policers Buttons	346
4.83	QoS – Port Scheduler	347

4.83.1	QoS Egress Port Schedulers and Shapers Page	348
4.83.2	QoS Egress Port Schedulers Buttons	350
4.84	QoS – Port Shaping	351
4.84.1	QoS Egress Port Shapers.....	351
4.85	QoS – Tag Remarking	352
4.85.1	QoS Tag Remarking	352
4.86	QoS – Port DSCP	353
4.86.1	QoS Tag Remarking	353
4.86.2	Port DSEP Buttons.....	354
4.87	QoS – DSCP Based QoS	355
4.87.1	QoS DSCP based QoS Ingress Classification	356
4.87.2	DSCP Based QoS Buttons	356
4.88	QoS – DSCP Translation.....	357
4.88.1	QoS DSCP Translation	358
4.88.2	DSCP Translation Buttons.....	358
4.89	QoS – DSCP Classification	359
4.89.1	QoS DSCP Classification	359
4.89.2	DSCP Buttons	359
4.90	QoS Control List	360
4.90.1	QoS Control List Configuration.....	360
4.90.2	QCE Configuration.....	363
4.90.3	QCE Configuration Buttons	368
4.91	QoS – Storm Control	369
4.91.1	Storm Control Configuration.....	369
4.91.2	Storm Control Configuration Buttons	370
4.92	Mirroring & Remote Mirroring	371
4.92.1	Mirror and Remote Mirroring Configuration.....	372
4.92.2	Source VLAN(s) Configuration	372
4.92.3	Remote Mirroring Port Configuration.....	373
4.92.4	Configuration Guideline for All Features	373
4.92.1	Mirror Configuration Buttons.....	374
4.93	UPnP	375
4.93.1	UPnP Configuration.....	375
4.93.2	UPnP Configuration Buttons	376
4.94	PTP	377
4.94.1	PTP External Clock Configuration.....	377
4.94.2	PTP Clock Configuration.....	378
4.94.3	PTP Configuration Buttons	379
4.95	GVRP – Global Configuration	380
4.95.1	GVRP Configuration.....	380
4.95.2	GVRP Configuration Buttons	380
4.96	GVRP – Port Configuration	381
4.96.1	GVRP Port Configuration.....	381
4.96.2	GVRP Port Configuration Buttons	381
4.97	sFLOW	382

4.97.1	Agent Configuration	382
4.97.2	Receiver Configuration.....	383
4.97.3	Port Configuration	383
4.97.4	sFLOW Buttons.....	384
4.98	UDLD	385
4.98.1	UDLD Port Configuration.....	385
4.98.2	UDLD Buttons.....	386
5	Web Interface – Monitor.....	387
5.1	System – Information.....	387
5.2	CPU Load	388
5.2.1	CPU Load Buttons	388
5.3	System – IP Status.....	389
5.3.1	IP Interfaces.....	389
5.3.2	IP Routes.....	389
5.3.3	Neighbour cache.....	390
5.3.4	IP Interface Buttons	390
5.4	System - Log.....	391
5.4.1	System Log Information Table	391
5.4.2	System Log Information Entry Columns	392
5.4.3	System Log Buttons.....	392
5.5	System – Detailed Log	393
5.5.1	Detailed System Log Information	393
5.5.2	System Log Information Buttons.....	393
5.6	Green Ethernet – Port Power Savings.....	394
5.6.1	Port Power Savings Status.....	394
5.6.2	Port Power Savings Status Buttons	395
5.7	Thermal Protection.....	396
5.7.1	Thermal Protection Port Status.....	396
5.7.2	Port Power Savings Status Buttons	396
5.8	Ports - State.....	397
5.8.1	Port State Overview	397
5.8.2	Port State Overview Buttons.....	397
5.9	Ports – Traffic Overview.....	398
5.9.1	Port Statistics Overview	398
5.9.2	Port Statistics Overview Buttons.....	399
5.10	Ports – QoS Statistics.....	400
5.10.1	Queuing Counters	400
5.10.2	Queuing Counters Buttons.....	400
5.11	Ports – QCL Status	401
5.11.1	QoS Control List Status.....	401
5.11.2	Queuing Counters Buttons.....	402
5.12	Ports – Detailed Statistics	403
5.12.1	Detailed Port Statistics	403
5.12.2	Detailed Port Statistics Buttons	405
5.13	Link OAM - Statistics.....	406

5.13.1	Detailed Link OAM Port Statistics	406
5.13.2	Detailed Link OAM Port Statistics Buttons	407
5.14	Link OAM – Port Status	408
5.14.1	Local and Peer.....	408
5.14.2	Link OAM Port Status Buttons	409
5.15	Link OAM – Event Status.....	410
5.15.1	Link OAM Link Event Status.....	410
5.15.2	Link OAM Event Status Buttons	412
5.16	DHCP – Server - Statistics	414
5.16.1	Database Counters	414
5.16.2	Binding Counters.....	414
5.16.3	DHCP Message Received Counters.....	414
5.16.4	DHCP Message Sent Counters	415
5.16.5	DHCP Server Buttons	415
5.17	DHCP – Server – Building IP	416
5.17.1	Binding IP Address	416
5.17.2	DHCP Building IP Buttons.....	417
5.18	DHCP – Server – Declined IP	418
5.18.1	Declined IP Addresses	418
5.18.2	Declined IP Buttons.....	418
5.19	DHCP – Snooping Table.....	419
5.19.1	Navigating the DHCP snooping Table.....	419
5.19.2	DHCP snooping Table Columns	419
5.19.3	Snooping Table Buttons.....	420
5.20	DHCP – Relay Statistics	421
5.20.1	Server Statistics	421
5.20.2	Client Statistics.....	421
5.20.3	Relay Statistics Buttons.....	422
5.21	DHCP – Detailed Statistics	423
5.21.1	Receive and Transmit Packets	423
5.21.2	Detailed Statistics Buttons	424
5.22	Security – Access Management	425
5.22.1	Access Management Statistics	425
5.22.2	Access Management Statistics Buttons.....	425
5.23	Security – Network – Port Security – Switch	426
5.23.1	Port Security-Switch Status.....	427
5.23.2	Access Management Statistics Buttons.....	428
5.24	Security – Network – Port Security – Port	429
5.24.1	Port Security Port Status Port n	429
5.24.2	Port Security Port Status Buttons	430
5.25	Security – Network – NAS – Switch	431
5.25.1	Network Access Server Switch Status	431
5.25.2	Network Access Server Switch Status Buttons.....	432
5.26	Security – Network – NAS – Port.....	433
5.26.1	NAS Statistics Port n	433

5.26.2	Port Counters	433
5.26.1	Selected Counters	435
5.26.2	Attached MAC Addresses.....	435
5.26.3	NAS Port Buttons	436
5.27	Security – Network – ACL Status.....	437
5.27.1	ACL Status.....	437
5.27.2	ACL Status Buttons	438
5.28	Security – ARP Inspection.....	439
5.28.1	Navigating the ARP Inspection Table	439
5.28.2	ARP Inspection Table Columns.....	439
5.28.3	ARP Inspection Table Buttons	440
5.29	Security – IP Source Guard	441
5.29.1	Navigating the IP Source Guard Table.....	441
5.29.2	IP Source Guard Table Columns	441
5.29.3	IP Source Guard Table Buttons.....	442
5.30	Security – AAA – RADIUS Overview	443
5.30.1	RADIUS Authentication Server Status Overview	443
5.30.2	RADIUS Authentication Server Status Buttons	444
5.31	Security – AAA – RADIUS Details.....	445
5.31.1	RADIUS Authentication Statistics for Server n.....	445
5.31.2	RADIUS Accounting Statistics.....	447
5.31.3	RADIUS Details Buttons.....	448
5.32	Security – Switch – RMON - Statistics	450
5.32.1	RMON Statistics Configuration.....	450
5.32.2	RMON Statistics Configuration Buttons	452
5.33	Security – Switch – RMON – History	453
5.33.1	RMON History Overview	453
5.33.2	RMON History Buttons	454
5.34	Security – Switch – RMON – Alarm	456
5.34.1	Alarm Overview	456
5.34.2	RMON Alarm Buttons	457
5.35	Security – Switch – RMON – Event	458
5.35.1	Event Overview	458
5.35.2	RMON Event Buttons	459
5.36	Aggregation – Static.....	460
5.36.1	Aggregation Group Status	460
5.36.2	Aggregation Status Buttons	460
5.37	Aggregation – LACP – System Status	461
5.37.1	LACP System Status.....	461
5.37.2	LACP System Status Buttons	461
5.38	LACP – Port Status.....	462
5.38.1	LACP Status	462
5.38.2	LACP Status Buttons.....	463
5.39	LACP – Port Statistics	464
5.39.1	LACP Statistics.....	464

5.39.2	LACP Statistics Buttons	464
5.40	Loop Protection	465
5.40.1	Loop Protection Status	465
5.40.2	LACP Status Buttons	465
5.41	Spanning Tree – Bridge Status	466
5.41.1	STP Detailed Bridge Status	466
5.41.2	STP Bridge Status Buttons	467
5.42	Spanning Tree – Port Status	468
5.42.1	STP Port Status	468
5.42.2	STP Port Status Buttons	468
5.43	Spanning Tree – Port Statistics	470
5.43.1	STP Statistics	470
5.43.2	STP Port Status Buttons	471
5.44	MVR - Statistics	472
5.44.1	MVR Statistics Table	472
5.44.2	MVR Statistics Buttons	472
5.45	MVR - Channels (Groups) Information	473
5.45.1	Navigating the MVR Channels (Groups) Information Table	473
5.45.2	MVR Channels (Groups) Information Table Columns	473
5.45.3	MVR Channels (Groups) Information Buttons	474
5.46	MVR - SFM Information	475
5.46.1	Navigating the MVR SFM Information Table	475
5.46.2	MVR SFM Information Table Columns	475
5.46.3	MVR SFM Information Buttons	476
5.47	IPMC – IGMP Snooping – Status	477
5.47.1	IGMP Snooping Status	477
5.47.2	STP Port Status Buttons	478
5.48	IPMC – IGMP Snooping – Groups Information	479
5.48.1	Navigating the IGMP Group Table	479
5.48.2	IGMP Snooping Groups Information	479
5.48.3	STP Port Status Buttons	480
5.49	IPMC – IGMP Snooping – IPV4 SFM Information	481
5.49.1	Navigating the SFM Information Table	481
5.49.2	IGMP SFM Information	482
5.49.3	IGMP SFM Information Buttons	482
5.50	IPMC – MLD Snooping – Status	483
5.50.1	MLD Snooping Status	483
5.50.2	MLD Status Buttons	484
5.51	IPMC – MLD Snooping – Groups Information	485
5.51.1	Navigating the MLD Group Table	485
5.51.2	MLD Group Table Columns	485
5.51.3	MLD Group Buttons	486
5.52	IPMC – MLD Snooping – IPV6 SFM Information	487
5.52.1	Navigating the MLD SFM Information Table	487
5.52.2	MLD SFM Information	487

5.52.3	MLD SFM Information Buttons.....	488
5.53	LLDP – Neighbors.....	489
5.53.1	LLDP Neighbor Information	489
5.53.2	LLDP Neighbor Information Buttons.....	490
5.54	LLDP – MED Neighbors.....	491
5.54.1	LLDP Media Neighbor Information	491
5.54.2	LLDP MED Neighbor Information Buttons.....	495
5.55	LLDP – EEE	496
5.55.1	LLDP Neighbors EEE Information.....	496
5.55.2	EEE Neighbor Information Buttons	497
5.56	LLDP – Port Statistics.....	499
5.56.1	LLDP Global Counters.....	499
5.56.2	LLDP Statistics Local Counters	500
5.56.3	LLDP Statistics Buttons	501
5.57	Ethernet Services – EVC Statistics	502
5.57.1	EVC Statistics	502
5.57.2	EVC Statistics Buttons.....	503
5.58	PTP	504
5.58.1	PTP External Clock Description	504
5.58.2	PTP Clock Description	505
5.58.3	PTP Buttons.....	505
5.59	MAC Table	506
5.59.1	Navigating the MAC Table	506
5.59.2	MAC Address Table.....	506
5.59.3	MAC Address Table Buttons	507
5.60	VLANs – Membership	508
5.60.1	Navigating the VLAN Membership Status Page	508
5.60.2	VLAN Membership for ___ user(s).....	509
5.60.3	VLAN Membership Status Buttons	509
5.61	VLANs – Ports	511
5.61.1	VLAN Port Status for ___ user(s)	511
5.61.2	VLAN Port Status Buttons	513
5.62	sFlow	514
5.62.1	Receiver Statistics	514
5.62.2	Port Statistics.....	515
5.62.3	sFlow Buttons.....	515
5.63	UDLD	516
5.63.1	UDLD port status	516
5.63.2	Neighbour Status.....	516
5.63.3	UDLD Buttons.....	517
6	Web Interface – Diagnostics	518
6.1	Ping.....	519
6.1.1	ICMP Ping	520
6.1.2	ICMP Ping Buttons.....	521
6.2	VeriPHY	522

6.2.1	VeriPHY Cable Diagnostics	522
6.2.2	Cable Status Table	523
6.2.3	VeriPHY Cable Diagnostics Buttons	523
7	Web Interface – Maintenance	524
7.1	Restart Device	525
7.1.1	Restart Device Buttons	525
7.2	Factory Defaults.....	526
7.2.1	Factory Defaults Buttons	526
7.3	Software – Upload.....	527
7.4	Software – Image Select	528
7.4.1	Software Image Selection	528
7.4.2	Software Image Selection Buttons	528
7.5	Configuration – Save Startup-Config	530
7.5.1	Save Running Configuration to Startup-Config.....	530
7.6	Configuration – Download	531
7.6.1	Download Configuration	531
7.7	Configuration – Upload.....	532
7.7.1	File to Upload.....	532
7.7.2	Destination File	532
7.8	Configuration – Activate	533
7.8.1	Activate Configuration	533
7.9	Configuration – Delete.....	534
7.9.1	Delete Configuration.....	534
8	Warranty	535
9	Accessories and Services.....	536

Document Title: CE Services – User Manual				
Description	Rev	Description of Change	ECO	Update Date
UM_001	1.00	Initial Version		11/02/2020

	Name	Signature	Date
Author	Meital Hadad		11/02/2020
Initiator	Ehud Palgi		21/04/2020
Approved	Ehud Palgi		21/04/2020

1 Overview

The CE Services upgraded products designed and produced by Techaya Inc., for use in harsh military environments.

The software delivers an enhanced feature set to support precision timing protocol (PTP) per IEEE 1588 V2, enhanced QoS, port control, Layer 2 features.

The upgrade supports PTP passthrough (per IEEE 1588 V2), which enables the switch to pass PTP packets through the switch as normal multicast traffic (forward mode) and facilitates synchronization of all switch ports with the master clock (end-to-end transparent mode). Added line protection features include support for 1+1, 1:1 and 1:N switching redundancy. Administrators can choose their network protection conditions. New L2 switching features include: VLAN translation and E-Line, E-LAN and E-TREE to enhance multipoint connectivity. For heightened QoS, the products now support service policing, H-QoS scheduling and per ASP and EVC queuing and scheduling.

This document is intended to provide the information required to interface with the Amphenol Socapex products which got the upgrade.

1.1 Indicators

Some of the 8MG CE Services products support “Dark Mode” operation, thus the LED indication is ON only when you press and hold the “STATUS” button. Those unit has one green LED on the front panel labeled PWR. This LED is illuminated when input power is applied to the unit.

Each of the LAN ports has single LED for Speed (10/100/1000) and Link / Activity.

Table 1 - LED Indicators

LED	Marking	Description
Speed	Port number	10 or 100 OFF
		1000 Green
Link/Activity	Port number	ON - Link is OK
		Flashing - Transmitting or Receiving Data
		OFF - No link and No Data

2 Command Line Interface

The Command Line Interface (CLI) is used for out-of-band control of the CE Services products. It provides the ability to customize configurations and status monitoring.

2.1 Command Line Overview

Some of the commands have optional parameters.

If a required parameter is missing the terminal will display the following message:

```
% Incomplete command
```

2.1.1 Context-Sensitive Help

To receive context-sensitive help directly from the command line:

Key	Help Description
?	Show next possible input and a description
Ctrl Q	Show syntax of possible commands
Tab	Show next possible input without a description or complete a word if it is unambiguous

2.1.2 Command Line Syntax

Each command is described by its syntax using the following delimiters:

- [...] square brackets indicate an optional construct
- { } curly brackets indicate a grouping
- "|" a straight line indicates a choice between two or more options

It is possible to have sequences of optional parameters. For example:

{ [a] [b] [c] }*1 the "*" indicates that at least one of the optional parameters must be present

[a] {[b]} [c] curly brackets in a sequence of optional parameters indicates one or more of the parameters has a fixed position

See the following examples:

Example 1:

Request help with the show access-list command (3 options):

Input (enter the command and then a question mark):

```
8MG# show access-list?
```

Output:

```
access-list    Access list
<cr>
```

Input (enter the command and then a question mark a second time):

8MG# show access-list?

Output:

```
show access-list [ interface [ ( <port_type> [ <v_port_type_list> ] )
] ] [ rate-limiter [ <rate_limiter_list> ] ] [ ace statistics [
<ace_list> ] ]
show access-list ace-status [ static ] [ link-oam ] [ loop-protect ] [
dhcp ] [ ptp ] [ upnp ] [ arp-inspection ] [ mep ] [ ipmc ] [ ip-
source-guard ] [ ip-mgmt ] [ conflicts ] [ switch <switch_list> ]
```

Input (enter the command a space and then a question mark):

8MG# show access-list ?

Output:

	Output modifiers
ace	Access list entry
ace-status	The local ACEs status
interface	Select an interface to configure
rate-limiter	Rate limiter
<cr>	

Example 2

Use the show command with no parameters:

Input:

8MG# show access-list

Since none of the optional parameters were used to limit the display, all entries in the access list are shown.

Output (partial view):

```
Switch access-list ace number: 0

Switch access-list rate limiter ID 1 is 1 pps
Switch access-list rate limiter ID 2 is 1 pps
Switch access-list rate limiter ID 3 is 1 pps
Switch access-list rate limiter ID 4 is 1 pps
Switch access-list rate limiter ID 5 is 1 pps
Switch access-list rate limiter ID 6 is 1 pps
Switch access-list rate limiter ID 7 is 1 pps
Switch access-list rate limiter ID 8 is 1 pps
Switch access-list rate limiter ID 9 is 1 pps
Switch access-list rate limiter ID 10 is 1 pps
Switch access-list rate limiter ID 11 is 1 pps
Switch access-list rate limiter ID 12 is 1 pps
Switch access-list rate limiter ID 13 is 1 pps
Switch access-list rate limiter ID 14 is 1 pps
Switch access-list rate limiter ID 15 is 1 pps
Switch access-list rate limiter ID 16 is 1 pps
.....
GigabitEthernet 1/2 :
-----
```

```
GigabitEthernet 1/2 access-list action is permit
GigabitEthernet 1/2 access-list policy ID is 0
GigabitEthernet 1/2 access-list rate limiter ID is disabled
GigabitEthernet 1/2 access-list redirect is disabled
GigabitEthernet 1/2 access-list mirror is disabled
GigabitEthernet 1/2 access-list logging is disabled
GigabitEthernet 1/2 access-list shutdown is disabled
GigabitEthernet 1/2 access-list port-state is enabled
GigabitEthernet 1/2 access-list counter is 0
```

Example 3

Use show access-list for port 6 on switch 1 only (1/6 only):

Input:

```
8MG# show access-list interface gigabitethernet 1/6
```

Output:

```
GigabitEthernet 1/6 :
-----
GigabitEthernet 1/6 access-list action is permit
GigabitEthernet 1/6 access-list policy ID is 0
GigabitEthernet 1/6 access-list rate limiter ID is disabled
GigabitEthernet 1/6 access-list redirect is disabled
GigabitEthernet 1/6 access-list mirror is disabled
GigabitEthernet 1/6 access-list logging is disabled
GigabitEthernet 1/6 access-list shutdown is disabled
GigabitEthernet 1/6 access-list port-state is enabled
GigabitEthernet 1/6 access-list counter is 0
```

2.1.3 Output Modifiers

It is possible to filter the output of display commands with output modifiers:

Modifier	Description
begin	begin with the line that matches
exclude	exclude lines that match
include	include lines that match
LINE	String to match output lines

The following example shows the proper syntax for an output modifier:

Input:

```
8MG# show access-list | include policy
```

Output:

```
GigabitEthernet 1/1 access-list policy ID is 0
GigabitEthernet 1/2 access-list policy ID is 0
GigabitEthernet 1/3 access-list policy ID is 0
GigabitEthernet 1/4 access-list policy ID is 0
GigabitEthernet 1/5 access-list policy ID is 0
```

```
GigabitEthernet 1/6 access-list policy ID is 0
GigabitEthernet 1/7 access-list policy ID is 0
GigabitEthernet 1/8 access-list policy ID is 0
```

2.1.4 Ethernet Interface Reference

In the CE Services product, the Ethernet interface (“port”) is referenced in the following manner:

* means all ports of all types on all switches

GigabitEthernet: defines the Ethernet type (1 Gigabit Ethernet Port), which requires a follow-up parameter (<port_type_list> in the sample below) that specifies the switch and the port number(s) on the switch (for example: 1/8 indicates port 8 on switch 1 or 3/1,3,5-7 indicates ports 1, 3, 5, 6, and 7 on switch 3)

Sample Syntax:

```
clear dot1x statistics [ interface ( <port_type> [ < port_type_list> ]
) ]
```

2.1.5 CLI Command Description

The following sections will describe each command as follows:

- List the individual command
- Give a brief description of the action triggered by the command
- Show the syntax of the command, and list the legal values and meanings of the parameters

2.2 Clear Commands

Use the clear commands to reset functions. The following functions can be reset (cleared):

Access	Access management.
Access-list	Access list.
Dot1x	IEEE Standard for port-based Network Access Control.
EPS	Ethernet Protection Switching.
ERPS	Ethernet Ring Protection Switching.
IP	Interface Internet Protocol config commands
Ipv6	IPv6 configuration commands.
LACP	Clear LACP statistics.
Link-OAM	Clear Link OAM statistics.
LLDP	Clears LLDP statistics.
Logging	Syslog
MAC	MAC Address Table

MEP	Maintenance Entity Point.
MVR	Multicast VLAN Registration configuration.
Network-clock	Clear active WTR timer.
sFlow	Statistics flow.
Spanning-Tree	STP Bridge.
Statistics	Clear statistics for one or more given interfaces.

2.2.1 Clear Access

Clear Access Management statistics.

Syntax:

```
clear access management statistics
```

2.2.2 Clear Access-List

Clear Access-List Entry (ACE) traffic statistics.

Syntax:

```
clear access-list ace statistics
```

2.2.3 Clear Dot1x

Clears the statistics counters for IEEE Standard for port-based Network Access Control.

Syntax:

```
clear dot1x statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

```
clear dot1x statistics
```

interface:

<port_type>: values are:

*

All switches or all ports

GigabitEthernet:

set specific Gigabit Ethernet Port number

<v_port_type_list> port list in 1/1-8

2.2.4 Clear EPS

The EPS instance number.

Syntax:

```
clear eps <uint> wtr
```

2.2.5 Clear ERPS

Syntax:

```
clear erps [ <groups> ] statistics
```

1~64: Zero or more ERPS group numbers

Statistics: Clear ERPS statistics

2.2.6 Clear EVC

Clear EVC statistic counters

Syntax:

```
clear evc statistics { [ <evc_id> | all ] } [ ece [ <ece_id> ] ] [
interface ( <port_type> [ <port_list> ] ) ] [ pw <pw_num_list> ]
```

interface:

*	All switches or All ports
	<port_type_list> Port list for all port types
GigabitEthernet	1 Gigabit Ethernet Port
	<port_type_list> Port list in 1/1-8

2.2.7 Clear IP

Interface Internet Protocol config commands.

IP ARP

Clear ARP cache.

Syntax:

```
clear ip arp
```

IP DHCP

Clear Dynamic Host Configuration Protocol.

Syntax:

```
clear ip dhcp detailed statistics { server | client | snooping | relay
| helper | all } [ interface ( <port_type> [ <in_port_list> ] ) ]
clear ip dhcp relay statistics
clear ip dhcp server binding <ip>
clear ip dhcp server binding type { automatic | manual | expired }
clear ip dhcp server statistics
clear ip dhcp snooping statistics [ interface ( <port_type> [
<in_port_list> ] ) ]
```

detailed: Detailed statistics

relay: DHCP relay agent configuration

server: Miscellaneous DHCP server information

snooping: DHCP snooping

server binding <ip> <ipv4_ucast> IP address of the binding

type Type of bindings to clear

snooping statistics interface:

*	All switches or All ports
	<port_type_list> Port list for all port types
GigabitEthernet	1 Gigabit Ethernet Port
	<port_type_list> Port list in 1/1-8

IP IGMP

Clear running IGMP snooping counters.

Syntax:

```
clear ip igmp snooping [ vlan <v_vlan_list> ] statistics
```

statistics: Running IGMP snooping counters

vlan: Search by VLAN

<vlan_list> VLAN identifier (VID)

IP Statistics

Clear IP statistic.

Syntax:

```
clear ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
```

[system]: IPv4 system traffic

[interface vlan <v_vlan_list>]:
VLAN identifier(s): VID)

[icmp]: IPv4 ICMP traffic

[icmp-msg <type>]:
IPv4 ICMP traffic for designated message type (<type> : 0~255)
ICMP message type ranges from 0 to 255)

Examples:

```
clear ip statistics
clear ip statistics icmp-msg 2
clear ip statistics interface vlan 2
clear ip statistics system
```

2.2.8 Clear IPV6

IPv6 configuration commands.

IPV6 MLD Snooping

Syntax:

```
clear ipv6 mld snooping [ vlan <v_vlan_list> ] statistics
```

statistics: Running MLD snooping counters

vlan: Search by VLAN

<vlan_list> VLAN identifier (VID)

IPV6 MLD Neighbors

Syntax:

```
clear ipv6 neighbors
```

IPV6 MLD Statistics

Syntax:

```
clear ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
```

icmp: IPv6 ICMP traffic

icmp-msg: IPv6 ICMP traffic for designated message type

interface: Select an interface to configure
 <vlan_list> VLAN identifier (VID)

system: IPv6 system traffic
 <type : 0~255> ICMP message type ranges from 0 to 255.

2.2.9 Clear LACP

Clear all LACP statistics.

Syntax:

```
clear lacp statistics
```

2.2.10 Clear Link-OAM

Clear Rx/Tx counters.

Syntax:

```
clear link-oam statistics [ interface ( <port_type> [ <plist> ] ) ]
```

interface: Clear Link OAM statistic on a specific interface or all interfaces.

* All switches or All ports
 <port_type_list> Port list for all port types

GigabitEthernet 1 Gigabit Ethernet Port
 <port_type_list> Port list in 1/1-8

2.2.11 Clear LLDP

Clears LLDP statistics.

Syntax:

```
clear lldp statistics { [ interface ( <port_type> [ <plist> ] ) ] | global }
```

2.2.12 Clear Logging

Clear System logs.

Syntax:

```
clear logging [ info ] [ warning ] [ error ] [ switch <switch_list> ]
```

logging options are: info
 notice
 warning
 error

2.2.13 Clear MAC

Clear the MAC Address Table.

Syntax:

```
clear mac address-table
```

2.2.14 Clear Mep

The MEP instance.

Syntax:

```
clear mep < uint >
```

2.2.15 Clear MVR

Multicast VLAN Registration configuration.

Name: MVR multicast name

Statistics: Running MVR protocol counters

Vlan: MVR multicast VLAN

Syntax:

```
clear mvr [ vlan <v_vlan_list> | name <mvr_name> ] statistics
statistics, name: Running MVR protocol counters.
```

2.2.16 Clear Network-clock

Clear active WTR timer.

Syntax:

```
clear network-clock clk-source <clk_list>
```

<1~2>: Clock source number.

2.2.17 Clear sFLOW

Clear sFlow statistics.

Syntax:

```
clear sflow statistics { receiver [ <receiver_index_list> ] | samplers
[ interface [ <samplers_list> ] ( <port_type> [ <v_port_type_list> ] )
] }
```

interface: Clear statistics for a specific interface or interfaces.

2.2.18 Clear Spanning-Tree

Clear the STP Bridge. It is possible to clear the whole bridge or a specific interface.
(detected-protocols – Set the STP migration check)

Syntax:

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


2.2.19 Clear Statistics

Clear the statistics for one or more interfaces.

Syntax:

```
clear statistics [ interface ] ( <port_type> [ <v_port_type_list> ] )
```

interface:

<port_type>, values are:

*	All switches or All ports
<port_type_list>	Port list for all port types
GigabitEthernet	1 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-8

Example:

```
clear statistics interface gigabitethernet 1/8
```

2.3 Configuration Commands

The CLI – Configuration section of this manual describes how to configure the CE Services Ethernet Switch, using the switch Command Line interface. Many parameters may be configured from the Web User interface described later in this manual (3 Web Interface – Introduction on page 126128).

Input:

```
M# config terminal
```

Output (prompt changes):

```
8MG(config)#
```

2.3.1 AAA

Set the Authentication, Authorization, and Accounting parameters for the authentication login.

Syntax:

```
aaa accounting { console | telnet | ssh } tacacs { [ commands
<priv_lvl> ] [ exec ] }*1
aaa authentication login { console | telnet | ssh | http } { { local |
radius | tacacs } [ { local | radius | tacacs } [ { local | radius |
tacacs } ] ] }
aaa authorization { console | telnet | ssh } tacacs commands
<priv_lvl> [ config-commands ]
```

console:	Configure Console
ssh:	Configure SSH command accounting
telnet:	Configure Telnet command accounting

2.3.2 Access

Set the Access Management configuration.

```
access management <access_id> <access_vid> <start_addr> [ to
<end_addr> ] { [ web ] [ snmp ] [ telnet ] | all }
```

<access_id>: ID of access management entry, values are 1-16

<access_vid>: The VLAN ID for the access management entry,
values are 1-4095.

<start_addr>: Start IPv4 address

<end_addr>: End IPv4 address

2.3.3 Access-List ACE

Configure the ACL Ports parameters (Access Control Entry - ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

Syntax:

```
access-list ace [ update ] <ace_id> [ next { <ace_id_next> | last } ]
[ ingress { switch <ingress_switch_id> | switchport {
<ingress_switch_port_id> | <ingress_switch_port_list> } | interface {
<port_type> <ingress_port_id> | ( <port_type> [ <ingress_port_list> ]
) } | any } ] [ policy <policy> [ policy-bitmask <policy_bitmask> ] ]
[ tag { tagged | untagged | any } ] [ vid { <vid> | any } ] [ tag-
priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any }
] [ dmac-type { unicast | multicast | broadcast | any } ] [ frame-type
{ any | etype [ etype-value { <etype_value> | any } ] [ smac {
<etype_smac> | any } ] [ dmac { <etype_dmac> | any } ] | arp [ sip {
<arp_sip> | any } ] [ dip { <arp_dip> | any } ] [ smac { <arp_smac> |
any } ] [ arp-opcode { arp | rarp | other | any } ] [ arp-flag [ arp-
request { <arp_flag_request> | any } ] [ arp-smac { <arp_flag_smac> |
any } ] [ arp-tmac { <arp_flag_tmac> | any } ] [ arp-len {
<arp_flag_len> | any } ] [ arp-ip { <arp_flag_ip> | any } ] [ arp-
ether { <arp_flag_ether> | any } ] ] | ipv4 [ sip { <sipv4> | any } ]
[ dip { <dipv4> | any } ] [ ip-protocol { <ipv4_protocol> | any } ] [
ip-flag [ ip-ttl { <ip_flag_ttl> | any } ] [ ip-options {
<ip_flag_options> | any } ] [ ip-fragment { <ip_flag_fragment> | any }
] ] | ipv4-icmp [ sip { <sipv4_icmp> | any } ] [ dip { <dipv4_icmp> |
any } ] [ icmp-type { <icmpv4_type> | any } ] [ icmp-code {
<icmpv4_code> | any } ] [ ip-flag [ ip-ttl { <ip_flag_icmp_ttl> | any
} ] [ ip-options { <ip_flag_icmp_options> | any } ] [ ip-fragment {
<ip_flag_icmp_fragment> | any } ] ] | ipv4-udp [ sip { <sipv4_udp> |
any } ] [ dip { <dipv4_udp> | any } ] [ sport { <sportv4_udp_start> [
to <sportv4_udp_end> ] | any } ] [ dport { <dportv4_udp_start> [ to
<dportv4_udp_end> ] | any } ] [ ip-flag [ ip-ttl { <ip_flag_udp_ttl> |
any } ] [ ip-options { <ip_flag_udp_options> | any } ] [ ip-fragment {
<ip_flag_udp_fragment> | any } ] ] | ipv4-tcp [ sip { <sipv4_tcp> |
any } ] [ dip { <dipv4_tcp> | any } ] [ sport { <sportv4_tcp_start> [
to <sportv4_tcp_end> ] | any } ] [ dport { <dportv4_tcp_start> [ to
<dportv4_tcp_end> ] | any } ] [ ip-flag [ ip-ttl { <ip_flag_tcp_ttl> |
any } ] [ ip-options { <ip_flag_tcp_options> | any } ] [ ip-fragment {
<ip_flag_tcp_fragment> | any } ] ] [ tcp-flag [ tcp-fin {
<tcpv4_flag_fin> | any } ] [ tcp-syn { <tcpv4_flag_syn> | any } ] [
tcp-rst { <tcpv4_flag_rst> | any } ] [ tcp-psh { <tcpv4_flag_psh> |
any } ] [ tcp-ack { <tcpv4_flag_ack> | any } ] [ tcp-urg {
<tcpv4_flag_urg> | any } ] ] | ipv6 [ next-header { <next_header> |
```

```

any } ] [ sip { <sipv6> [ sip-bitmask <sipv6_bitmask> ] | any } ] [
hop-limit { <hop_limit> | any } ] | ipv6-icmp [ sip { <sipv6_icmp> [
sip-bitmask <sipv6_bitmask_icmp> ] | any } ] [ icmp-type {
<icmpv6_type> | any } ] [ icmp-code { <icmpv6_code> | any } ] [ hop-
limit { <hop_limit_icmp> | any } ] | ipv6-udp [ sip { <sipv6_udp> [
sip-bitmask <sipv6_bitmask_udp> ] | any } ] [ sport {
<sportv6_udp_start> [ to <sportv6_udp_end> ] | any } ] [ dport {
<dportv6_udp_start> [ to <dportv6_udp_end> ] | any } ] [ hop-limit {
<hop_limit_udp> | any } ] | ipv6-tcp [ sip { <sipv6_tcp> [ sip-bitmask
<sipv6_bitmask_tcp> ] | any } ] [ sport { <sportv6_tcp_start> [ to
<sportv6_tcp_end> ] | any } ] [ dport { <dportv6_tcp_start> [ to
<dportv6_tcp_end> ] | any } ] [ hop-limit { <hop_limit_tcp> | any } ]
[ tcp-flag [ tcp-fin { <tcpv6_flag_fin> | any } ] [ tcp-syn {
<tcpv6_flag_syn> | any } ] [ tcp-rst { <tcpv6_flag_rst> | any } ] [
tcp-psh { <tcpv6_flag_psh> | any } ] [ tcp-ack { <tcpv6_flag_ack> |
any } ] [ tcp-urg { <tcpv6_flag_urg> | any } ] ] [ action { permit
| deny | filter { switchport <filter_switch_port_list> | interface (
<port_type> [ <filter_port_list> ] ) } } ] [ rate-limiter {
<rate_limiter_id> | disable } ] [ evc-policer { <evc_policer_id> |
disable } ] [ mirror [ disable ] ] [ logging [ disable ] ] [ shutdown
[ disable ] ] [ lookup-second [ disable ] ] [ redirect { switchport {
<redirect_switch_port_id> | <redirect_switch_port_list> } | interface
{ <port_type> <redirect_port_id> | ( <port_type> [
<redirect_port_list> ] ) } | disable } ]

```

<1-256>: ACE ID

update: Update an existing ACE

2.3.3.1 Access-List ACE Action

Configure the ACE action to be taken.

Example:

Input:

```
8MG (config)# access-list ace 1 action deny
```

<ace_id>: ID of ace entry, value can be 1-256

action values: deny
filter
permit

2.3.3.2 Access-List ACE Dmac-Type

Set the type of destination MAC address for the ACL.

Syntax:

```
access-list ace <ace_id> dmac-type < any | broadcast | multicast |  
uniicast >
```

<ace_id>: ID of ace entry, value can be 1-256

dmac-type:

any: Don't-care the type of destination MAC address

broadcast: Broadcast destination MAC address

multicast: Multicast destination MAC address

unicast: Unicast destination MAC address)

2.3.3.3 Access-List ACE Frame-type

Set the frame type for the ACL.

Syntax:

```
access-list ace <ace_id> frametype < any | arp | etype | ipv4 | ipv4-  
icmp | ipv4-tcp | ipv4-udp | ipv6 | ipv6-icmp | ipv6-tcp | ipv6-udp >
```

<ace_id>: ID of ace entry, value can be 1-256

frametype:

any: Don't-care the frame type

arp: Frame type of ARP

etype: Frame type of etype

ipv4: Frame type of IPv4

ipv4-icmp: Frame type of IPv4 ICMP

ipv4-tcp: Frame type of IPv4 TCP

ipv4-udp: Frame type of IPv4 TCP

ipv6: Frame type of IPv6

ipv6-icmp: Frame type of IPv6 ICMP

ipv6-tcp: Frame type of IPv6 TCP

ipv6-udp: Frame type of IPv6 UDP

2.3.3.4 Access-List ACE Ingress

Set the ingress configuration for the ACL.

Syntax:

```
access-list ace <ace_id> ingress
{ any | interface { * | gigabitethernet <port-list> } }
```

<ace_id>: ID of ace entry, value can be 1-256

ingress options:

any: do not care which ingress interface

interface:

<port_type>, values are:

* All switches or all ports

GigabitEthernet: set specific Gigabit Ethernet Port number

<port-list> port list in 1/1-8

2.3.3.5 Access-List ACE Logging

Set the ACL logging configuration.

Syntax:

```
access-list ace <ace_id> logging
```

<ace_id>: ID of ace entry, value can be 1-256

Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

2.3.3.6 Access-List ACE Mirror

Mirror frame to destination mirror port according to the ACL.

Syntax:

```
access-list ace <ace_id> mirror
```

<ace_id>: ID of ace entry, value can be 1-256

2.3.3.7 Access-List ACE Next

Insert the current ACE before the next ACE ID, values are:

Syntax:

```
access-list ace <ace_id> next { <ace_id_next> | last }
```

<ace_id>: ID of ace entry, value can be 1-256

<ace_id_next>: the next ID, values can be: 1-256

last: place the current ACE to the end of access list

2.3.3.8 Access-List ACE Policy

Set the ACE Policy ID.

Syntax:

```
access-list ace <ace_id> policy <policy_id>
```

<ace_id>: ID of ace entry, value can be 1-256

<policy_id>: value can be 0-255

2.3.3.9 Access-List ACE Rate Limiter

Set the rate limiter ID or disable rate limiter for specific ACL.

Syntax:

```
access-list ace <ace_id> rate-liimiter {<rate_limiter_id> | disable}
```

<ace_id>: ID of ace entry, value can be 1-256

<rate_limiter_id>: rate limiter ID (values are: 1-16)

Disable: disable rate-limiter

2.3.3.10 Access-List ACE Redirect

Redirect frame to specific port according to ACL.

Syntax:

```
access-list ace <ace_id> redirect
{ disable | interface {* | gigabitethernet <port-list>} }
```

<ace_id>: ID of ace entry, value can be 1-256

redirect options:

disable: disable redirect

interface: select an interface to configure

<port_type>, values are:

* All switches or all ports

GigabitEthernet: set specific Gigabit Ethernet Port number

<port-list> port list in 1/1-8

2.3.3.11 Access-List ACE Shutdown

Shutdown incoming traffic according to specific ACL. The shutdown feature only works when the packet length is less than 1,518 (without VLAN tags).

Syntax:

```
access-list ace <ace_id> shutdown
```

<ace_id>: ID of ace entry, value can be 1-256

2.3.3.12 Access-List ACE Tag

Set an ACE according to packet's Tag status.

Syntax:

```
access-list ace <ace_id> tag <any | tagged | untagged>
```

<ace_id>: ID of ace entry, value can be 1-256

any: don't-care tagged or untagged

tagged: tagged

untagged: untagged

2.3.3.13 Access-List ACE Tag-Priority

Set the ACE according to packet's tag priority.

Syntax:

```
access-list ace <ace_id> tag-priority <tag_priority_value >
```

<ace_id>: ID of ace entry, value can be 1-256

<tag_priority_value>:

0-1: the range of tag priority

0-3: the range of tag priority

2-3: the range of tag priority

4-5: the range of tag priority

4-7: the range of tag priority

6-7: the range of tag priority

0-7: the value of tag priority,
value may be any single number from 1 thru 7

any: don't care the value of tag priority field

2.3.3.14 Access-List ACE VID

Set the ACE according to packet's VLAN ID.

Syntax:

```
access-list ace <ace_id> vid {<vid> | any}
```

<vid>: the value(s) of VID field, values are: 1-4095

any: do not-care the value of VID field

2.3.4 Access-List Rate-Limiter

Set the Access (Control) List Rate Limiter.

Syntax:

```
access-list rate-limiter [ <rate_limiter_list> ] { pps <pps_rate> |
100pps <pps100_rate> | kpps <kpps_rate> | 100kbps <kpbs100_rate> }
```

[<rate_limiter_list>]: rate limiter id, values are 1-16

pps: packets per second

kpps: thousands of packets per second

100kbps: 100k bits per second

2.3.5 Aggregation

Set Link Aggregation (LAG) parameters.

Syntax:

```
aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }
```

mode: Traffic distribution mode

smac: source MAC affects the distribution

dmac: destination MAC affects the distribution

ip: IP address affects the distribution

port: IP port affects the distribution

2.3.6 Banner

Define a log in banner. There are three types of banners:

exec: set EXEC process creation banner

login: set login banner

motd: set Message of the Day banner

Syntax:

```
banner [ motd ] <banner>
```

```
banner exec <banner>
```

```
banner login <banner>
```

The banner text is delimited by a user defined character:

c banner-text c, where 'c' is a delimiting character and "banner-text" is the banner.

Example:

Input:

```
8MG(config)# banner x This is the banner. x<CR>
(the delimiter is "x")
```

2.3.7 Clock

Configure time-of-day clock.

Options:

summer-time : Configure summer (daylight savings) time.

Timezone: Configure time zone.

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> ] ]
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> ] ]
clock timezone <word_var> <hour_var> [ <minute_var> [ <subtype_var> ]
]
```

<word16> name of time zone in summer, timezone.

2.3.8 Default

Set a command to its defaults.

Default options:

```
access-list:      Access list
snmp-server:      SNMP (Simple Network Management Protocol)
```

Syntax:

```
default access-list rate-limiter [ <rate_limiter_list> ]
default snmp-server community v2c { ro | rw }
```

<1~16> Rate limiter ID

2.3.9 Do

To run exec commands in config mode (while working in a sub-menu)

Syntax:

```
do <command>
```

2.3.10 Dot1x

IEEE Standard protocol for port-based Network Access Control

8MG (config) # dot1x ?

dot1x authentication timer

Time in seconds between check for activity on successfully authenticated MAC addresses.

Syntax:

```
dot1x authentication timer inactivity <v_10_to_100000>
dot1x authentication timer re-authenticate <v_1_to_3600>
```

```
inactivity:      Time in seconds between check for activity on
                  successfully authenticated MAC addresses.
                  <10-1000000> seconds.
```

```
re-authenticate: The period between re-authentication attempts in seconds.
                  <1-3600> seconds.
```

dot1x feature

Globally enables/disables a dot1x feature functionality.

Syntax:

```
dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] } *1
```

guest-vlan: Globally enables/disables state of guest-vlan

radius-qos: Globally enables/disables state of RADIUS-assigned QoS.

radius-vlan: Globally enables/disables state of RADIUS-assigned VLAN.

dot1x system-auth-control

Set the global dot1x state.

Syntax:

```
dot1x system-auth-control
```

dot1x timeout quiet-period

Time in seconds before a MAC-address that failed authentication gets a new authentication chance.

Syntax:

```
dot1x timeout quiet-period <v_10_to_1000000>
```

<v_10_to_1000000>: value can be 10-1,000,000 seconds

dot1x timeout tx-period

The time between EAPOL retransmissions.

Syntax:

```
dot1x timeout tx-period <v_1_to_65535>
```

<v_1_to_65535>: value can be 1-65,535 seconds

2.3.11 Enable

Modify enable password parameters.

Enable Password

Assign the privileged level clear password.

Syntax:

```
enable password [ level <priv> ] <password>
```

<word32>: The UNENCRYPTED (clear-text) password

Level: Set exec level password

Enable Secret

Assign the privileged level password encryption.

Syntax:

```
enable secret { 0 | 5 } [ level <priv> ] <password>
```

0: Specifies an UNENCRYPTED password will follow

5: Specifies an ENCRYPTED secret will follow

[level <priv>]: Set exec level password. Level number values can be from 1-15

<password>: Password

Example:

Input:

```
8MG(config)# enable secret 0 level 1 miltech918pswr
```

2.3.12 End

Go back to EXEC mode.

Syntax:

```
end
```

2.3.13 EPS

Ethernet Protection Switching.

Syntax:

```
eps <inst> 1plus1 { bidirectional | { unidirectional [ aps ] } }
eps <inst> command { lockout | forced | manualp | manualw | exercise |
freeze | lockoutlocal }
eps <inst> domain { port | tunnel-tp | pw } architecture { 1plus1 |
1for1 } work-flow { <flow_w> | <port_type> <port_w> } protect-flow {
<flow_p> | <port_type> <port_p> }
eps <inst> holdoff <hold>
eps <inst> mep-work <mep_w> mep-protect <mep_p> mep-aps <mep_aps>
eps <inst> revertive { 10s | 30s | 5m | 6m | 7m | 8m | 9m | 10m | 11m |
12m | { wtr-value <wtr_value> } }
```

<1-100>: The EPS instance number.

EPS 1plus1

EPS 1+1 architecture.

Syntax:

```
eps <inst> 1plus1 { bidirectional | { unidirectional [ aps ] } }
```

bidirectional: EPS 1+1 bidirectional protection type.

Unidirectional: EPS 1+1 unidirectional protection type.

EPS command

EPS command.

Syntax:

```
eps <inst> command { lockout | forced | manualp | manualw | exercise |
freeze | lockoutlocal }
```

exercise: Exercise of the protocol - not traffic effecting. This is only allowed in case of 'Bidirectional' protection type

forced:	Force switch normal traffic to protection.
Freeze:	Local Freeze of EPS.
Lockout:	Lockout of protection.
Lockoutlocal:	Local lockout of EPS.
Manual:	Manual switch normal traffic to protection.
Manual:	Manual switch normal traffic to working. This is only allowed in case of 'non-revertive' mode.

EPS domain

The domain of the EPS.

Syntax:

```
eps <inst> domain { port | tunnel-tp | pw } architecture { 1plus1 | 1for1 } work-flow { <flow_w> | <port_type> <port_w> } protect-flow { <flow_p> | <port_type> <port_p> }
```

port: This EPS is protecting in the Port domain.

pw: This EPS is protecting in the MPLS-TP Pseudo-Wire domain.

tunnel-tp: This EPS is protecting in the MPLS-TP tunnel domain.

EPS holdoff

Hold off timer.

Syntax:

```
eps <inst> holdoff <hold>
```

<uint>: The hold off timer value in 100 ms. Max 10 sec.

EPS mep-work

Working MEP instance.

Syntax:

```
eps <inst> mep-work <mep_w> mep-protect <mep_p> mep-aps <mep_aps>
```

<uint>: Working MEP instance number.

EPS revertive

Revertive EPS.

Syntax:

```
eps <inst> revertive { 10s | 30s | 5m | 6m | 7m | 8m | 9m | 10m | 11m | 12m | { wtr-value <wtr_value> } }
```

10m WTR is 10 min.

10s WTR is 10 sec.

11m WTR is 11 min.

12m WTR is 12 min.

30s WTR is 30 sec.

5m WTR is 5 min.

6m WTR is 6 min.

7m	WTR is 7 min.
8m	WTR is 8 min.
9m	WTR is 9 min.
wtr-value	WTR as value.

2.3.14 ERPS

Ethernet Ring Protection Switching.

Syntax:

```
erps <group> guard <guard_time_ms>
erps <group> holdoff <holdoff_time_ms>
erps <group> major port0 interface <port_type> <port0> port1 interface
<port_type> <port1> [ interconnect ]
erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps
<p1_aps>
erps <group> revertive <wtr_time_minutes>
erps <group> rpl { owner | neighbor } { port0 | port1 }
erps <group> sub port0 interface <port_type> <port0> { { port1
interface <port_type> <port1> } | { interconnect <major_ring_id> } } [
virtual-channel ]
erps <group> topology-change propagate
erps <group> version { 1 | 2 }
erps <group> vlan { none | [ add | remove ] <vlans> }
```

1-64: ERPS group number.

ERPS guard

Syntax:

```
erps <group> guard <guard_time_ms>
```

10-2000: Guard time in ms.

ERPS holdoff

Syntax:

```
erps <group> holdoff <holdoff_time_ms>
```

0-10000: Hold-off time in ms.

ERPS major port0

Syntax:

```
erps <group> major port0 interface <port_type> <port0> port1 interface
<port_type> <port1> [ interconnect ]
```

interface:

GigabitEthernet: 1 Gigabit Ethernet Port

<port_type_id> Port ID in 1/1-8

ERPS mep port0 sf

Syntax:

```
erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps
<p1_aps>
```

1-100: Index of Port 0 SignalFail MEP.

ERPS revertive

Syntax:

```
erps <group> revertive <wtr_time_minutes>
```

1-12: Wait-to-restore time in minutes

ERPS rpl

Syntax:

```
erps <group> rpl { owner | neighbor } { port0 | port1 }
```

neighbor: Neighbor role

owner: Owner role

port0: ERPS Port 0 interface

port1: ERPS Port 1 interface

ERPS sub port0

Syntax:

```
erps <group> sub port0 interface <port_type> <port0> { { port1  
interface <port_type> <port1> } | { interconnect <major_ring_id> } } [  
virtual-channel ]
```

interface:

GigabitEthernet: 1 Gigabit Ethernet Port

ERPS topology-change propagate

Syntax:

```
erps <group> topology-change propagate
```

ERPS version

Syntax:

```
erps <group> version { 1 | 2 }
```

1: ERPS version 1

2: ERPS version 2

ERPS vlan

Syntax:

```
erps <group> vlan { none | [ add | remove ] <vlans> }
```

<vlan_list> List of VLANs

Add: Add to set of included VLANs

None: Do not include any VLANs

Remove: Remove from set of included VLANs

2.3.15 EVC

Ethernet Virtual Connections.

Syntax:

```

evc [ update ] <evc_id> [ name <evc_name> ] { [ vid <evc_vid> ] } [
  ivid <ivid> ] [ interface ( <port_type> [ <port_list> ] ) ] { [ leaf {
    [ vid <leaf_vid> ] [ ivid <leaf_ivid> ] [ interface { ( <port_type> [
      <leaf_port_list> ] ) | none } ] }*1 ] [ learning [ disable ] ] [
    policer { <policer_id> | none | discard } ] [ inner-tag add { [ type {
      none | c-tag | s-tag | s-custom-tag } ] [ vid-mode { normal | tunnel }
    ] [ vid <it_add_vid> ] [ preserve [ disable ] ] [ pcp <it_add_pcp> ] [
      dei <it_add_dei> ] }*1 ] [ outer-tag add vid <ot_add_vid> ] [ pw [
        <pw_num_list> ] [ split-horizon <pw_num_list_split_horizon> ] ] }
evc ece [ update ] <ece_id> [ next { <ece_id_next> | last } ] [ lookup
  { basic | advanced } ] [ interface ( <port_type> [ <port_list> ] ) ] [
  smac { <smac> | any } ] [ dmac { <dmac> | unicast | multicast |
  broadcast | any } ] [ outer-tag { [ match { [ type { untagged | tagged
    | c-tagged | s-tagged | any } ] [ vid { <ot_match_vid> | any } ] [ pcp
    { <ot_match_pcp> | any } ] [ dei { <ot_match_dei> | any } ] }*1 ] [
    add { [ mode { enable | disable } ] [ vid <ot_add_vid> ] [ preserve [
      disable ] ] [ pcp-mode { classified | fixed | mapped } ] [ pcp
      <ot_add_pcp> ] [ dei-mode { classified | fixed | dp } ] [ dei
      <ot_add_dei> ] }*1 ] }*1 ] [ inner-tag { [ match { [ type { untagged |
      tagged | c-tagged | s-tagged | any } ] [ vid { <it_match_vid> | any }
    ] [ pcp { <it_match_pcp> | any } ] [ dei { <it_match_dei> | any } ]
    }*1 ] [ add { [ type { none | c-tag | s-tag | s-custom-tag } ] [ vid
      <it_add_vid> ] [ preserve [ disable ] ] [ pcp-mode { classified |
      fixed | mapped } ] [ pcp <it_add_pcp> ] [ dei-mode { classified |
      fixed | dp } ] [ dei <it_add_dei> ] }*1 ] }*1 ] [ frame-type { any | {
    ipv4 [ proto { <pr4> | udp | tcp | any } ] [ dscp { <dscp4> | any } ]
    [ sip { <sip4> | any } ] [ dip { <dip4> | any } ] [ fragment { yes |
    no | any } ] [ sport { <sp4> | any } ] [ dport { <dp4> | any } ] } | {
    ipv6 [ proto { <pr6> | udp | tcp | any } ] [ dscp { <dscp6> | any } ]
    [ sip { <sip6> | any } ] [ dip { <dip6> | any } ] [ sport { <sp6> |
    any } ] [ dport { <dp6> | any } ] } } | { etype [ etype-value {
      <etype_value> | any } ] [ etype-data { <etype_data> | any } ] [
      <etype_mask> ] } } | { llc [ dsap { <dsap> | any } ] [ ssap { <ssap> |
      any } ] [ control { <control> | any } ] [ llc-data { <llc_data> | any
    } [ <llc_mask> ] } } | { snap [ oui { <oui> | any } ] [ pid { <pid> |
    any } ] } } | { l2cp { stp | pause | lacp | lamp | loam | dot1x | elmi |
    pb | pb-gvrp | lldp | gmrp | gvrp | uld | pagp | pvst | cisco-vlan |
    cdp | vtp | dtp | cisco-stp | cisco-cfm } } } ] [ direction { both |
    uni-to-nni | nni-to-uni } ] [ rule-type { both | rx | tx } ] [ tx-
    lookup { vid | pcp-vid | isdx } ] [ l2cp { [ mode { tunnel | peer |
    forward | discard } ] [ tmac { cisco | custom } ] }*1 ] [ evc {
    <evc_id> | none } ] [ policer { <policer_id> | none | discard | evc }
  ] [ pop <pop> ] [ policy <policy_no> ] [ cos { <cos> | disable } ] [
  dpl { <dpl> | disable } ]

```

<1-256>: EVC identifier.
 Ece: EVC Control Entry
 Policer: Policer (ingress bandwidth profile)
 Update: Update existing entry

2.3.16 Exit

Exit from current mode.

Syntax:

```
exit
```

2.3.17 Firmware

Zeroization.

Syntax:

```
firmware zeroization { enable | disable }
```

disable: disable system zeroization

enable: enable system zeroization (volatile memory erase)

2.3.18 Green-Ethernet

Green Ethernet, reduces power consumption. The following Green Ethernet options are available:

eee: Energy Efficient Ethernet, power down of PHYs when there is no traffic

led: LED power reduction, reduce LED intensity

green-ethernet eee optimize-for-power

Set if EEE shall be optimized for least power consumption (else optimized for least traffic latency).

Syntax:

```
green-ethernet eee optimize-for-power
```

green-ethernet led interval

Set the interval in whole hours at which to configure the LED intensity.

Syntax:

```
green-ethernet led interval <v_0_to_24> intensity <v_0_to_100>
```

<v_0_to_24>: interval from 00.00 to 24.00 hours

(00 is used to start at midnight,

24 is used to stop at midnight).

<v_0_to_100>: LED intensity from 0 to 100

green-ethernet led on-event

Specifies when to turn LEDs on at 100% intensity.

Syntax:

```
green-ethernet led on-event { [ link-change <v_0_to_65535> ]  
[ error ] }*1
```

link-change: specifies how long to turn LEDs intensity to 100%,
when a link changes state

<v_0_to_65535>: number of seconds to set LEDs intensity to 100%
at link change, values 0 to 65,535

[error]: set LEDs intensity to 100% if an error occurs

2.3.19 GVRP

Enable GVRP feature.

Syntax:

```
gvrp max-vlans <maxvlans>
```

```
gvrp time { [ join-time <jointime> ] [ leave-time <leavetime> ] [  
leave-all-time <leavealltime> ] }*1
```


max-vlans

Number of simultaneous VLANs that GVRP can control <1-4095>

Time

Configure GARP protocol timer parameters. IEEE 802.1D-2004, clause 12.11.

join-time: Set GARP protocol parameter JoinTime.
 leave-all-time: Set GARP protocol parameter LeaveAllTime.
 leave-time: Set GARP protocol parameter LeaveTime.

2.3.20 Help

Description of the interactive help system

Syntax:

help

2.3.21 Hostname

Set system's network name.

Syntax:

hostname <hostname>

2.3.22 Interface - Port Type

Select an interface to configure.

Syntax:

interface (<port_type> [<plist>])

interface:

<plist>: port list in 1/1-8
 <port_type>: values are:
 * All switches or all ports
 GigabitEthernet: set specific Gigabit Ethernet Port number
 vlan: VLAN interface configurations

Input:

```
8MG(config)# interface *
```

Or Input:

```
8MG(config)# interface gigabitethernet 1/8
```

Output (prompt change to interface mode – port type):

```
8MG(config-if)#
```

Or Input:

```
8MG(config)# interface vlan 1
```

Output (prompt change to interface mode – port type):

```
8MG(config-if-vlan)#
```

2.3.22.1 (Interface - Port Type) Access-List

The following access-list options are available:

Access-List Action

Set the access-list action.

Syntax:

```
access-list action <deny | permit>
```

Access-List EVC-Policer

EVC policer.

Syntax:

```
access-list evc-policer <evc_policer_id>  
<1-256>: EVC policer ID
```

Access-List Logging

Logging frame information.

Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

Access-List Mirror

Mirror frame to destination mirror port.

Syntax:

```
access-list mirror
```

Access-List Policy

Set specific policy to access list.

Syntax:

```
access-list policy <policy_id>  
<0-255>: Policy ID
```

Access-List Port-State

Re-enable shutdown port that was shut down by access-list module.

Syntax:

```
access-list port-state
```

Access-List Rate-Limiter

Set Rate Limiter to an ACL.

Syntax:

```
access-list rate-limiter <rate_limiter_id>  
<rate_limiter_id>: rate limiter ID (values are: 1-16)
```

Access-List Redirect

Re-direct port traffic to another port by access-list module.

Syntax:

```
access-list redirect interface { <port_type> <port_type_id> | (
<port_type> [ <port_type_list> ] ) }
```

interface: <port_type>, values are:

- * all switches or all ports
- GigabitEthernet: set specific Gigabit Ethernet Port number
- <port-list>: port list in 1/1-8

Access-List Shutdown

Shut down incoming port. The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

Syntax:

```
access-list shutdown
```

Note: To re-enable a port that was shut down, use the <0-255>: Policy ID

Access-List Port-State command described on page 46.

2.3.22.2 (Interface - Port Type) Aggregation

Create an aggregation group.

Syntax:

```
aggregation group <v_uint>
```

Example:

```
aggregation group 1
```

2.3.22.3 (Interface - Port Type) Description

Syntax:

```
description <v_line>
```

<line>: Up to 256 ASCII characters describing this interface.

2.3.22.4 (Interface - Port Type) Do

Use the do command to run exec commands in config mode.

Syntax:

```
do <command>
```

2.3.22.5 (Interface - Port Type) dot1x

Dot1x is the IEEE Standard for port-based Network Access Control. This command sets dot1x per port.

Dot1x guest-vlan

Enables/disables guest VLAN.

Syntax:

```
dot1x guest-vlan
```

Dot1x Port Control

Set the port security state, values are:

force-authorized: port access is allowed
 force-unauthorized: port access is not allowed
 auto: port-based 802.1X authentication
 mac-based: switch authenticates on behalf of the client
 multi: Multiple Host 802.1X Authentication
 single: Single Host 802.1X Authentication

Syntax:

```
dot1x port-control { force-authorized | force-unauthorized | auto |
single | multi | mac-based }
```

Dot1x Radius-qos

Enables/disables per-port state of RADIUS-assigned QoS.

Syntax:

```
dot1x radius-qos
```

Dot1x Radius-vlan

Enables/disables per-port state of RADIUS-assigned VLAN.

Syntax:

```
dot1x radius-vlan
```

Dot1x Re-authenticate

Refresh (restart) 802.1X authentication process.

Syntax:

```
dot1x re-authenticate
```

2.3.22.6 (Interface - Port Type) Duplex

Set the interface duplexity. Values are:

half: forced half duplex
 full: forced full duplex
 auto: auto negotiation of duplex mode, with an optional specification:
 full: advertise full duplex
 half: advertise half duplex

Syntax:

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

2.3.22.7 (Interface - Port Type) End

Go back to EXEC mode.

Syntax:

```
end
```

2.3.22.8 (Interface - Port Type) Excessive-Restart

Restart back off algorithm after 16 collisions. (No excessive-restart means discard frame after 16 collisions.)

Syntax:

```
excessive-restart
```

2.3.22.9 (Interface - Port Type) Exit

Exit from current mode.

Syntax:

```
exit
```

2.3.22.10 (Interface - Port Type) Flowcontrol

Set traffic flow control, values are:

off: disable flow control

on: enable flow control

Syntax:

```
flowcontrol { on | off }
```

2.3.22.11 (Interface - Port Type) frame-length-check

Drop frames with mismatch between EtherType/Length field and actually payload size.

Syntax:

```
frame-length-check
```

2.3.22.12 (Interface - Port Type) Green-Ethernet

Green Ethernet is used to reduce power consumption. The following options are available:

Green-Ethernet EEE

Enable powering down of PHYs when there is no traffic.

Syntax:

```
green-ethernet eee
```

Green-Ethernet Urgent-Queues

Enable EEE urgent queue. When urgent queue is enabled latency is kept to a minimum for traffic going to that queue.

Note: EEE power savings will be reduced

It has the following optional parameter:

[<urgent_queue_range_list>]: EEE interface

Syntax:

```
green-ethernet eee urgent-queues [ <urgent_queue_range_list> ]
```

Green-Ethernet Energy-Detect

Enable power saving for ports with no link partner.

Syntax:

```
green-ethernet energy-detect
```

Green-Ethernet Short Reach

Enable power saving for ports connected to link partner with short cable.

Syntax:

```
green-ethernet short-reach
```

2.3.22.13 (Interface - Port Type) Gvrp

Enable GVRP on interface or interfaces.

Syntax:

```
gvrp
```

2.3.22.14 (Interface - Port Type) Help

The Help command displays a description of the interactive help system.

Syntax:

```
help
```

2.3.22.15 (Interface - Port Type) IP

Set the interface IGMP Snooping state. The following options are available:

Arp

Address Resolution Protocol.

Syntax:

```
ip arp inspection check-vlan
ip arp inspection logging { deny | permit | all }
ip arp inspection trust
```

inspection:

check-vlan:	ARP inspection VLAN mode configuration
logging:	ARP inspection logging mode configuration
trust:	ARP inspection trust configuration

Dhcp

Dynamic Host Configuration Protocol.

Syntax:

```
ip dhcp snooping trust
```

Snooping:

trust: DHCP Snooping trust configuration.

Igmp

Syntax:

```
ip igmp snooping immediate-leave
```

```
ip igmp snooping mrouter
```

Internet Group Management Protocol:

 immediate-leave: immediate leave configuration

 mrouter: multicast router port configuration

Verify

verify command.

Syntax:

```
ip verify source
```

```
ip verify source limit <cnt_var>
```

 source: verify source

 limit: limit command

2.3.22.16 (Interface - Port Type) Ipv6

IPv6 configuration commands.

Syntax:

```
ipv6 mld snooping filter <profile_name>
```

```
ipv6 mld snooping immediate-leave
```

```
ipv6 mld snooping max-groups <throttling>
```

```
ipv6 mld snooping mrouter
```

MLD Snooping

Snooping Multicast Listener Discovery.

 filter: Access control on MLD multicast group registration

 <word16> Profile name in 16 characters

 immediate-leave: Immediate leave configuration

 max-groups: MLD group throttling configuration

 <1-10> Maximum number of MLD group registration.

 mrouter: Multicast router port configuration

2.3.22.17 (Interface - Port Type) LACP

Enable LACP on this interface.

Syntax:

```
lacp
```

LACP Key

Set the key of the LACP aggregation. Values are:

1-65,535: key value

auto: choose a key based on port speed

Syntax:

```
lacp key { <v_1_to_65535> | auto }
```

LACP Port-Priority

Set the LACP priority of the port. Values are:

1-65,535: priority value, lower means higher priority

Syntax:

```
lacp port-priority <v_1_to_65535>
```

LACP Role

Set the LACP active / passive role. Values are:

active: transmit LACP BPDUs continuously

passive: wait for neighbor LACP BPDUs before transmitting

Syntax:

```
lacp role { active | passive }
```

LACP Timeout

Set the period between BPDU transmissions. Values are:

fast: transmit BPDU each second (fast timeout)

slow: transmit BPDU each 30th second (slow timeout)

Syntax:

```
lacp timeout { fast | slow }
```

2.3.22.18 (Interface - Port Type) Link-OAM

Enable or Disable (when the no keyword is entered) Link OAM on the interface.

Link-monitor

Configure link monitoring.

frame: Configure frame error event thresholds and window for error frames that trigger an error-frame link event

frame-seconds: Configure frame seconds summary.

supported: Enable or Disable (when the no keyword is entered) link monitor on the interface.

symbol-period: Configure window and thresholds for an error-symbol period that triggers an error-symbol period link event.

Syntax:

```
link-oam link-monitor frame { [ window <error_window> ] [ threshold <error_threshold> ] }*1
```

```
link-oam link-monitor supported
```

```
link-oam link-monitor symbol-period { [ window <error_window> ] [ threshold <error_threshold> ] }*1
```

threshold: Set a threshold in number of frames

<0-4294967295>: Number of permissible errors frames in the period defined by the error window.

window: Set a window of time during which error frames are counted.
 <1-60>: Duration of the monitoring period in terms of seconds.

mib-retrieval

Set MIB retrieval support.

Syntax:

```
link-oam mib-retrieval supported
```

Supported: Enable or Disable (when the no keyword is entered) MIB retrieval support on the interface.

Mode

Set Link OAM mode Active or Passive on this interface.

Syntax:

```
link-oam mode { active | passive }
```

active: Enable Link OAM Active mode on this interface

passive: Enable Link OAM Passive mode on this interface

remote-loopback

Link OAM remote loopback support.

Syntax:

```
link-oam remote-loopback supported
```

supported: Enable or Disable (when the no keyword is entered) remote loopback on the interface.

variable-retrieve

Set MIB variable retrieve local info or remote info.

Syntax:

```
link-oam variable-retrieve { local-info | remote-info }
```

local-info: Set MIB retrieve local info

remote-info: Set MIB retrieve remote info

2.3.22.19 (Interface - Port Type) LLDP

Set LLDP configurations. The following options are available:

cdp-aware: Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table)

med: Media Endpoint Discovery.

receive: Enable/Disable decoding of received LLDP frames.

tlv-select: Which optional TLVs to transmit.

transmit: Enable/Disabled transmission of LLDP frames.

Syntax:

```
lldp cdp-aware
```

```

lldp med media-vlan policy-list <v_range_list>
lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ]
[ poe ]
lldp med type { connectivity | end-point }
lldp receive
lldp tlv-select { management-address | port-description | system-
capabilities | system-description | system-name }
lldp transmit

```

2.3.22.20 (Interface - Port Type) Loop-Protect

Set the loop protection configuration on the port.

loop-protect: enable loop protection configuration on this port

loop-protect action: action to take if loop detected, values are:

shutdown: shutdown port

log: generate log

loop-protect tx-mode: actively generate PDUs

Syntax:

```

loop-protect
loop-protect action { [ shutdown ] [ log ] }*1
loop-protect tx-mode

```

2.3.22.21 (Interface - Port Type) MAC

Set the MAC security mode.

Syntax:

```

mac address-table learning [ secure ]
address-table: MAC table configuration
learning: port learning mode
[secure]: port secure mode

```

2.3.22.22 (Interface - Port Type) Media-Type

Set the media type, values are:

Syntax:

```

media-type { rj45 | sfp | dual }
dual: dual media interface (copper and fiber interface)
rj45: rj45 interface (copper interface only)
sfp: sfp interface (fiber interface)

```

2.3.22.23 (Interface - Port Type) MTU

Set the maximum transmission unit. The following is a required parameter:

<max_length>: maximum frame size in bytes (values are: 1,518-9,600)

Syntax:

```
mtu <max_length>
```

2.3.22.24 (Interface - Port Type) MVR

Multicast VLAN Registration configuration.

Syntax:

```
mvr immediate-leave
mvr name <mvr_name> type { source | receiver }
mvr vlan <v_vlan_list> type { source | receiver }
<word16> MVR multicast VLAN name
<vlan_list> MVR multicast VLAN list
```

2.3.22.25 (Interface - Port Type) network-clock

Syntax:

```
network-clock synchronization ssm.
```

Synchronization: SSM enable/disable.

2.3.22.26 (Interface - Port Type) No

Negate a command or set its defaults. The following is a list of no commands available from interface Port Mode:

Interface Mode - No Commands (a)

```
no access-list evc-policer
no access-list logging
no access-list mirror
no access-list policy
no access-list port-state
no access-list rate-limiter
no access-list redirect
no access-list shutdown
no aggregation group
```

Interface Mode - No Commands (d-i)

```
no debug phy loopback [ near | far ]
no description
no dot1x guest-vlan
no dot1x port-control
no dot1x radius-qos
no dot1x radius-vlan
no duplex
no excessive-restart
no flowcontrol
no frame-length-check
no green-ethernet eee
no green-ethernet eee urgent-queues [ <urgent_queue_range_list>
]
no green-ethernet energy-detect
```

```
no green-ethernet short-reach
no gvrp
no ip arp inspection check-vlan
no ip arp inspection logging
no ip arp inspection trust
no ip dhcp snooping trust
no ip igmp snooping filter
no ip igmp snooping immediate-leave
no ip igmp snooping max-groups
no ip igmp snooping mrouter
no ip verify source
no ip verify source limit
no ipv6 mld snooping filter
no ipv6 mld snooping immediate-leave
no ipv6 mld snooping max-groups
no ipv6 mld snooping mrouter
```

Interface Mode - No Commands (l)

```
no lacp
no lacp key { <v_1_to_65535> | auto }
no lacp port-priority <v_1_to_65535>
no lacp role { active | passive }
no lacp timeout { fast | slow }
no link-oam
no link-oam link-monitor frame
no link-oam link-monitor frame-seconds
no link-oam link-monitor supported
no link-oam link-monitor symbol-period
no link-oam mib-retrieval supported
no link-oam mode
no link-oam remote-loopback supported
no link-oam variable-retrieve
no lldp cdp-aware
no lldp med media-vlan policy-list [ <v_range_list> ]
no lldp med transmit-tlv [ capabilities ] [ location ] [
    network-policy ] [ poe ]
no lldp med type
no lldp receive
no lldp tlv-select { management-address | port-description |
    system-capabilities | system-description | system-
    name }
no lldp transmit
no loop-protect
no loop-protect action
no loop-protect tx-mode
```

Interface Mode - No Commands (m-p)

```
no mac address-table learning [ secure ]
```

```

no media-type
no mtu
no mvr immediate-leave
no mvr name <mvr_name> type
no mvr vlan <v_vlan_list> type
no network-clock synchronization ssm
no port-security
no port-security maximum
no port-security violation
no ptp <clockinst>
no ptp <clockinst> announce { interval | timeout }
no ptp <clockinst> delay-asymmetry
no ptp <clockinst> delay-mechanism
no ptp <clockinst> delay-req interval
no ptp <clockinst> egress-latency
no ptp <clockinst> ingress-latency
no ptp <clockinst> localpriority
no ptp <clockinst> not-slave
no ptp <clockinst> sync-interval
no pvlan <pvlan_list>
no pvlan isolation

```

Interface Mode - No Commands (q-r)

```

no qos cos
no qos dei
no qos dpl
no qos dscp-classify
no qos dscp-remark
no qos dscp-translate
no qos map cos-tag cos <cos> dpl <dpl>
no qos map tag-cos pcp <pcp> dei <dei>
no qos pcp
no qos policer
no qos qce { [ addr ] [ key ] }*1
no qos queue-policer queue <queue>
no qos queue-shaper queue <queue>
no qos shaper
no qos tag-remark
no qos trust dscp
no qos trust tag
no qos wrr
no rmon collection history <id>
no rmon collection stats <id>

```

Interface Mode - No Commands (s-u)

```

no sflow [ <sampler_idx_list> ]
no sflow counter-poll-interval [ <sampler_idx_list> ]
no sflow max-sampling-size [ sampler <sampler_idx_list> ]

```

```

no shutdown
no snmp-server host <conf_name> traps
no spanning-tree
no spanning-tree auto-edge
no spanning-tree bpdu-guard
no spanning-tree edge
no spanning-tree link-type
no spanning-tree mst <instance> cost
no spanning-tree mst <instance> port-priority
no spanning-tree restricted-role
no spanning-tree restricted-tcn
no speed
no switchport access vlan
no switchport forbidden vlan
no switchport hybrid acceptable-frame-type
no switchport hybrid allowed vlan
no switchport hybrid egress-tag
no switchport hybrid ingress-filtering
no switchport hybrid native vlan
no switchport hybrid port-type
no switchport mode
no switchport trunk allowed vlan
no switchport trunk native vlan
no switchport trunk vlan tag native
no switchport vlan ip-subnet <ipv4>
no switchport vlan mac <mac_addr> [ vlan <vlan_id> ]
no switchport vlan mapping
no switchport vlan protocol group <grp_id> [ vlan <vlan_id> ]
no switchport voice vlan discovery-protocol
no switchport voice vlan mode
no switchport voice vlan security
no thermal-protect grp
no uddl port

```

2.3.22.27 (Interface - Port Type) port-security

Private VLAN.

Syntax:

port-security

port-security maximum [<v_1_to_1024>]

port-security violation { protect | trap | trap-shutdown | shutdown }

maximum: Maximum number of MAC addresses that can be learned on this set of interfaces.

<1-1024>: Number of addresses.

violation: The action involved with exceeding the limit.

Protect:	Don't do anything
Shutdown:	Shutdown the port
Trap:	Send an SNMP trap
trap-shutdown:	Send an SNMP trap and shutdown the port

2.3.22.28 (Interface - Port Type) PTP

Precision time Protocol (1588).

<0-3>: [0-3] Clock instance.

Syntax:

```
ptp <clockinst> [ internal ]
ptp <clockinst> announce { [ interval <interval> ] [ timeout <timeout>
] } *1
ptp <clockinst> delay-asymmetry <delay_asymmetry>
ptp <clockinst> delay-mechanism { e2e | p2p }
ptp <clockinst> delay-req interval <interval>
ptp <clockinst> egress-latency <egress_latency>
ptp <clockinst> ingress-latency <ingress_latency>
ptp <clockinst> localpriority <localpriority>
ptp <clockinst> mcast-dest { default | link-local }
ptp <clockinst> not-slave
ptp <clockinst> sync-interval <interval>
```

Example: 8MG(config-if)# ptp 1 ?

announce:	Set announce interval and timeout
delay-asymmetry:	Set path delay asymmetry <-100000-100000>: Delay asymmetry in ns.
delay-mechanism:	Set delay mechanism e2e: End to End Delay mechanism. p2p: Peer to Peer Delay mechanism.
delay-req:	Set Path-Delay request interval
egress-latency:	Set port egress latency <-100000-100000>: Egress latency in ns.
ingress-latency:	Set port ingress latency <-100000-100000>: Ingress latency in ns.
internal:	Enable as an internal interface
localpriority:	Local priority pr port for G8275.1 BMC algorithm (1 is highest priority). <1-255>: PTP clock priority1: range = 1-255.
mcast-dest:	Set multicast destination address type for the port default: Default destination address

link-local: Link-local destination address
not-slave: Set 'not-slave' attribute for G8275.1 BMC algorithm
sync-interval: Set sync interval.
<-7-4>: sync interval.

2.3.22.29 (Interface - Port Type) PVLAN

Set the private VLAN options. There are two private VLAN options:

<range_list>: list of PVLANs. Range is from 1 to number of ports.

isolation: port isolation

Syntax:

```
pvlan <pvlan_list>
```

```
pvlan isolation
```


2.3.22.30 (Interface - Port Type) QoS

Set the Quality of Service (QoS) parameters. The following QoS options are available:

QoS COS

Set the class of service configuration. The parameter is:

<cos>: Specific class of service, values are 0-7

Syntax:

```
qos cos <cos>
```

QoS DEI

Set Drop Eligible Indicator configuration. The parameter is:

<dei>: Specific Drop Eligible Indicator, values are 0-1

Syntax:

```
qos dei <dei>
```

QoS DPL

Set Drop Precedence Level configuration. The parameter is:

<dpl>: specific Drop Precedence Level

Syntax:

```
qos dpl <dpl>
```

QoS DSCP-classify

DSCP ingress classification.

Syntax:

```
qos dscp-classify { zero | selected | any }
```

any: Classify to new DSCP always

selected: Classify to new DSCP if classify is enabled for specific DSCP value in global DSCP classification map

zero: Classify to new DSCP if DSCP is 0

QoS DSCP- remark

DSCP egress remarking.

Syntax:

```
qos dscp-remark { rewrite | remap | remap-dp }
```

remap: Rewrite DSCP field using classified DSCP and DPL=0 remapped through global dscp-egress-translation map

remap-dp: Rewrite DSCP field using classified DSCP and DPL remapped through global DSCP egress translation map

rewrite: Rewrite DSCP field with classified DSCP value (no translation)

QoS DSCP- translate

DSCP ingress translation.

Syntax:

```
qos dscp-translate
```

QoS Map

QoS Map/Table configuration.

Syntax:

```
qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>
```

```
qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>
```

cos-tag: Map for cos to tag configuration

cos: <0~7> Specific class of service or range.

tag-cos: Map for tag to cos configuration

pcp: Specify PCP (Priority Code Point)

<0~7> Specific PCP or range.

QoS PCP

Set the Priority Code Point configuration. The parameter is:.

<pcp>: specific Priority Code Point, values are 0-7

Syntax:

```
qos pcp <pcp>
```

QoS Policer

Set the rate limitation policer configuration.

Syntax:

```
qos policer <rate> [ kbps | mbps | fps | kfps ] [ flowcontrol ]
```

The parameters are:

<1-3276700>: Policer rate (default kbps). Internally rounded up to the nearest value supported by the port policer.

fps: rate is fps

flowcontrol: enable flow control

QoS QCE

Set the QoS Control Entry according to Source or Destination MAC address.

Syntax:

```
qos qce { [ addr { source | destination } ] [ key { double-tag |
normal | ip-addr | mac-ip-addr } ] } *1
```

The parameters are:

addr: setup address match mode

source: Match SMAC and SIP (default)

destination: Match DMAC and DIP

QoS Queue-Policer Queue

Queue policer configuration.

Syntax:

```
qos queue-policer queue <queue> <rate> [ kbps | mbps ]
```

<0~7>: Specific queue or range.

QoS Queue-Shaper Queue

Set the queue-shaper configuration.

Syntax:

```
qos queue-shaper queue <queue> <rate> [ kbps | mbps ] [ excess ] [
rate-type { line | data } ]
```

The parameters are:

<0~7>: Specific queue or range

<rate>: shaper rate in kbps, values are 100-3,300,000

[excess]: allow use of excess bandwidth

QoS Tag-remark

Tag remarking configuration.

Syntax:

```
qos tag-remark { pcp <pcp> dei <dei> | mapped }
```

mapped: Used mapped values (COS, DPL -> PCP, DEI)

pcp: Specify default PCP

QoS Trust

Trust configuration.

Syntax:

```
qos trust dscp
```

```
qos trust tag
```

dscp: DSCP value

tag: VLAN tag

QoS WRR

Set the Weighted Round Robin configuration.

Syntax:

```
qos wrr <w0> <w1> <w2> <w3> <w4> <w5>
```

The parameters are:

<w0> <w1> <w2> <w3> <w4> <w5>:

weight for queue n, values can be from 1 to 100

2.3.22.31 (Interface - Port Type) RMON

Configure Remote Monitoring on an interface.

Syntax:

```
rmon collection history <id> [ buckets <buckets> ] [ interval
<interval> ]
rmon collection stats <id>
```

Collection

Configure Remote Monitoring Collection on an interface. The parameters are:

History: Configure history

<1-65535>: History entry ID.

Stats: Configure statistics

<1-65535>: Statistics entry ID.

2.3.22.32 (Interface - Port Type) sFLOW

Statistics flow.

Syntax:

```
sflow [ <sampler_idx_list> ]
sflow counter-poll-interval [ sampler <sampler_idx_list> ] [
<poll_interval> ]
sflow max-sampling-size [ sampler <sampler_idx_list> ] [
<max_sampling_size> ]
sflow sampling-rate [ sampler <sampler_idx_list> ] [ <sampling_rate> ]
```

counter-poll-interval: The interval - in seconds - between counter poller samples.

<1-3600>: seconds.

max-sampling-size: Specifies the maximum number of bytes to transmit per flow sample.

<14-200>: bytes.

sampling-rate: Specifies the statistical sampling rate. The sample rate is specified as N to sample 1/Nth of the packets in the monitored flows. There are no restrictions on the value, but the switch will adjust it to the closest possible sampling rate.

<1-4294967295>: Sampling rate.

2.3.22.33 (Interface - Port Type) Shutdown

Use the shutdown command to shut down the interface.

Syntax:

```
shutdown
```

2.3.22.34 (Interface - Port Type) SNMP-Server Host

Set SNMP host's configurations.

Syntax:

```
snmp-server host <conf_name> traps [ linkup ] [ linkdown ] [ lldp ]
```

<conf_name>: name of the host configuration

traps: enable traps

[linkdown]: link down event

[linkup]: link up event

[lldp]: LLDP event

2.3.22.35 (Interface - Port Type) Spanning-Tree

Set the spanning tree protocol mode per interface.

auto-edge: auto detect edge status

bpdu-guard: enable/disable BPDU guard

edge: edge port

link-type: port link-type

mst: STP bridge instance

restricted-role: port role is restricted (never root port)

restricted-tcn: restrict topology change notifications

Syntax:

```
spanning-tree
```

```
spanning-tree auto-edge
```

```
spanning-tree bpdu-guard
```

```
spanning-tree edge
```

```
spanning-tree link-type { point-to-point | shared | auto }
```

```
spanning-tree mst <instance> cost { <cost> | auto }
```

```
spanning-tree mst <instance> port-priority <prio>
```

```
spanning-tree restricted-role
```

```
spanning-tree restricted-tcn
```

2.3.22.36 (Interface - Port Type) Speed

Configures interface speed. If you use 10, 100, or 1000 keywords with the auto keyword the port will only advertise the specified speeds. Values are:

10: 10Mbps

100: 100Mbps

1000: 1Gbps

Auto: auto negotiation

Syntax:

```
speed { 10g | 2500 | 1000 | 100 | 10 | auto { [ 10 ] [ 100 ] [ 1000 ] } }
```

2.3.22.37 (Interface - Port Type) Switchport

Set VLAN characteristics.

Switchport Access VLAN

Set VLAN access mode characteristics of the interface. Requires the following parameter:

vlan: Set VLAN when interface is in access mode, enter the pvid:

<pvid>: VLAN ID of the VLAN when this port is in access mode

Syntax:

```
switchport access vlan <pvid>
```

Switchport Forbidden VLAN

Add or remove forbidden VLANs from the current list of forbidden VLANs.

The parameters are:

<vlan_list>: VLAN IDs

add/remove: add to or remove from the existing list

Syntax:

```
switchport forbidden vlan { add | remove } <vlan_list>
```

Switchport Hybrid Acceptable-Frame-Type

Set acceptable frame type on a port. Values are:

all: allow all frames

tagged: allow only tagged frames

untagged: allow only untagged frames

Syntax:

```
switchport hybrid acceptable-frame-type { all | tagged | untagged }
```

Switchport Hybrid Allowed VLAN

Set allowed VLAN characteristics when interface is in hybrid mode. Values are:

<vlan_list> VLAN IDs of the allowed VLANs when this port is in hybrid mode

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

Syntax:

```
switchport hybrid allowed vlan { all | none | [ add | remove | except ] <vlan_list> }
```

Switchport Hybrid Egress-Tag

Set egress VLAN tagging configuration. Values are:

none: no egress tagging

all: tag all frames

except-native: tag all frames except frames classified to native VLAN of the hybrid port

Syntax:

```
switchport hybrid egress-tag { none | all [ except-native ] }
```

Switchport Hybrid Ingress-Filtering

VLAN ingress filter configuration (enable ingress filtering).

Syntax:

```
switchport hybrid ingress-filtering
```

Switchport Hybrid Native VLAN

Set native VLAN. Values are:

<pvid>: VLAN ID of the native VLAN when this port is in hybrid mode

Syntax:

```
switchport hybrid native vlan <pvid>
```

Switchport Hybrid Port-Type

Set the port type. Values are:

c-port: customer port

s-custom-port: custom provider port

s-port: provider port

unaware: port in not aware of VLAN tags

Syntax:

```
switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }
```

Switchport Mode

Set mode of the interface.

access: set mode to ACCESS unconditionally

hybrid: set mode to HYBRID unconditionally

trunk: set mode to TRUNK unconditionally

Syntax:

```
switchport mode { access | trunk | hybrid }
```

Switchport Trunk Allowed VLAN

Set allowed VLAN characteristics when interface is in trunk mode. Set the following additional parameters:

<vlan_list>: VLAN IDs of the allowed VLANs when this port is in trunk mode

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

Syntax:

```
switchport trunk allowed vlan { all | none | [ add | remove | except ]  
<vlan_list> }
```

Switchport Trunk Native VLAN

Set native VLAN when interface is in trunk mode. Set the following parameter:

<vlan_id>: VLAN ID of the native VLAN when this port is in trunk mode

Syntax:

```
switchport trunk native vlan <pvid>
```

Switchport Trunk VLAN Tag Native

Tag Native VLAN.

Syntax:

```
switchport trunk vlan tag native
```

switchport vlan ip-subnet

Syntax:

```
switchport vlan ip-subnet [ id <1-128> ] <ipv4> vlan <vid>
```

<ipv4_subnet>: Source IP address and mask (Format:

xx.xx.xx.xx/mm.mm.mm.mm).

id: Specify an index for the IP subnet entry (deprecated).

switchport vlan mac

Syntax:

```
switchport vlan mac <mac_addr> vlan <vid>
```


<mac_ucast>: 48 bit unicast MAC address: xx:xx:xx:xx:xx:xx

switchport vlan mapping

Syntax:

```
switchport vlan mapping <gid>
```

<1-8>: Group id.

switchport vlan protocol group

Syntax:

```
switchport vlan protocol group <grp_id> vlan <vid>
```

<word16>: Group Name (Range: 1 - 16 characters).

switchport voice vlan discovery-protocol

Syntax:

```
switchport voice vlan discovery-protocol { oui | lldp | both }
```

both: Detect telephony device by OUI address and LLDP

lldp: Detect telephony device by LLDP

oui: Detect telephony device by OUI address

switchport voice vlan mode

Syntax:

```
switchport voice vlan mode { auto | force | disable }
```

auto: Enable auto detect mode

disable: Disjoin Voice VLAN

force: Force to join Voice VLAN

switchport voice vlan security

Syntax:

```
switchport voice vlan security
```

2.3.22.38 (Interface - Port Type) Thermal-Protect Port-Prio

Set the thermal priority for the interface. Set the priority values:

<prio>: priority values can be from 0-3

Syntax:

```
thermal-protect port-prio <prio>
```

2.3.23 Interface - VLAN

Set the VLAN interface configuration parameters.

Syntax:

```
interface vlan <vlist>
```

vlan: VLAN interface configurations

<vlist>: List of VLAN interface numbers, 1~4095

Input:

```
8MG(config)# interface vlan 1
```

Output (prompt change to interface mode – vlan):

```
8MG(config-if-vlan)#
```

The following commands are available in interface mode – vlan:

2.3.23.1 (Interface - VLAN) Do

Run exec commands in config mode.

Syntax:

```
do <command>
```

2.3.23.2 (Interface - VLAN) End

Go back to EXEC mode

Syntax:

```
end
```

2.3.23.3 (Interface - VLAN) Exit

Exit from current mode.

Syntax:

```
exit
```

2.3.23.4 (Interface - VLAN) Help

Display description of the interactive help system.

Syntax:

```
help
```

2.3.23.5 (Interface - VLAN) IP

Set IPv4 Address configuration.

IP Address

Set the IP address configuration.

<address>: IP (IPv4) address

dhcp: enable Dynamic Host Configuration Protocol (DHCP)

fallback: dhcp fallback settings

<fallback_address> dhcp fallback address (send traffic to this ip address if the DHCP server goes offline)

<fallback_netmask> dhcp fallback netmask

[timeout <fallback_timeout>] dhcp fallback timeout, length of time in seconds that the DHCP server can be unresponsive, before traffic will be sent to the fallback address

Syntax:

```
ip address { { <address> <netmask> } | { dhcp
[ fallback <fallback_address> <fallback_netmask>
[ timeout <fallback_timeout> ] ] } }
```

IP IGMP Snooping

Enable IGMP snooping.

Syntax:

```
ip igmp snooping
```

IP IGMP Snooping Compatibility

Syntax:

```
ip igmp snooping compatibility { auto | v1 | v2 | v3 }
```

auto: Compatible with IGMPv1/IGMPv2/IGMPv3

v1: Forced IGMPv1

v2: Forced IGMPv2

v3: Forced IGMPv3

IP IGMP Snooping last-member-query-interval

Syntax:

```
ip igmp snooping last-member-query-interval <ipmc_lmqi>
```

<0-31744>: 0 - 31744 tenths of seconds.

IP IGMP Snooping Priority

Syntax:

```
ip igmp snooping priority <cos_priority>
```

<0-7>: CoS priority ranges from 0 to 7

IP IGMP Snooping Querier

Set the IGMP Querier configuration.

Syntax:

```
ip igmp snooping querier { election | address <v_ipv4_ucast> }
```

Election: act as an IGMP Querier to join Querier-Election

Address: IGMP Querier address configuration

<ipv4_ucast>: a valid IPv4 unicast address.

2.3.23.6 (Interface - VLAN) IPV6

IPv6 configuration commands.

Address

Configure the IPv6 address of an interface.

Syntax:

```
ipv6 address <subnet>
```

```
ipv6 address { autoconfig | dhcp [ rapid-commit ] }
```

<ipv6_subnet>: IPv6 prefix x:x::y/z

Dhcp: Enable DHCPv6 client function

rapid-commit: Enable DHCPv6 client Rapid-Commit option

MLD Snooping Compatibility

Interface compatibility.

Syntax:

```
ipv6 mld snooping compatibility { auto | v1 | v2 }
```

auto: Compatible with MLDv1/MLDv2

v1: Forced MLDv1

v2: Forced MLDv2

MLD Snooping last-member-query-interval

Last Member Query Interval in tenths of seconds.

Syntax:

```
ipv6 mld snooping last-member-query-interval <ipmc_lmqi>
```

<0-31744>: 0 - 31744 tenths of seconds.

MLD Snooping Priority

Interface CoS priority.

Syntax:

```
ipv6 mld snooping priority <cos_priority>
```

<0-7>: CoS priority ranges from 0 to 7.

MLD Snooping Querier

MLD Querier configuration.

Syntax:

```
ipv6 mld snooping querier election
```

MLD Snooping Query-Interval

Query Interval in seconds.

Syntax:

```
ipv6 mld snooping query-interval <ipmc_qi>
```

<1-31744>: 1 - 31744 seconds.

MLD Snooping Query-Max-Response-Time

Query Response Interval in tenths of seconds.

Syntax:

```
ipv6 mld snooping query-max-response-time <ipmc_gri>
```

<0-31744>: 0 - 31744 seconds.

MLD Snooping Query-Robustness-Variable

Robustness Variable.

Syntax:

```
ipv6 mld snooping robustness-variable <ipmc_rv>
```

<1-255>: Packet loss tolerance count from 1 to 255.

MLD Snooping Unsolicited-Report-Interval

Unsolicited Report Interval in seconds.

Syntax:

```
ipv6 mld snooping unsolicited-report-interval <ipmc_uri>
```

<0-31744>: 0 - 31744 seconds.

2.3.23.7 (Interface - VLAN) No

Negate a command or set its defaults.

Syntax of available no commands (for interface VLAN):

```
no ip address
no ip dhcp server
no ip igmp snooping
no ip igmp snooping compatibility
no ip igmp snooping last-member-query-interval
no ip igmp snooping priority
no ip igmp snooping querier { election | address }
no ip igmp snooping query-interval
no ip igmp snooping query-max-response-time
no ip igmp snooping robustness-variable
no ip igmp snooping unsolicited-report-interval
no ipv6 address [ <ipv6_subnet> ]
no ipv6 address { autoconfig | dhcp [ rapid-commit ] }
no ipv6 mld snooping
no ipv6 mld snooping compatibility
```

```
no ipv6 mld snooping last-member-query-interval
no ipv6 mld snooping priority
no ipv6 mld snooping querier election
no ipv6 mld snooping query-interval
no ipv6 mld snooping query-max-response-time
no ipv6 mld snooping robustness-variable
no ipv6 mld snooping unsolicited-report-interval
```

2.3.24 IP

Interface Internet Protocol config commands for the following protocols:

arp: Address Resolution Protocol
 dhcp: Dynamic Host Configuration Protocol
 dns: Domain Name System
 domain: IP DNS Resolver
 helper-address: DHCP relay server
 http: Hypertext Transfer Protocol
 igmp: Internet Group Management Protocol
 name-server: Domain Name System
 route: Add IP route
 routing: Enable routing for IPv4 and IPv6
 source: Source command
 ssh: Secure Shell
 verify: Verify command

IP arp

Syntax:

```
ip arp inspection
ip arp inspection entry interface <port_type> <in_port_type_id>
<vlan_var> <mac_var> <ipv4_var>
ip arp inspection translate [ interface <port_type> <in_port_type_id>
<vlan_var> <mac_var> <ipv4_var> ]
ip arp inspection vlan <in_vlan_list>
ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }
```

entry: ARP inspection entry
 translate: ARP inspection translate all entries
 vlan: ARP inspection VLAN setting

IP dhcp

Syntax:

```
ip dhcp excluded-address <low_ip> [ <high_ip> ]
ip dhcp pool <pool_name>
ip dhcp relay
ip dhcp relay information option
```

```
ip dhcp relay information policy { drop | keep | replace }
ip dhcp relay module id [ <mid> ]
ip dhcp server
ip dhcp snooping
ip dns proxy
```

excluded-address Prevent DHCP from assigning certain addresses

pool: Configure DHCP address pools

<word32>: Pool name in 32 characters

relay: DHCP relay agent configuration

information: DHCP information option(Option 82)

module: DHCP option(Option 82) relay module ID

server: Enable DHCP server

snooping: DHCP snooping

IP dns

Syntax:

```
ip dns proxy
```

IP domain

Syntax:

```
ip domain name { <v_domain_name> | dhcp [ ipv4 | ipv6 ] [ interface
vlan <v_vlan_id_dhcp> ] }
```

name: Define the default domain name.

IP helper-address

Syntax:

```
ip helper-address <v_ipv4_ucast>
```

<ipv4_ucast>: IP address of the DHCP relay server.

IP HTTP Secure-certificate

Syntax:

```
ip http secure-certificate { upload <url_file> [ pass-phrase
<pass_phrase> ] | delete | generate }
```

delete: Delete the current certificate

generate: Generate a new self-signed RSA certificate

upload: Upload a certificate PEM file

IP HTTP Secure-Redirect

Secure HTTP web redirection.

Syntax:

```
ip http secure-redirect
```

IP HTTP Secure -Server

Secure HTTP web server.

Syntax:

```
ip http secure-server
```

IP IGMP Snooping

Snooping IGMP.

Syntax:

```
ip igmp snooping
```

IP IGMP Snooping VLAN

IGMP VLAN.

Syntax:

```
ip igmp snooping vlan <v_vlan_list>
```

<v_vlan_list>: VLAN identifier(s): VID

IP IGMP Unknown-Flooding

Flooding unregistered IPv4 multicast traffic.

Syntax:

```
ip igmp unknown-flooding
```

IP name-server

Domain Name System.

Syntax:

```
<v_vlan_id_static> ] } | dhcp [ ipv4 | ipv6 ] [ interface vlan  
<v_vlan_id_dhcp> ] }
```

<0-3>: Preference of DNS server. Default selection is 0

<ipv4_ucast>: A valid IPv4 unicast address

<ipv6_ucast>: A valid IPv6 unicast address

dhcp: Dynamic Host Configuration Protocol

IP Route

Add IP route.

Syntax:

```
ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
```

<v_ipv4_addr>: Network

<v_ipv4_netmask>: Netmask

<v_ipv4_gw>: Gateway

IP Routing

Enable routing for IPv4 and IPv6.

Syntax:

```
ip routing
```

IP source

Source command.

Syntax:

```
ip source binding interface <port_type> <in_port_type_id> <vlan_var>
<ipv4_var> <mac_var>
```

binding: IP source binding.

IP ssh

Secure Shell.

Syntax:

```
ip ssh
```

IP verify

Verify command.

Syntax:

```
ip verify source
ip verify source translate
```

source: verify source.

2.3.25 IPMC

IPv4/IPv6 multicast configuration.

Syntax:

```
ipmc profile
ipmc profile <profile_name>
ipmc range <entry_name> { <v_ipv4_mcast> [ <v_ipv4_mcast_1> ] |
<v_ipv6_mcast> [ <v_ipv6_mcast_1> ] }
```

profile: IPMC profile configuration

< profile_name > Profile name in 16 characters.

range: A range of IPv4/IPv6 multicast addresses for the profile

< entry_name > Range entry name in 16 characters.

2.3.26 IPV6

IPv6 configuration commands.

Syntax:

```
ipv6 mld host-proxy [ leave-proxy ]
ipv6 mld snooping
ipv6 mld snooping vlan <v_vlan_list>
ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>
ipv6 mld unknown-flooding
ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan
<v_vlan_id> <v_ipv6_addr> }
```

mld

Multicast Listener Discovery.

Syntax:

```
ipv6 mld host-proxy [ leave-proxy ]
ipv6 mld snooping
```

```

ipv6 mld snooping vlan <v_vlan_list>
ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>
ipv6 mld unknown-flooding
host-proxy:      MLD proxy configuration
                  [leave-proxy]: MLD proxy for leave configuration
snooping:        Snooping MLD
                  <vlan_list>:  VLAN identifier (VID)
ssm-range:       IPv6 address range of Source Specific Multicast
                  <ipv6_mcast>: Valid IPv6 multicast address
unknown-flooding: Flooding unregistered IPv6 multicast traffic

```

route

Configure static routes.

Syntax:

```

ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan
<v_vlan_id> <v_ipv6_addr> }
<ipv6_subnet>: IPv6 prefix x:x::y/z.

```

2.3.27 JSON

JavaScript Object Notation RPC.

Syntax:

```

json notification host <hname>
json notification listen <notification> <host>
notification: Notification request object options:
                host: Notification host
                listen: JSON-RPC notification event subscription.

```

2.3.28 LACP

Set the LACP settings.

lacp system-priority

Syntax:

```

lacp system-priority <v_1_to_65535>
<v_1_to_65535>: Priority value, lower means higher priority,
                values are: 1 to 65,535

```

2.3.29 Line

Configure a terminal line.

Syntax:

```

line { <0~16> | console 0 | vty <0~15> }
<0~16>: List of line numbers
console: Console terminal line

```

vty: Virtual terminal

2.3.30 Lldp

LLDP configurations.

LLDP holdtime

Sets LLDP hold time (The neighbor switch will discarded the LLDP information after “hold time” multiplied with “timer” seconds.).

Syntax:

```
lldp holdtime <val>
```

<val> 2-10 seconds.

LLDP Med

Media Endpoint Discovery.

Syntax:

```
lldp med datum { wgs84 | nad83-navd88 | nad83-mllw }
lldp med fast <v_1_to_10>
lldp med location-tlv altitude { meters | floors } <v_word11>
lldp med location-tlv civic-addr { { country <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_line> }
lldp med location-tlv elin-addr <v_word25>
lldp med location-tlv latitude { north | south } <v_word8>
lldp med location-tlv longitude { west | east } <v_word9>
lldp med media-vlan-policy <policy_index> { voice | voice-signaling |
guest-voice-signaling | guest-voice | softphone-voice | video-
conferencing | streaming-video | video-signaling } { untagged | tagged
<v_vlan_id> [ 12-priority <v_0_to_7> ] } [ dscp <v_0_to_63> ]
```

LLDP Med datum

Syntax:

```
lldp med datum { wgs84 | nad83-navd88 | nad83-mllw }
```

Datum (geodetic system) type options:

nad83-mllw:	Mean lower low water datum 1983
nad83-navd88:	North American vertical datum 1983
wgs84:	World Geodetic System 1984

LLDP Med fast

Syntax:

```
lldp med fast <v_1_to_10>
```

Number of times to repeat LLDP frame transmission at

fast start. <1-10>.

LLDP location-tlv

LLDP-MED Location Type Length Value parameter.

Syntax:

```
lldp med location-tlv altitude { meters | floors } <v_word11>
lldp med location-tlv civic-addr { { country <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_line> }
lldp med location-tlv elin-addr <v_word25>
lldp med location-tlv latitude { north | south } <v_word8>
lldp med location-tlv longitude { west | east } <v_word9>
```

altitude: Altitude parameter.

civic-addr: Civic address information and postal information. The total number of characters for the combined civic address information must not exceed 250 characters. Note: 1) A non empty civic address location will use 2 extra characters in addition to the civic address location text. 2) The 2 letter country code is not part of the 250 characters limitation.

elin-addr: Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling. Emergency Location Identification Number, (e.g. E911 and others), such as defined by TIA or NENA.

latitude: Latitude parameter.

longitude: Longitude parameter.

LLDP media-vlan-policy

Used to create a policy, which can be assigned to an interface.

Syntax:

```
lldp med media-vlan-policy <policy_index> { voice | voice-signaling |
guest-voice-signaling | guest-voice | softphone-voice | video-
conferencing | streaming-video | video-signaling } { untagged | tagged
<v_vlan_id> [ 12-priority <v_0_to_7> ] } [ dscp <v_0_to_63> ]
<0-31>: Policy id for the policy which is created.
```

LLDP Reinit

LLDP tx reinitialization delay in seconds.

Syntax:

```
lldp reinit <val>
```

<val>: 1-10 seconds.

LLDP Timer

Sets LLDP TX interval (The time -in seconds- between each LLDP frame transmitted).

Syntax:

```
lldp timer <val>
```

<val>: 5-32,768 seconds

LLDP Transmission-delay

Sets LLDP transmission-delay in seconds. (The amount of time that the transmission of LLDP frames will be delayed after LLDP configuration has changed.)

Syntax:

```
lldp transmission-delay <val>
```

<val>: 1-8,192 seconds

2.3.31 Logging

Set syslog parameters.

Logging Host

Select the host to be logged.

Syntax:

```
logging host { <v_ipv4_ucast> | <v_word45> }
```

<ipv4_ucast> IP address of the log server

<v_word45> <hostname> Domain name of the log server

Logging Level

Set the level of logging.

Syntax:

```
logging level { info | warning | error }
```

error: Severity 3: Error conditions

informational: Severity 6: Informational messages

notice: Severity 5: Normal but significant condition

warning: Severity 4: Warning conditions

Logging On

Enable syslog server

Syntax:

```
logging on
```

2.3.32 Loop-Protect

Loop protection configuration.

Syntax:

```
loop-protect
```

Loop Protection Shutdown-Time

Loop protection shutdown time interval.

Syntax:

```
loop-protect shutdown-time <t>
```

<t> shutdown time in seconds, values are 0-604,800

Loop Protection Transmit-Time

Loop protection transmit time interval.

Syntax:

```
loop-protect transmit-time <t>
```

<t> transmit time in seconds, values are 1-10

2.3.33 Mac

Set MAC table entries and configuration.

Mac Address-Table Ageing Time

Set MAC address ageing time.

Syntax:

```
mac address-table aging-time <v_0_10_to_1000000>
```

aging-time Mac address aging time

<v_0_10_to_1000000> aging time in seconds, values are

0 - disables aging

10 to 1,000,000

Mac Address-Table Learning Vlan

Syntax:

```
mac address-table learning vlan <vlan_list>
```

Mac Address-Table Static

Set static MAC address.

Syntax:

```
mac address-table static <v_mac_addr> vlan <v_vlan_id>  
interface ( <port_type> [ <v_port_type_list> ] )
```

<v_mac_addr>: 48 bit MAC address: xx:xx:xx:xx:xx:xx

<v_vlan_id>: Vlan ID

Interface:

<port_type>, values are:

*

All switches or all ports

GigabitEthernet: set specific Gigabit Ethernet Port number

<v_port_type_list>: port list in 1/1-8 (monitor source)

2.3.34 Mep

Maintenance Entity Point.

Syntax:

```
mep <inst> [ mip ] { up | down } domain { port | evc | vlan | tp-link
| tunnel-tp | pw | lsp } [ vid <vid> ] [ flow <flow> ] level <level> [
interface <port_type> <port> ]
mep <inst> ais [ frls | frlm ] [ protect ]
mep <inst> aps <prio> [ multi | uni ] { laps | { raps [ octet <octet>
] } }
mep <inst> cc <prio> [ fr300s | fr100s | fr10s | frls | fr6m | frlm |
fr6h ]
mep <inst> ccm-tlv
mep <inst> client domain { evc | vlan | lsp } flow <cflow> [ level
<level> ] [ ais-prio [ <aisprio> | ais-highest ] ] [ lck-prio [
<lckprio> | lck-highest ] ]
mep <inst> dm <prio> [ multi | { uni mep-id <mepid> } ] [ single |
dual ] [ rdtrp | flow ] interval <interval> last-n <lastn>
mep <inst> dm bin fd <num_fd_var>
mep <inst> dm bin ifdv <num_ifdv_var>
mep <inst> dm bin threshold <threshold_var>
mep <inst> dm ns
mep <inst> dm overflow-reset
mep <inst> dm proprietary
mep <inst> dm synchronized
mep <inst> lb <prio> [ dei ] [ multi | { uni { { mep-id <mepid> } | {
mac <mac> } } } | mpls ttl <mpls_ttl> ] count <count> size <size>
interval <interval>
mep <inst> lck [ frls | frlm ]
mep <inst> level <level>
```

<1-100>: The MEP instance number.

os-tlv: Organization-Specific TLV.

2.3.35 Monitor

Set monitor configuration for port mirroring.

The destination port is the port that traffic should be mirrored to.

The source port(s) is the port(s) to be mirrored. (It will be mirrored to the destination port.)

Syntax:

```
monitor session <session_number> [ destination { interface (
<port_type> [ <di_list> ] ) | remote vlan <drvid> 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 ] } | intermediate { interface ( <port_type> [
<ii_list> ] ) | remote vlan <irvid> } ]
```

destination: MIRROR destination interface or VLAN

intermediate: MIRROR intermediate interface, VLAN

source: MIRROR source interface, VLAN
 interface:
 <port_type>, values are:
 * All switches or all ports
 GigabitEthernet: set specific Gigabit Ethernet Port number
 <in_port_type>: port list in 1/1-8 (monitor destination)
 <v_port_type_list>: port list in 1/1-8 (monitor source)
 both: setting source port to both will mirror both ingress and egress traffic
 rx: setting source port to rx will mirror ingress traffic
 tx: Setting source port to tx will mirror egress traffic

2.3.36 MVR

Multicast VLAN Registration configuration.

2.3.36.1 MVE Name

MVR multicast name.

Syntax:

```
mvr name <mvr_name> channel <profile_name>
mvr name <mvr_name> frame priority <cos_priority>
mvr name <mvr_name> frame tagged
mvr name <mvr_name> igmp-address <v_ipv4_ucast>
mvr name <mvr_name> last-member-query-interval <ipmc_lmqi>
mvr name <mvr_name> mode { dynamic | compatible }
```

<word16>: MVR multicast VLAN name.

Input:

```
8MG(config)# mvr name word ?
```

Output:

MVR Name Channel

MVR channel configuration.

Syntax:

```
mvr name <mvr_name> channel <profile_name>
```

<word16>: Profile name in 16 characters.

MVR Name Frame

MVR control frame in TX.

Syntax:

```
mvr name <mvr_name> frame priority <cos_priority>
```

```
mvr name <mvr_name> frame tagged
```

priority: Interface CoS priority

<0-7>: CoS priority ranges from 0 to 7.

tagged: Tagged IGMP/MLD frames will be sent.

MVR Name IGMP-Address

MVR address configuration used in IGMP.

Syntax:

```
mvr name <mvr_name> igmp-address <v_ipv4_ucast>
```

<ipv4_ucast>: A valid IPv4 unicast address.

MVR Name Last-member-query-interval

Last Member Query Interval in tenths of seconds.

Syntax:

```
mvr name <mvr_name> last-member-query-interval <ipmc_lmqi>
<0-31744>: 0 - 31744 tenths of seconds.
```

MVR Name Mode

MVR mode of operation.

Syntax:

```
mvr name <mvr_name> mode { dynamic | compatible }
compatible: Compatible MVR operation mode
dynamic:    Dynamic MVR operation mode.
```

2.3.36.2 MVR Vlan

MVR multicast VLAN.

Syntax:

```
mvr vlan <v_vlan_list> [ name <mvr_name> ]
mvr vlan <v_vlan_list> channel <profile_name>
mvr vlan <v_vlan_list> frame priority <cos_priority>
mvr vlan <v_vlan_list> frame tagged
mvr vlan <v_vlan_list> igmp-address <v_ipv4_ucast>
mvr vlan <v_vlan_list> last-member-query-interval <ipmc_lmqi>
mvr vlan <v_vlan_list> mode { dynamic | compatible }
```

<vlan_list>: MVR multicast VLAN list.

Input:

```
8MG(config)# mvr vlan 1 ?
```

Output:

MVR Vlan Channel

MVR channel configuration.

Syntax:

```
mvr vlan <v_vlan_list> channel <profile_name>
<word16>: Profile name in 16 characters.
```

MVR Vlan Frame

MVR control frame in TX.

Syntax:

```
mvr vlan <v_vlan_list> frame priority <cos_priority>
mvr vlan <v_vlan_list> frame tagged
priority:    Interface CoS priority
             <0-7>: CoS priority ranges from 0 to 7.
```

tagged: Tagged IGMP/MLD frames will be sent.

MVR Vlan IGMP-Address

MVR address configuration used in IGMP.

Syntax:

```
mvr vlan <v_vlan_list> igmp-address <v_ipv4_ucast>
<ipv4_ucast>: A valid IPv4 unicast address.
```

MVR Vlan Last-member-query-interval

Last Member Query Interval in tenths of seconds.

Syntax:

```
mvr name <mvr_name> last-member-query-interval <ipmc_lmqi>
```

<0-31744>: 0 - 31744 tenths of seconds.

MVR Vlan Mode

MVR mode of operation.

Syntax:

```
mvr name <mvr_name> mode { dynamic | compatible }
```

compatible: Compatible MVR operation mode

dynamic: Dynamic MVR operation mode.

2.3.37 Network-clock

Syntax:

```
network-clock clk-source <clk_list> nominate { clk-in | { ptp
<ptp_inst> } | { interface <port_type> <port> } }
network-clock clk-source <clk_src> aneg-mode { master | slave | forced
}
network-clock clk-source <clk_src> hold-timeout <v_3_to_18>
network-clock clk-source <clk_src> priority <prio>
network-clock clk-source <clk_src> ssm-overwrite { prc | ssua | ssub |
eec2 | eec1 | dnu | prs | stu | st2 | tnc | st3e | smc | prov | dus }
network-clock input-source { 1544khz | 2048khz | 10mhz }
network-clock option { eec1 | eec2 }
network-clock output-source { 1544khz | 2048khz | 10mhz }
network-clock selector { { manual clk-source <v_uint> } | selected |
nonrevertive | revertive | holdover | freerun }
network-clock ssm-freerun { prc | ssua | ssub | eec2 | eec1 | dnu |
inv | prs | stu | st2 | tnc | st3e | smc | prov | dus }
network-clock ssm-holdover { prc | ssua | ssub | eec2 | eec1 | dnu |
inv | prs | stu | st2 | tnc | st3e | smc | prov | dus }
network-clock wait-to-restore <wtr_value>
```

clk-source: clk-source - commands related to a specific clock source.

<1~2>: Clock source number.

option: EEC options:

EEC1: DPLL bandwidth = 3,5 Hz, pull-in range = +/-12 ppm

EEC2: DPLL bandwidth = 0,1 Hz, pull-in range = +/-12 ppm.

selector: Selection mode of nominated clock sources:

freerun: Selector is forced in free run.

holdover: Selector is forced in holdover.

manual: Selector is manually set to the chosen clock source.

nonrevertive: Selector is automatically selecting the best clock source - non revertively.

revertive: Selector is automatically selecting the best clock source – revertively.

Selected: Selector is manually set to the pt. selected clock

ssm-freerun:	Source (not possible in unlocked mode).
ssm-holdover:	Free Running SSM overwrite.
wait-to-restore:	Hold Over SSM overwrite.
	WTR time (0-12 min) '0' is disable.
	<0-12> : wait-to-restore value in min.

2.3.38 No

Negate a command or set its defaults.

No Commands (a-b)

```
no aaa accounting { console | telnet | ssh }
no aaa authentication login { console | telnet | ssh | http }
no aaa authorization { console | telnet | ssh }
no access management
no access management <access_id_list>
no access-list ace <ace_list>
no access-list rate-limiter [ <rate_limiter_list> ]
no aggregation mode
no banner [ motd | login | exec ]
```

No Commands (c-d)

```
no clock summer-time
no clock timezone
no debug mep <inst> dm tx { dual | single } <prio> [ interval
<interval> ] [ synchronized ]
no debug mep <inst> test tx { lb | tst } { <prio> | all } [ dei ] [
all-zero | all-one | one-zero ] [ rate <rate> ] [ size <size> ]
no debug mep <inst> volatile
no dot1x authentication timer inactivity
no dot1x authentication timer re-authenticate
no dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }*1
no dot1x guest-vlan
no dot1x guest-vlan supplicant
no dot1x max-reauth-req
no dot1x re-authentication
no dot1x system-auth-control
no dot1x timeout quiet-period
no dot1x timeout tx-period
```

No Commands (e)

```
no enable password [ level <priv> ]
no enable secret { [ 0 | 5 ] } [ level <priv> ]
no eps <inst>
no eps <inst> command
no eps <inst> holdoff
no eps <inst> revertive
no erps <group>
no erps <group> guard
```

```

no erps <group> holdoff
no erps <group> mep
no erps <group> revertive
no erps <group> rpl
no erps <group> topology-change propagate
no erps <group> version
no erps <group> vlan
no evc <evc_id>
no evc ece <ece_id>

```

No Commands (g-i)

```

no green-ethernet eee optimize-for-power
no green-ethernet led interval <v_0_to_24>
no green-ethernet led on-event { [ link-change ] [ error ] }*1
no gvrp
no gvrp max-vlans <maxvlans>
no gvrp time { [ join-time <jointime> ] [ leave-time <leavetime> ] [
leave-all-time <leavealltime> ] }*1
no hostname
no interface vlan <vlist>

```

No Commands (ip-ipv6)

```

no ip arp inspection
no ip arp inspection entry interface <port_type> <in_port_type_id>
<vlan_var> <mac_var> <ipv4_var>
no ip arp inspection vlan <in_vlan_list>
no ip arp inspection vlan <in_vlan_list> logging
no ip dhcp excluded-address <low_ip> [ <high_ip> ]
no ip dhcp pool <pool_name>
no ip dhcp relay
no ip dhcp relay information option
no ip dhcp relay information policy
no ip dhcp relay module id [ <mid> ]
no ip dhcp server
no ip dhcp snooping
no ip dns proxy
no ip domain name
no ip helper-address
no ip http secure-redirect
no ip http secure-server
no ip igmp host-proxy [ leave-proxy ]
no ip igmp snooping
no ip igmp snooping vlan [ <v_vlan_list> ]
no ip igmp ssm-range
no ip igmp unknown-flooding
no ip name-server [ <order> ]
no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
no ip routing

```

```

no ip source binding interface <port_type> <in_port_type_id>
<vlan_var> <ipv4_var> <mac_var>
no ip ssh
no ip verify source
no ipmc profile
no ipmc profile <profile_name>
no ipmc range <entry_name>
no ipv6 mld host-proxy [ leave-proxy ]
no ipv6 mld snooping
no ipv6 mld snooping vlan [ <v_vlan_list> ]
no ipv6 mld ssm-range
no ipv6 mld unknown-flooding
no ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan
<v_vlan_id> <v_ipv6_addr> }

```

No Commands (j-m)

```

no json notification host <name>
no json notification listen [ <notification> [ <host> ] ]
no lacp system-priority <v_1_to_65535>
no lldp holdtime
no lldp med datum
no lldp med fast
no lldp med location-tlv altitude
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 }
no lldp med location-tlv elin-addr
no lldp med location-tlv latitude
no lldp med location-tlv longitude
no lldp med media-vlan-policy <policies_list>
no lldp reinit
no lldp timer
no lldp transmission-delay
no logging host
no logging on
no loop-protect
no loop-protect shutdown-time
no loop-protect transmit-time
no mac address-table aging-time
no mac address-table aging-time <v_0_10_to_1000000>
no mac address-table learning vlan <vlan_list>
no mac address-table static <v_mac_addr> vlan <v_vlan_id> [ interface
( <port_type> [ <v_port_type_list> ] ) ]
no mep <inst>
no mep <inst> ais
no mep <inst> aps

```

```

no mep <inst> cc
no mep <inst> ccm-tlv
no mep <inst> client domain { evc | vlan | lsp } flow { <cflow> | all
}
no mep <inst> dm
no mep <inst> dm bin fd <num_fd_var>
no mep <inst> dm bin ifdv <num_ifdv_var>
no mep <inst> dm bin threshold <threshold_var>
no mep <inst> dm ns
no mep <inst> dm overflow-reset
no mep <inst> dm proprietary
no mep <inst> dm synchronized
no mep <inst> lb
no mep <inst> lck
no mep <inst> link-state-tracking
no mep <inst> lm
no mep <inst> lm flow-counting
no mep <inst> lm oam-counting { [ y1731 | all ] }
no mep <inst> lm rx [ synthetic ] [ fr100s | fr10s | fr1s | fr6m ] [
flr <flr> ] [ meas <meas> ] [ threshold <loss_th> ]
no mep <inst> lm-avail
no mep <inst> lm-avail maintenance
no mep <inst> lm-hli
no mep <inst> lm-notif
no mep <inst> lm-sdeg
no mep <inst> lt
no mep <inst> peer-mep-id { <mepid> | all }
no mep <inst> performance-monitoring
no mep <inst> syslog
no mep <inst> tst rx
no mep <inst> tst tx
no mep <inst> vid
no mep <inst> voe
no monitor session <session_number> [ destination { interface (
<port_type> [ <di_list> ] ) | remote vlan <drvid> reflector-port } |
source { interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] |
remote vlan <srvid> | vlan <source_vlan_list> | cpu [ both | rx | tx ]
} | intermediate { interface ( <port_type> [ <ii_list> ] ) | remote
vlan <irvid> } ]
no mvr
no mvr name <mvr_name> channel
no mvr name <mvr_name> frame priority
no mvr name <mvr_name> frame tagged
no mvr name <mvr_name> igmp-address
no mvr name <mvr_name> last-member-query-interval
no mvr name <mvr_name> mode
no mvr vlan <v_vlan_list>
no mvr vlan <v_vlan_list> channel

```

```

no mvr vlan <v_vlan_list> frame priority
no mvr vlan <v_vlan_list> frame tagged
no mvr vlan <v_vlan_list> igmp-address
no mvr vlan <v_vlan_list> last-member-query-interval
no mvr vlan <v_vlan_list> mode

```

No Commands (n-q)

```

no network-clock clk-source <clk_list> nominate
no network-clock clk-source <clk_src> aneg-mode
no network-clock clk-source <clk_src> hold-timeout
no network-clock clk-source <clk_src> priority
no network-clock clk-source <clk_src> ssm-overwrite
no network-clock input-source
no network-clock option
no network-clock output-source
no network-clock selector
no network-clock ssm-freerun
no network-clock ssm-holdover
no network-clock wait-to-restore
no ntp
no ntp server <index_var>
no port-security
no port-security aging
no port-security aging time
no privilege <mode_name> level <0-15> <cmd>
no ptp <clockinst> clk
no ptp <clockinst> domain
no ptp <clockinst> filter
no ptp <clockinst> ho
no ptp <clockinst> localpriority
no ptp <clockinst> log
no ptp <clockinst> mode { boundary | e2etransparent | p2ptransparent |
master | slave | bcfrontend }
no ptp <clockinst> priority1
no ptp <clockinst> priority2
no ptp <clockinst> servo ad
no ptp <clockinst> servo ai
no ptp <clockinst> servo ap
no ptp <clockinst> servo displaystates
no ptp <clockinst> servo gain
no ptp <clockinst> servo phase-mode
no ptp <clockinst> uni <idx>
no ptp ext
no ptp ho-spec
no ptp system-time
no qos map cos-dscp <cos> dpl <dpl>

```

```

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 } }
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 } }
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>
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 } }
no qos qce <qce_id_range>
no qos storm { unicast | multicast | broadcast }

```

No Commands (r)

```

no radius-server attribute 32
no radius-server attribute 4
no radius-server attribute 95
no radius-server deadtime
no radius-server host <host_name> [ auth-port <auth_port> ] [ acct-
port <acct_port> ]
no radius-server key
no radius-server retransmit
no radius-server timeout
no rmon alarm <id>
no rmon event <id>

```

No Commands (s)

```

no sflow agent-ip
no sflow collector-address [ receiver <rcvr_idx_list> ]
no sflow collector-port [ receiver <rcvr_idx_list> ]
no sflow max-datagram-size [ receiver <rcvr_idx_list> ]
no sflow timeout [ receiver <rcvr_idx_list> ]
no snmp-server
no snmp-server access <group_name> model { v1 | v2c | v3 | any } level
{ auth | noauth | priv }
no snmp-server community v2c { ro | rw }
no snmp-server community v3 <community>
no snmp-server contact
no snmp-server engined-id local
no snmp-server host <conf_name>
no snmp-server location
no snmp-server security-to-group model { v1 | v2c | v3 } name
<security_name>
no snmp-server trap
no snmp-server user <username> engine-id <engineID>
no snmp-server version
no snmp-server view <view_name> <oid_subtree>
no spanning-tree edge bpdu-filter

```



```

no spanning-tree edge bpdu-guard
no spanning-tree mode
no spanning-tree mst <instance> priority
no spanning-tree mst <instance> vlan
no spanning-tree mst forward-time
no spanning-tree mst hello-time
no spanning-tree mst max-age
no spanning-tree mst max-hops
no spanning-tree mst name
no spanning-tree recovery interval
no spanning-tree transmit hold-count
no switchport vlan mapping <gid> <vlan_list>

```

No Commands (t-v)

```

no tacacs-server deadtime
no tacacs-server host <host_name> [ port <port> ]
no tacacs-server key
no tacacs-server timeout
no thermal-protect grp <grp_list>
no udld { aggressive | enable }
no upnp
no upnp advertising-duration
no upnp ttl
no username <username>
no vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap
{ <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } [
group <word16> ]
no vlan { { ethertype s-custom-port } | <vlan_list> }
no voice vlan
no voice vlan aging-time
no voice vlan class
no voice vlan oui <oui>
no voice vlan vid
no web privilege group [ <group_name> ] level

```

2.3.39 NTP

Configure NTP.

Syntax:

```
ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> |
<name_var> }
```

<1-5>: index number

<domain_name>:	domain name
<ipv4_u cast>:	IPv4 address
<ipv6_u cast>:	IPv6 address

2.3.40 Port Security

Enable/disable port security globally.

Syntax:

```
port-security
port-security aging
port-security aging time <v_10_to_10000000>
<10-10000000>: seconds.
```

2.3.41 Privilege

Set the command privilege parameters, to allow or deny access to specific parameters.

Syntax:

```
privilege <mode_name> level <privilege> <cmd>
<word> Valid words are 'config-vlan' 'configure' 'dhcp-pool' 'exec'
        'if-vlan' 'interface' 'ipmc-profile' 'json-noti-host' 'line'
        'snmps-host' 'stp-aggr'.
level:      set privilege level of command.
<privilege>: privilege level, values are 0-15.
```

2.3.42 PTP

Precision time Protocol (1588).

Syntax:

```
ptp <clockinst> clk sync <threshold> ap <ap>
ptp <clockinst> domain <domain>
ptp <clockinst> filter [ delay <delay> ] [ filter-type { basic | ms-
pdv } ] [ period <period> ] [ dist <dist> ]
ptp <clockinst> ho [ filter <ho_filter> ] [ adj-threshold
<adj_threshold> ]
ptp <clockinst> localpriority <localpriority>
ptp <clockinst> log <debug_mode>
ptp <clockinst> mode { boundary | e2ettransparent | p2pttransparent |
master | slave | bcfrontend } [ onestep | twostep ] [ ethernet |
ethernet-mixed | ip4multi | ip4mixed | ip4unicast | oam | onepps ] [
oneway | twoway ] [ id <v_clock_id> ] [ vid <vid> [ <prio> ] [ tag ] ]
[ mep <mep_id> ] [ profile { ieee1588 | g8265.1 | g8275.1 } ] [ clock-
domain 0 ] [ dscp <dscp_id> ]
ptp <clockinst> priority1 <priority1>
ptp <clockinst> priority2 <priority2>
ptp <clockinst> servo ad <ad>
ptp <clockinst> servo ai <ai>
ptp <clockinst> servo ap <ap>
ptp <clockinst> servo displaystates
ptp <clockinst> servo gain <gain>
ptp <clockinst> servo phase-mode
ptp <clockinst> slave-cfg [ stable-offset <stable_offset> ] [ offset-
ok <offset_ok> ] [ offset-fail <offset_fail> ]
```

```

ptp <clockinst> time-property [ utc-offset <utc_offset> ] [ valid ] [
  leap-59 | leap-61 ] [ time-traceable ] [ freq-traceable ] [
  ptptimescale ] [ time-source <time_source> ]
ptp <clockinst> uni <idx> [ duration <duration> ] <ip>
ptp ext [ output | input | out-in ] [ ext <clockfreq> ] [ vcxo | ltc-
  freq | synce-dpll | osc | ltc-phase ]
ptp ho-spec [ cat1 <cat1> ] [ cat2 <cat2> ] [ cat3 <cat3> ]
ptp ref-clock { mhz125 | mhz156p25 | mhz250 }
ptp system-time { get | set }
ptp tc-internal [ mode <mode> ]

```

<0-3>: Clock instance [0-3]

ext: Update the 1PPS and External clock output configuration and
vcxo frequency rate adjustment option

ho-spec: Set the Holdover specification for G8275 PTP clocks

system-time: Enable synchronization between PTP time and system time

tc-internal: Define the internal mode used in TC's.

Example:

Input:

8MG(config)# ptp 0 ?

Output:

Clk Sync: Set PTP slave clock options.

<1-1000>: [1..1000] Threshold in ns for offsetFromMaster
defines when the offset increment/decrement mode is entered.

Domain: Clock domain for PTP.

<0-127>: PTP domain: range = 0-127.

Filter: Set filter parameters:

delay: Set delay filter parameter.

<0-6>: Log2 of timeconstant in delay lowpass
filter, valid range: 1-6, Setting the value to 0 means
use the same filter function as for the offset
measurement, in this case the delay filter uses the
'period' and 'dist' parameters.

dist: Set offset filter dist parameter.

<0-10>: Distance between servo update n number
of measurement periods, valid range: 0-10, 0 => 0,1
Hz lowpass filtering, 1 => averaging over period,
>1 => 'min' offset filtering.

filter-type: Define offset filter type:

basic: Basic offset filter.

ms-pdv: MS-PDV.

period: Set offset filter period parameter.
<1-10000> Measurement period in number of sync events, valid range: 1-10000.

ho: Set PTP Servo holdover parameters.

adj-threshold: Set adjustment threshold.
<1-3000>: [1..3000] max frequency adjustment change within the holdover stabilization period (in units of 0.1 ppb).

filter: Set stabilization period.
<10-86400>: [10..86400] Holdover filter and stabilization period.

localpriority: Local priority for G8275.1 BMC algorithm (1 is highest priority).
<1-255>: PTP clock priority1: range = 1-255.

log: Set the PTP debug mode.
<1-4>: 1-4 Debug log mode, 1 => log offset from master, 2 => log sync packets, 3 => log Delay_req, 4 => log both.

mode: Enable a PTP instance:

- bcfrend: Boundary Clock front end
- boundary: Ordinary / Boundary clock
- e2transparent: End to end transparent clock
- master: Master only clock
- p2transparent: Peer to peer transparent clock
- slave: Slave only clock.

priority1: Clock priority 1 for PTP BMC algorithm (0 is highest priority).
<0-255>: PTP clock priority1: range = 0-255.

priority2: Clock priority 2 for PTP BMC algorithm (0 is highest priority).
<0-255>: PTP clock priority2: range = 0-255.

servo: Set Servo parameters:

- ad: Set 'D' parameter in the servo
- ai: Set 'I' parameter in the servo
- ap: Set 'P' parameter in the servo
- displaystates: Enable logging of servo parameters on the console
- gain: Set PID servo gain parameter.
- phase-mode: Enable phase mode in the servo

slave-cfg: Set PTP clock Slave Configuration.

- offset-fail: set the offset-fail threshold
- offset-ok: set the offset-ok threshold
- stable-offset: set the stable-offset threshold.

time-property: Set time properties.

- freq-traceable: frequency is traceable
- leap-59: leap59 in current day
- leap-61: leap61 in current day
- ptptimescale: timing is a PTP time scale
- time-source: set timesource
- time-traceable: timing is traceable
- utc-offset: set utc offset
- valid: UTC offset is valid.

uni: Set a Unicast Slave configuration entry.

<0-4> [0..4] Index in the slave table.

2.3.43 Qos

Quality of Service.

QoS QCE Map

Refresh a QoS Control Entry (QCE) tables in hardware.

Syntax:

```
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 } }
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 } }
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>
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> 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 } }
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 } }
```

cos-dscp: Map for COS to DSCP

<0~7>: Specific class of service or range.

dscp-classify: Map for DSCP classify enable

dscp-cos: Map for DSCP to COS

dscp-egress-translation: Map for DSCP egress translation

dscp-ingress-translation: Map for DSCP ingress translation.

<0~63>: Specific DSCP or range

af11 Assured Forwarding PHB AF11(DSCP 10)

af12 Assured Forwarding PHB AF12(DSCP 12)

af13 Assured Forwarding PHB AF13(DSCP 14)

af21 Assured Forwarding PHB AF21(DSCP 18)

af22 Assured Forwarding PHB AF22(DSCP 20)

af23 Assured Forwarding PHB AF23(DSCP 22)

af31 Assured Forwarding PHB AF31(DSCP 26)

af32 Assured Forwarding PHB AF32(DSCP 28)

af33 Assured Forwarding PHB AF33(DSCP 30)

af41 Assured Forwarding PHB AF41(DSCP 34)

af42 Assured Forwarding PHB AF42(DSCP 36)

af43 Assured Forwarding PHB AF43(DSCP 38)

be Default PHB(DSCP 0) for best effort traffic

cs1 Class Selector PHB CS1 precedence 1(DSCP 8)

cs2 Class Selector PHB CS2 precedence 2(DSCP 16)

cs3 Class Selector PHB CS3 precedence 3(DSCP 24)

cs4 Class Selector PHB CS4 precedence 4(DSCP 32)

cs5 Class Selector PHB CS5 precedence 5(DSCP 40)

cs6 Class Selector PHB CS6 precedence 6(DSCP 48)

cs7 Class Selector PHB CS7 precedence 7(DSCP 56)

ef Expedited Forwarding PHB(DSCP 46)

va Voice Admit PHB(DSCP 44).

QoS QCE

Update an existing QCE (QoS Control Entry).

Syntax:

```
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 } ] [ pcp-dei {
<action_pcp> <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 ]

```

refresh: Refresh QCE tables in hardware

[update]: update an existing QCE

<qce_id>: QCE ID, values are 1-256.

QoS Storm

Set the QoS storm policer configuration.

Syntax:

```

qos storm { unicast | multicast | broadcast } <rate> [ fps | kfps |
kbps | mbps ]

```

unicast: police unicast frames

multicast: police multicast frames

broadcast: police broadcast frames

<rate>: 1024 kfps (Policer rate is <1,2,4,8,16,32,64,128,256,512> (default fps))

[kfps]: rate is kfps.

2.3.44 Radius-Server

Configure RADIUS. The radius-server has the following options:

Radius-Server Attribute

Set the attributes to be used in the RADIUS Access-Request packets.

Syntax:

```

radius-server attribute 32 <id>
radius-server attribute 4 <ipv4>
radius-server attribute 95 <ipv6>

```

32: attribute number 32 = NAS-Identifier

4: attribute number 4 = NAS-IP-Address

95: attribute number 95 = NAS-IPv6-Address.

Radius-Server Deadtime

Set the time to stop using a RADIUS server that does not respond.

Syntax:

```
radius-server deadtime <minutes>
```

<minutes>: Time in minutes, value from 1-1,440

Radius-Server Host

Specify a RADIUS server.

Syntax:

```
radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port
<acct_port> ] [ timeout <seconds> ] [ retransmit <retries> ] [ key
<key> ]
```

<host_name>: host name or IP address, from 1 to 255 characters

[auth-port <auth_port>]: UDP port for RADIUS authentication server

<auth_port>: value of UDP port number can be 0-65,535

[acct-port <acct_port>]: UDP port for RADIUS accounting server

<acct_port>: value of UDP port number can be 0-65,535

[timeout <seconds>]: Time to wait for this RADIUS server to reply

<seconds>: wait time in seconds, value can be 1-1,000
(overrides default)

[retransmit <retries>]: Specify the number of retries to active server

<retries>: number of retries for a transaction, value can be 1-1,000
(overrides default)

[key <key>]: Server specific key (overrides default)

<key>: the shared key, value can be 1-63 characters

Radius-Server Key

Set RADIUS encryption key

Syntax:

```
radius-server key <key>
```

<key>: the shared key, value can be 1-63 characters

Radius-Server Retransmit

Specify the number of retries to active server

Syntax:

```
radius-server retransmit <retries>
```

<retries> number of retries for a transaction, value can be 1-1,000

Radius-Server timeout

Time to wait for a RADIUS server to reply

Syntax:

```
radius-server timeout <seconds>
```

<seconds>: wait time in seconds, value can be 1-1,000

2.3.45 Rmon

Remote Monitoring.

Alarm

Configure an RMON alarm.

Syntax:

```
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
] }
```

<1-65535>: Alarm entry ID.

ifInDiscards:	The number of inbound packets that are discarded even the packets are normal.
ifInErrors:	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
ifInNUcastPkts:	The number of broadcast and multicast packets delivered to a higher-layer protocol.
ifInOctets:	The total number of octets received on the interface, including framing characters.
ifInUcastPkts:	The number of unicast packets delivered to a higher-layer protocol.
ifInUnknownProtos:	The number of the inbound packets that were discarded because of the unknown or unsupported protocol.
ifOutDiscards:	The number of outbound packets that are discarded event the packets is normal.
ifOutErrors:	The number of outbound packets that could not be transmitted because of errors.
ifOutNUcastPkts:	The number of broadcast and multicast packets that request to transmit.
ifOutOctets:	The number of octets transmitted out of the interface including framing characters.
ifOutUcastPkts:	The number of unicast packets that request to transmission.

Event

Configure an RMON event.

```
rmon event <id> [ log ] [ trap <community> ] { [ description
<description> ] }
```

<1-65535>: Event entry ID.

description: Specify a description of the event.
 <line127>: Event description.

log: Generate RMON log when the event fires.
 trap: Generate SNMP trap when the event fires.
 <word127>: SNMP community string.

2.3.46 sFLOW

Statistics flow.

Agent-IP

The agent IP address used as agent-address in UDP datagrams. Defaults to IPv4 loopback address.

Syntax:

```
sflow agent-ip { ipv4 <v_ipv4_addr> | ipv6 <v_ipv6_addr> }
```

Collector-Address

Collector address.

Syntax:

```
sflow collector-address [ receiver <rcvr_idx_list> ] [ <ipv4_var> | <ipv6_var> | <domain_name> ]
```

<domain_name>: Domain name identifying the collector receiver

<ipv4_addr>: IPv4 address identifying the collector receiver

<ipv6_ucast>: IPv6 address identifying the collector receiver.

Collector-Port

Collector UDP port.

```
sflow collector-port [ receiver <rcvr_idx_list> ] <collector_port>
```

<1-65535>: Port number.

Max-Datagram-Size

Maximum datagram size.

Syntax:

```
sflow max-datagram-size [ receiver <rcvr_idx_list> ] <datagram_size>
```

<200-1468>: bytes.

Timeout

Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults.

Syntax:

```
sflow timeout [ receiver <rcvr_idx_list> ] <timeout>
```

<0-2147483647>: Number of seconds.

2.3.47 SNMP-Server

Set SNMP server's configurations (enable the SNMP server).

Syntax:

```
snmp-server
```

2.3.47.1 SNMP-Server SNMP Access

Set SNMP access configuration.

Syntax:

```
snmp-server access <group_name> model { v1 | v2c | v3 | any }
level { auth | noauth | priv } [ read <view_name> ] [ write
<write_name> ]
```

<group_name>: group name, value can be 1 to 32 characters

model: set the security model, values are:

any: any security model
v1: v1 security model
v2c: v2c security model
v3: v3 security model

level: set the level, values are:

auth: authNoPriv Security Level
noauth: noAuthNoPriv Security Level
priv: authPriv Security Level

<view_name>: view name, value can be 1 to 255 characters (read)

<write_name>: write name, value can be 1 to 255 characters (write)

2.3.47.2 SNMP-Server Community SNMP v2c

Set the SNMP community (SNMPv2c) configuration.

Syntax:

```
snmp-server community v2c <comm> [ ro | rw ]
```

<comm>: community name, value can be 1 to 255 characters

ro: read only

rw: read write

2.3.47.3 SNMP-Server Community SNMP v3

Set the SNMP community (SNMPv3) configuration.

Syntax:

```
snmp-server community v3 <v3_comm> [ <v_ipv4_addr> <v_ipv4_netmask> ]
```

<v3_comm>: community name, value can be 1 to 127 characters

<v_ipv4_addr>: IPv4 address

2.3.47.4 SNMP-Server Contact

Set the SNMP server's contact string.

```
snmp-server contact <v_line255>
```

<v_line255>: contact string, value can be from 1 to 255 characters

2.3.47.5 SNMP-Server Engine-Id Local

Set SNMP local engine ID.

Syntax:

```
snmp-server engine-id local <engineID>
```

<word10-64>: local engine ID.

2.3.47.6 SNMP-Server Host

Set SNMP host's configurations.

Syntax:

```
snmp-server host <conf_name>
```

<word32>: Name of the host configuration.

Example:

Input:

```
8MG(config)# snmp-server host 8MG_host
```

Output:

```
8MG(config-snmps-host)#
```

The following option are available from the SNMP host:

do:	to run exec commands in config mode
end:	go back to EXEC mode
exit:	exit from current mode
help:	description of the interactive help system
host:	host configuration
informs:	send Inform messages to this host
no:	negate a command or set its defaults
shutdown:	disable the trap configuration
traps:	trap event configuration
version:	set SNMP trap version

2.3.47.7 SNMP-Server Host Commands**(SNMP-Server Host) Informs**

Send Inform messages to this host.

Syntax:

```
informs retries <retries> timeout <timeout>
```

<retries>: number of times to retry sending inform message,
value can be from 0 to 255

<timeout>: timeout interval, value can be from 0 to 2,147 seconds

(SNMP-Server Host) Traps

Set the trap event configuration.

Syntax:

```
traps [ aaa authentication ] [ system [ coldstart ] [ warmstart ] ]
[ switch [ stp ] [ rmon ] ]
```

aaa: AAA event group

system: system event group

coldstart: cold start event

warmstart: warm start event

switch: switch event group

rmon: RMON event

stp: STP event

system: System event group

(SNMP-Server Host) Version

Set SNMP trap version.

Syntax:

```
version { v1 [ <v1_comm> ] | v2 [ <v2_comm> ] |
v3 [ probe | engineID <v_word10_to_32> ] [ <securtyname> ] }
```

v1: SNMP trap version 1

[<v1_comm>]: community name, value can be 1 to 127 characters

v2: SNMP trap version 2

[<v2_comm>]: community name, value can be 1 to 127 characters

v3: SNMP trap version 3

engineID: configure trap server's engine ID

probe: probe trap server's engine ID

2.3.47.8 SNMP-Server Location

Set the SNMP server's location string.

Syntax:

```
snmp-server location <v_line255>
```

<v_line255>: location string, value can be 1 to 255 characters

2.3.47.9 SNMP-Server Security-to-group

Set security-to-group configuration.

Syntax:

```
snmp-server security-to-group model { v1 | v2c | v3 } name
<security_name> group <group_name>
```

model: set the security model, values are:

v1: v1 security model

v2c: v2c security model

v3: v3 security model

<security_name>: security group, value can be 1 to 32 characters
 <group_name>: group name, value can be 1 to 32 characters

2.3.47.10 SNMP-Server Trap

Set trap's configurations (enable the SNMP server traps).

Syntax:

```
snmp-server trap
```

2.3.47.11 SNMP-Server User

Set the SNMPv3 user's configurations.

Syntax:

```
snmp-server user <username> engine-id <engineID> [ { md5 <md5_passwd>  
| sha <sha_passwd> } [ priv { des | aes } <priv_passwd> ] ]
```

<username>: user name, value can be 1 to 32 characters

<engineID>: engine identifier, value can be 10 to 32 characters

md5: set MD5 protocol

<md5_passwd> md5 protocol password, value can be 8 to 32 characters

sha: set SHA protocol

<sha_passwd> sha protocol password, value can be 8 to 40 characters

[priv { des | aes } <priv_passwd>:

priv: set Privacy

aes: Set AES protocol

des: Set DES protocol

<priv_passwd>: set privacy password, value can be 8 to 32 characters

2.3.47.12 SNMP-Server Version

Set the SNMP server's version.

Syntax:

```
snmp-server version { v1 | v2c | v3 }
```

v1: SNMPv1

v2c: SNMPv2c

v3: SNMPv3

2.3.47.13 SNMP-Server View

MIB view configuration

Syntax:

```
snmp-server view <view_name> <oid_subtree> { include | exclude }
```

<view_name>: MIB view name, value can be up to 32 characters

<oid_subtree>: MIB view OID, value can be up to 255 characters
 exclude: excluded type from the view
 include: included type from the view

2.3.48 Spanning-tree

Spanning Tree protocol.

Aggregation

Aggregation mode.

Syntax:

```
spanning-tree aggregation
```

Adge

Edge ports.

Syntax:

```
spanning-tree edge bpdu-filter
spanning-tree edge bpdu-guard
```

Mode

STP protocol mode.

Syntax:

```
spanning-tree mode { stp | rstp | mstp }
```

mstp: Multiple Spanning Tree (802.1s)

rstp: Rapid Spanning Tree (802.1w)

stp: 802.1D Spanning Tree

Mst

STP bridge instance.

Syntax:

```
spanning-tree mst <instance> priority <prio>
spanning-tree mst <instance> vlan <v_vlan_list>
spanning-tree mst forward-time <fwdtime>
spanning-tree mst hello-time <hellotime>
spanning-tree mst max-age <maxage> [ forward-time <fwdtime> ]
spanning-tree mst max-hops <maxhops>
spanning-tree mst name <name> revision <v_0_to_65535>
```

<0-7>: instance 0-7 (CIST=0, MST2=1...)

forward-time: Delay between port states
 <4-30>: Range in seconds.

hello-time: MSTP bridge hello time
 <1-10>: Hello BPDU timer value.

max-age: Max bridge age before timeout
 <6-40>: Range in seconds.

max-hops: MSTP bridge max hop count
 <6-40>: Hop count range.

name: Name keyword
 <word32>: Name of the bridge.

priority: <0-61440>: Range in seconds.

<vlan_list>: Range of VLANs.

Recovery

The error recovery timeout.

Syntax:

```
spanning-tree recovery interval <interval>
```

interval:

<30-86400>: Range in seconds.

Transmit

BPDUs to transmit.

Syntax:

```
spanning-tree transmit hold-count <holdcount>
```

hold-count: Max number of transmit BPDUs per sec

<1-10>: 1-10 per sec, 6 is default.

2.3.49 Switchport

Set switching mode characteristics.

Syntax:

```
switchport vlan mapping <gid> <vlan_list> <tvid>
```

vlan mapping: Add VLAN translation entry into a group.

<1-8>: Group id.

2.3.50 Tacacs-server

Configure TACACS+

Syntax:

```
tacacs-server deadtime <minutes>
```

```
tacacs-server host <host_name> [ port <port> ] [ timeout <seconds> ] [ key <key> ]
```

```
tacacs-server key <key>
```

```
tacacs-server timeout <seconds>
```

deadtime: Time to stop using a TACACS+ server that doesn't respond

<1-1440>: Time in minutes.

host: Specify a TACACS+ server

<word1-255>: Hostname or IP address.

key: Set TACACS+ encryption key

<line1-63>: The shared key.
 timeout: Time to wait for a TACACS+ server to reply
 <1-1000>: Wait time in seconds.

2.3.51 thermal-protect

Thermal protection configurations.

Syntax:

```
thermal-protect grp <grp_list> temperature <new_temp>
```

grp:

<0~3>: group number.

temperature: temperature keyword.

<0-255>: Temperature at which to turn ports mapped to the corresponding group off.

2.3.52 UDLD

Enable UDLD in the aggressive or normal mode and to set the configurable message timer on all fiber-optic ports.

Syntax:

```
udld { aggressive | enable | message time-interval <v_interval> }
```

aggressive: Enables UDLD in aggressive mode on all fiber-optic ports.

enable: Enables UDLD in normal mode on all fiber-optic ports.

message: 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 (currently default message time interval 7 sec is supported).

2.3.53 UPnP

Set UPnP configuration.

Advertising-duration

Set advertising duration.

Syntax:

```
upnp advertising-duration <v_100_to_86400>
```

<100-86400>: advertising duration.

TTL

Set TTL value.

Syntax:

```
upnp ttl <v_1_to_255>
```

<1-255>: TTL value.

2.3.54 Username

Establish User Name Authentication.

Syntax:

```
username <username> privilege <priv> password encrypted <encry_password>
username <username> privilege <priv> password none
username <username> privilege <priv> password unencrypted <password>
```

<word31>: User name allows letters, numbers and underscores.

privilege:

<0-15>: User privilege level.

2.3.55 Vlan

VLAN commands.

Syntax:

```
vlan <vlist>
vlan ethertype s-custom-port <etype>
vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui>
| rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>
```

<vlan_list>: ISL VLAN IDs 1~4095

Ethertype: EtherType for Custom S-ports

s-custom-port:

<0x0600-0xffff>: EtherType (Range: 0x0600-0xffff).

Protocol: Protocol-based VLAN commands:

eth2: Ethernet-based VLAN commands:

<0x600-0xffff> Ether Type (Range: 0x600 - 0xFFFF)

arp: Ether Type is ARP

at: Ether Type is AppleTalk

ip: Ether Type is IP

ipx: Ether Type is IPX

llc: LLC based VLAN group

<0x0-0xff>: DSAP (Range: 0x00 - 0xFF).

snap: SNAP-based VLAN group:

rfc-1042: SNAP OUI is rfc-1042

snap-8021h: SNAP OUI is 8021h.

2.3.56 Voice

Voice appliance attributes.

Syntax:

```
voice vlan
voice vlan aging-time <aging_time>
voice vlan class { <traffic_class> | low | normal | medium | high }
```

```
voice vlan oui <oui> [ description <description> ]
voice vlan vid <vid>
aging-time: Set secure learning aging time
              <10-10000000>: Aging time, 10-10000000 seconds.
class:        Set traffic class
              <0-7>: Traffic class value.
oui:          OUI value.
vid:          Set VLAN ID
              <vlan_id>: VLAN ID, 1-4095.
```

2.3.57 Web

Syntax:

```
web privilege group <group_name> level { [ configRoPriv <configRoPriv>
] [ configRwPriv <configRwPriv> ] [ statusRoPriv <statusRoPriv> ] [
statusRwPriv <statusRwPriv> ] }*1
```

Group Privilege

<cword>: Valid words are 'Aggregation' 'DHCP' 'DHCPv6_Client' 'Debug' 'Diagnostics' 'EPS' 'ERPS' 'ETH_LINK_OAM' 'EVC' 'Green_Ethernet' 'IP' 'IPMC_Snooping' 'JSON_RPC' 'JSON_RPC_Notification' 'LACP' 'LLDP' 'Loop_Protect' 'MAC_Table' 'MEP' 'MVR' 'Maintenance' 'NTP' 'PTP' 'Ports' 'Private_VLANs' 'QoS' 'RMirror' 'Security' 'Spanning_Tree' 'System' 'UDLD' 'UPnP' 'VCL' 'VLAN_Translation' 'VLANs' 'Voice_VLAN' 'XXRP' 'sFlow'

Example:

Input: 8MG (config)# web privilege group dhcp level ?

Output:

configRoPriv	Configuration Read-only level
configRwPriv	Configuration Read-write level
statusRoPriv	Status/Statistics Read-only level
statusRwPriv	Status/Statistics Read-write level
<0-15>	

2.4 Copy

Copy one of the following source file types to a specified destination:

running-config Currently running configuration
startup-config Startup configuration

Syntax:

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

<url_file> File in FLASH or on TFTP server. Syntax: <flash:filename
| tftp://server/path-and-filename>. A valid file name is
a text string drawn from alphabet (A-Za-z), digits (0-9),
dot (.), hyphen (-), underscore (_). The maximum length
is 63 and hyphen must not be first character. The file
name content that only contains '.' is not allowed.

<source_path>/<destination_path>:

flash:filename: file in FLASH or on TFTP server

[syntax-check]: Perform syntax check on source configuration

2.5 Delete

Delete one file in flash: file system.

Syntax:

```
delete <path>
```

<path>: path and name of file to delete

<url_file> File in FLASH. Syntax: <flash:filename>. A valid file name is
a text string drawn from alphabet (A-Za-z), digits (0-9), dot
(.), hyphen (-), underscore (_). The maximum length is 63 and
hyphen must not be first character. The file name content
that only contains '.' is not allowed.

2.6 Dir

Directory of all files in flash: file system.

Syntax:

```
Dir | Output modifiers
```

Output Modifiers

begin: begin with the line that matches

exclude: exclude lines that match

include: include lines that match

LINE: string to match output lines

2.7 Disable

Turn off privileged commands.

Syntax:

```
disable [ <new_priv> ]
```

Values:

[<new_priv>]: values are <0-15>

2.8 Do

Perform an Exec Command while located in a sub-folder.

Syntax:

```
do <command>
```

2.9 Dot1x

Configure IEEE Standard for port-based Network Access Control.

Syntax:

```
dot1x initialize [ interface ( <port_type> [ <plist> ] ) ]
```

Dot1x Initialize

Force re-authentication immediately.

interface: <port_type>, values are:

*	all switches or all ports
GigabitEthernet:	set specific Gigabit Ethernet Port number
<plist>	port list in 1/1-8

2.10 Enable

Turn on privileged commands.

Syntax:

```
enable [ <new_priv> ]
```

[<new_priv>]: Privileged level, values are <0-15>

2.11 Erps

Ethernet Ring Protection Switching.

Syntax:

```
erps <group> command { force | manual | clear } { port0 | port1 }
```

1-64: ERPS group number.

2.12 Exit

Exit from EXEC mode.

Syntax:

`Exit`

2.13 Firmware

Perform a firmware upgrade or swap.

Firmware Swap

Swap between Active and Alternate firmware image.

Syntax:

`firmware swap`

Firmware Upgrade

Upgrade Firmware software with specified file.

Syntax:

`firmware upgrade <tftpserver_path_file>`

`<url_file>` Uniform Resource Locator. It is a specific character string

that constitutes a reference to a resource. Syntax:

`<protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>`

`]/<file_name>`

If the following special characters: space

`!"#$%&'()*+,-./:;<=>?@[\\]^_{|}~` need to be contained in the

input URL string, they should be percent-encoded. A valid

file name is a text string drawn from alphabet (A-Za-z),

digits (0-9), dot (.), hyphen (-), underscore (_). The

maximum length is 63 and hyphen must not be first character.

The file name content that only contains '.' is not allowed.

2.14 Help

Description of the interactive help system

Syntax:

`help`

2.15 IP

Set IPv4 commands.

Syntax:

```
ip dhcp retry interface vlan <vlan_id>
```

dhcp: Dynamic Host Configuration Protocol (DHCP) commands

retry: restart the DHCP query process

interface: interface

vlan: Vlan interface

<vlan_id>: Vlan ID

2.16 **Ipv6**

IPv6 configuration commands.

Syntax:

```
ipv6 dhcp-client restart [ interface vlan <v_vlan_list> ]
```

dhcp-client: Manage DHCPv6 client service.

Restart: Restart DHCPv6 client service.

Interface: Select an interface to configure.

Vlan: VLAN of IPv6 interface.

<vlan_list>: IPv6 interface VLAN list.

2.17 **Link-OAM**

Link OAM configuration.

Syntax:

```
link-oam remote-loopback { start | stop } interface ( <port_type> [ <v_port_type_list> ] )
```

remote-loopback: Configure remote loopback on interface.

Start: Start remote loopback test on interface.

Stop: Stop remote loopback test on interface.

Interface: Start/Stop remote loopback test on a specific interface or interfaces.

*	All switches or All ports
	<port_type_list> Port list for all port types.
GigabitEthernet	1 Gigabit Ethernet Port
	<port_type_list> Port list in 1/1-8.

2.18 **Logout**

Exit from EXEC mode.

Syntax:

logout

2.19 More

Display a file in FLASH or on TFTP server.

Syntax:

more <path>

<Path>: Path to file in FLASH or on TFTP server

2.20 No

Negate a command or set its defaults.

No debug

Debugging functions.

Syntax:

no debug interrupt-monitor source <source>

no debug ipv6 nd

no debug trace hunt

interrupt-monitor: Print out of reception of the selected interrupt source.

ipv6: IPv6 configuration commands trace.

No port-security

Port security (MAC limiter).

Syntax:

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

shutdown: Reopen one or more ports whose limit is exceeded and shut do.

Interface:

* All switches or All ports

GigabitEthernet 1 Gigabit Ethernet Port

<port_type_list> Port list in 1/1-8.

No PTP

Misc non persistent 1588 settings.

Syntax:

no ptp <clockinst> wireless mode interface (<port_type> [<v_port_type_list>])

<0-3>: Clock instance [0-3].

No terminal

Set terminal line parameters.

Syntax:


```
no terminal editing
no terminal exec-timeout
no terminal history size
no terminal length
no terminal width
```

editing: Enable command line editing
exec-timeout: Set the EXEC timeout
history: Control the command history function
length: Set number of lines on a screen
width: Set width of the display terminal

2.21 Ping

Send ICMP echo messages.

IP

IP (ICMP) echo.

Syntax:

```
ping ip { <v_ip_addr> | <v_ip_name> } [ repeat <count> ] [ size <size>
] [ interval <seconds> ]
```

<domain_name>: ICMP destination IP domain name.

<ipv4_addr>: ICMP destination IPv4 address.

IPv6

IPv6 (ICMPv6) echo.

Syntax:

```
ping ipv6 { <v_ipv6_addr> | <v_ipv6_name> } [ repeat <count> ] [ size
<size> ] [ interval <seconds> ] [ interface vlan <v_vlan_id> ]
```

<domain_name>: ICMPv6 destination IP domain name.

<ipv6_addr>: ICMPv6 destination IPv6 address.

2.22 Platform

Platform configuration.

Syntax:

```
platform debug { allow | deny }
```

debug: Debug command setting.

Allow: Allow debug commands.

Deny: Deny debug commands.

2.23 PTP

Misc non persistent 1588 settings.

Syntax:

```
ptp <clockinst> local-clock { update | ratio <ratio> }
ptp <clockinst> wireless delay <base_delay> [ <incr_delay> ] interface
( <port_type> [ <v_port_type_list> ] )
ptp <clockinst> wireless mode interface ( <port_type> [
<v_port_type_list> ] )
ptp <clockinst> wireless pre-notification interface ( <port_type> [
<v_port_type_list> ] )
```

<0-3>: PTP Clock instance [0-3].

2.24 Reload

Reload system.

Syntax:

```
reload { { { cold | warm } [ sid <usid> ] } | { defaults [ keep-ip ] }
}
```

reload options:

cold: reload cold

defaults: reload defaults without rebooting

2.25 Send

Send a message to other tty lines.

Syntax:

```
send { * | <session_list> | console 0 | vty <vty_list> } <message>
```

* All tty lines

<0~16>: send a message to multiple lines

console: primary terminal line

vty: virtual terminal

The message text is delimited by a user defined character:

c message-text c, where 'c' is a delimiting character and "message-text" is the message.

Example:

Input:

```
8MG (config)# send x Hello. x<CR> (the delimiter is "x")
```

2.26 Show

Show running system information.

Show Commands (a-c)

```
show aaa
show access management [ statistics | <access_id_list> ]
show access-list [ interface ( ( <port_type> [ <v_port_type_list> ] ) ) ] [ rate-limiter [ <rate_limiter_list> ] ] [ ace statistics [ <ace_list> ] ]
show access-list ace-status [ static ] [ link-oam ] [ loop-protect ] [ dhcp ] [ ptp ] [ upnp ] [ arp-inspection ] [ evc ] [ mep ] [ ipmc ] [ ip-source-guard ] [ ip-mgmt ] [ tt-loop ] [ y1564 ] [ ztp ] [ conflicts ] [ switch <switch_list> ]
show aggregation [ mode ]
show clock
show clock detail
```

Show Dot1x-e Commands

```
show dot1x statistics { eapol | radius | all } [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show dot1x status [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ brief ]
show eps [ <inst> ] [ detail ]
show erps { [ <groups> ] } [ detail | statistics ]
show evc statistics { [ <evc_id> | all ] } [ ece [ <ece_id> ] ] [ interface ( <port_type> [ <port_list> ] ) ] [ pw <pw_num_list> ] [ cos <cos> ] [ green | yellow | red | discard ] [ frames | bytes ]
show evc { [ <evc_id> | all ] } [ ece [ <ece_id> ] ]
```

Show Green-Ethernet Commands

```
show green-ethernet [ interface ( <port_type> [ <port_list> ] ) ]
show green-ethernet eee [ interface ( <port_type> [ <port_list> ] ) ]
show green-ethernet energy-detect [ interface ( <port_type> [ <port_list> ] ) ]
show green-ethernet short-reach [ interface ( <port_type> [ <port_list> ] ) ]
show history
```

Show Interface Commands

```
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> ] ) description
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 IP-IPV6 Commands

```

show ip arp
show ip arp inspection [ interface ( <port_type> [ <in_port_type_list>
] ) | vlan <in_vlan_list> ]
show ip arp inspection entry [ dhcp-snooping | static ] [ interface (
<port_type> [ <in_port_type_list> ] ) ]
show ip dhcp detailed statistics { server | client | snooping | relay
| normal-forward | combined } [ interface ( <port_type> [
<in_port_list> ] ) ]
show ip dhcp excluded-address
show ip dhcp pool [ <pool_name> ]
show ip dhcp relay [ statistics ]
show ip dhcp server
show ip dhcp server binding <ip>
show ip dhcp server binding [ state { allocated | committed | expired
} ] [ type { automatic | manual | expired } ]
show ip dhcp server declined-ip
show ip dhcp server declined-ip <declined_ip>
show ip dhcp server statistics
show ip dhcp snooping [ interface ( <port_type> [ <in_port_list> ] ) ]
show ip dhcp snooping table
show ip domain
show ip http server secure status
show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [
interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ]
] [ detail ]
show ip igmp snooping mrouter [ detail ]
show ip interface brief
show ip name-server
show ip route
show ip source binding [ dhcp-snooping | static ] [ interface (
<port_type> [ <in_port_type_list> ] ) ]
show ip ssh
show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp
] [ icmp-msg <type> ]
show ip verify source [ interface ( <port_type> [ <in_port_type_list>
] ) ]
show ipmc profile [ <profile_name> ] [ detail ]
show ipmc range [ <entry_name> ]
show ipv6 dhcp-client [ interface vlan <v_vlan_list> ]
show ipv6 interface [ vlan <v_vlan_list> { brief | statistics } ]
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 neighbor [ interface vlan <v_vlan_list> ]
show ipv6 route
show ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [
icmp ] [ icmp-msg <type> ]

```

Show Commands (l-n)

```

show lacp { internal | statistics | system-id | neighbor }
show line [ alive ]
show link-oam { [ status ] [ link-monitor ] [ statistics ] } [
interface ( <port_type> [ <plist> ] ) ]
show lldp eee [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show lldp med media-vlan-policy [ <v_0_to_31> ]
show lldp med remote-device [ interface ( <port_type> [ <port_list> ]
) ]
show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] )
]
show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ]
) ]
show logging <log_id> [ switch <switch_list> ]
show logging [ informational ] [ notice ] [ warning ] [ error ] [
switch <switch_list> ]
show loop-protect [ interface ( <port_type> [ <plist> ] ) ]
show mac address-table [ conf | static | aging-time | { { learning |
count } [ interface ( <port_type> [ <v_port_type_list> ] ) | vlan
<v_vlan_id_2> ] } | { address <v_mac_addr> [ vlan <v_vlan_id> ] } |
vlan <v_vlan_id_1> | interface ( <port_type> [ <v_port_type_list_1> ]
) ]
show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps |
client | ais | lck | pm | syslog | tlv | bfd | rt | lst | lm-avail ] [
lm-hli ] [ detail ]
show monitor [ session { <session_number> | all | remote } ]
show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [
interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ]
] [ detail ]
show network-clock
show network-clock clock-selection-config
show network-clock port-config
show network-clock port-status
show network-clock ptp-ports
show network-clock source-nomination-config
show network-clock station-clock-config
show network-clock synchronization
show ntp status

```

Show Platform Commands

```

show platform debug
show platform phy [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show platform phy id [ interface ( <port_type> [ <v_port_type_list> ]
) ]
show platform phy instance

```

Show Commands (p-r)

```

show port-security port [ interface ( <port_type> [ <v_port_type_list>
] ) ]
show port-security switch [ interface ( <port_type> [
<v_port_type_list> ] ) ]

```

```

show privilege
show process list [ detail ]
show process load
show ptp <clockinst> local-clock
show ptp <clockinst> slave-cfg
show ptp <clockinst> slave-table-unicast
show ptp <clockinst> { default | current | parent | time-property |
filter | servo | servo-extended | clk | ho | uni | master-table-
unicast | slave | { { port-state | port-ds | wireless | foreign-
master-record } [ interface ( <port_type> [ <v_port_type_list> ] ) ] }
}
show ptp ext
show ptp servo best-master
show ptp system-time
show pvlan [ <pvlan_list> ]
show pvlan isolation [ interface ( <port_type> [ <plist> ] ) ]
show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | {
maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [
cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
show radius-server [ statistics ]
show rmon alarm [ <id_list> ]
show rmon event [ <id_list> ]
show rmon history [ <id_list> ]
show rmon statistics [ <id_list> ]

```

Show Running-Config Commands

```

show running-config [ all-defaults ]
show running-config feature <feature_name> [ all-defaults ]
show running-config interface ( <port_type> [ <list> ] ) [ all-
defaults ]
show running-config interface vlan <list> [ all-defaults ]
show running-config line { console | vty } <list> [ all-defaults ]
show running-config vlan { [ <vlan_list> ] } [ all-defaults ]

```

Show sFLOW-web Commands

```

show sflow
show sflow statistics { receiver [ <rcvr_idx_list> ] | samplers [
interface [ <samplers_list> ] ( <port_type> [ <v_port_type_list> ] ) ]
}
show snmp
show snmp access [ <group_name> { v1 | v2c | v3 | any } { auth |
noauth | priv } ]
show snmp community v3 [ <community> ]
show snmp host [ <conf_name> ] [ system ] [ switch ] [ interface ] [
aaa ]
show snmp mib context
show snmp mib ifmib ifIndex
show snmp security-to-group [ { v1 | v2c | v3 } <security_name> ]
show snmp user [ <username> <engineID> ]
show snmp view [ <view_name> <oid_subtree> ]

```

```

show spanning-tree [ summary | active | { interface ( <port_type> [
<v_port_type_list> ] ) } | { detailed [ interface ( <port_type> [
<v_port_type_list_1> ] ) ] } | { mst [ configuration | { <instance> [
interface ( <port_type> [ <v_port_type_list_2> ] ) ] } ] } ] ]
show switchport forbidden [ { vlan <vlan_list> } | { name <name> } ]
show system cpu status
show system led status
show tacacs-server
show terminal
show thermal-protect [ interface ( <port_type> [ <port_list> ] ) ]
show uddl [ interface ( <port_type> [ <plist> ] ) ]
show upnp
show user-privilege
show users [ myself ]
show version [ brief ]
show vlan [ id <vlan_list> | name <name> | brief ] [ all ]
show vlan ip-subnet [ <ipv4> ]
show vlan mac [ address <mac_addr> ]
show vlan protocol [ eth2 { <etype> | arp | ip | ipx | at } ] [ snap {
<oui> | rfc-1042 | snap-8021h } <pid> ] [ llc <dsap> <ssap> ]
show vlan status [ interface ( <port_type> [ <plist> ] ) ] [ admin |
all | combined | conflicts | erps | evc | gvrp | mep | mstp | mvr |
nas | rmirror | vcl | voice-vlan ]
show voice vlan [ oui <oui> | interface ( <port_type> [ <port_list> ]
) ]
show web privilege group [ <group_name> ] level

```

2.27 Terminal

Editing

Enable command line editing.

Syntax:

```
terminal editing
```

Exec-timeout

Set the EXEC timeout.

Syntax:

```
terminal exec-timeout <min> [ <sec> ]
```

<min>: timeout in minutes, values are <0-1440>

Help

Display a description of the interactive help system.

Syntax:

```
help
```

History

Control the command history function.

Syntax:

```
terminal history size <history_size>
```

history size:

<0-32>: Number of history commands, 0 means disable.

Length

Set the number of lines on a screen.

Syntax:

```
terminal length <lines>
```

<lines>: number of lines on screen (0 for no pausing), values are: 0 or 3-512

Width

Set the width of the display terminal.

Syntax:

```
terminal width <width>
```

<width>: Number of characters on a screen line (0 for unlimited width),
values are: 0 or 40-512

2.28 Veriphy

VeriPHY keyword.

Syntax:

```
veriphy [ { interface ( <port_type> [ <v_port_type_list> ] ) } ]
```

interface:

*	All switches or All ports
	<port_type_list> Port list for all port types.
GigabitEthernet	1 Gigabit Ethernet Port
	<port_type_list> Port list in 1/1-8.

2.29 Factory Default Configuration

The factory default configuration is a VLAN unaware L2 switch with automatic learning/ageing and auto negotiation enabled on all ports:

- **System:** The system name string is 8MG.
- **Console:** The password string is empty and inactivity timeout is disabled. The prompt is ">".
- **Port:** All ports are enabled for auto negotiation and flow control is disabled. Max frame size is 1518.
- **MAC Table:**
 - ◆ The table is empty

- ◆ Auto learning and ageing are enabled
- ◆ The ageing timer is 300 seconds
- **VLAN:**
 - ◆ Only VLAN 1 is present in the table and includes all ports
 - ◆ All ports are VLAN unaware with Port VLAN ID 1
 - ◆ All ports accept all frame types
- **Aggregation:** No ports are aggregated, but aggregation mode is set to XOR.
- **LACP:** No ports have LACP enabled.
- **RSTP:** No ports and no aggregations have RSTP enabled
- **User Groups:** User group 1 exists and includes all ports.
- **QoS:**
 - ◆ IP ToS Precedence priority is enabled and all Precedence values are given high priority
 - ◆ VLAN tag priorities will be set according to 802.1p
 - ◆ The UDP/TCP port list is empty
 - ◆ Default priority is high
 - ◆ Default user priority is 0
 - ◆ L4 default priority and match priority are low
 - ◆ All shaper and policers are disabled
- **Mirror:** Mirroring is disabled.
- **IP:**
 - ◆ IP address is 192.168.1.111
 - ◆ Mask: 255.255.255.0
 - ◆ Gateway:
 - ◆ Web interface is enabled.
 - ◆ DHCP mode is disabled.
- **SNMP:** SNMP is enabled. Traps are disabled.
- **Dot1X:** 802.1X is disabled. All ports set to "Force Authorized"
- **IGMP Snooping:** Disabled in each defined VLAN

3 Web Interface - Introduction

From the Web Interface the user can manage the following aspects of the switch:

- Customize configurations and status monitoring
- Perform diagnostics and maintenance procedures

3.1 Web Interface – Configuration

Below is a list of some of the configurations that may be done using the Web interface:

- IP interfaces and routes
- SNTP mode and server address
- Log mode, address, and level
- Green Ethernet configurations for power savings
- Thermal Protection
- Port Configurations
- Security settings
- Aggregation settings
- Loop Protection settings
- Spanning Tree Protocol (STP) settings
- IPMC (Intelligent Platform Management Controller) snooping configurations
- LLDP () configurations
- MAC table configurations
- VLAN configurations
- QoS (Quality of Service) configurations
- Mirror Configurations

3.2 Web Interface – Monitoring

Below is a list of some of the monitoring that may be done using the Web interface:

- System information
 - ◆ CPU load
 - ◆ IP status
 - ◆ System Logs
- Green Ethernet power savings
- Thermal Protection status

- Ports
 - ◆ State
 - ◆ Traffic
 - ◆ QoS Statistics
 - ◆ Detailed Statistics
- Security
- Loop Protection
- Spanning Tree Protocol
- IPMC – IGMP snooping
- MVR
- LLDP
- VLAN

3.3 Web Interface – Diagnostics

Below is a list of some of the diagnostics that may be done using the Web interface:

- Ping to troubleshoot connectivity
- VeriPHY to perform cable diagnostics

3.4 Web Interface – Maintenance

Below is a list of some of the maintenance that may be done using the Web interface:

- Restart the device
- Reset the device to factory defaults
- Upload software
- Save and download configuration files

3.5 Web Interface – Getting Started

All operations are password protected. The password must be entered at login. It is the password as the one used in the command line interface.

The Web interface is enabled in the factory before delivery.

- Default IP address: 192.168.1.111
- Default Subnet Mask: 255.255.255.0
- Default User Name: admin

- Default Password: <empty>

You may restart the Dynamic Host Configuration Protocol (DHCP) query process, if your environment includes a DHCP server.

Example input:

```
8MG# ip dhcp retry interface vlan 1
```

Open the Web Interface

To open the Web Interface:

1. Open a Web browser
2. Enter the IP address in the browser address bar (default is 192.168.1.111)
3. Press enter

The login window pops up.

3.6 Web Interface – Login Window

Enter the User name* and Password**, and then click **OK** to login.

* The user name string is “admin” by default.

** The password string is empty by default.



The Web Interface opens with the available menu options on the left side of the screen.

4 Web Interface - Configuration

The Web Interface – Configuration section of this manual describes how to configure the Switch, using the User Interface. Not all configurations are supported via the WEB interface; some configurations may be done strictly from the CLI.

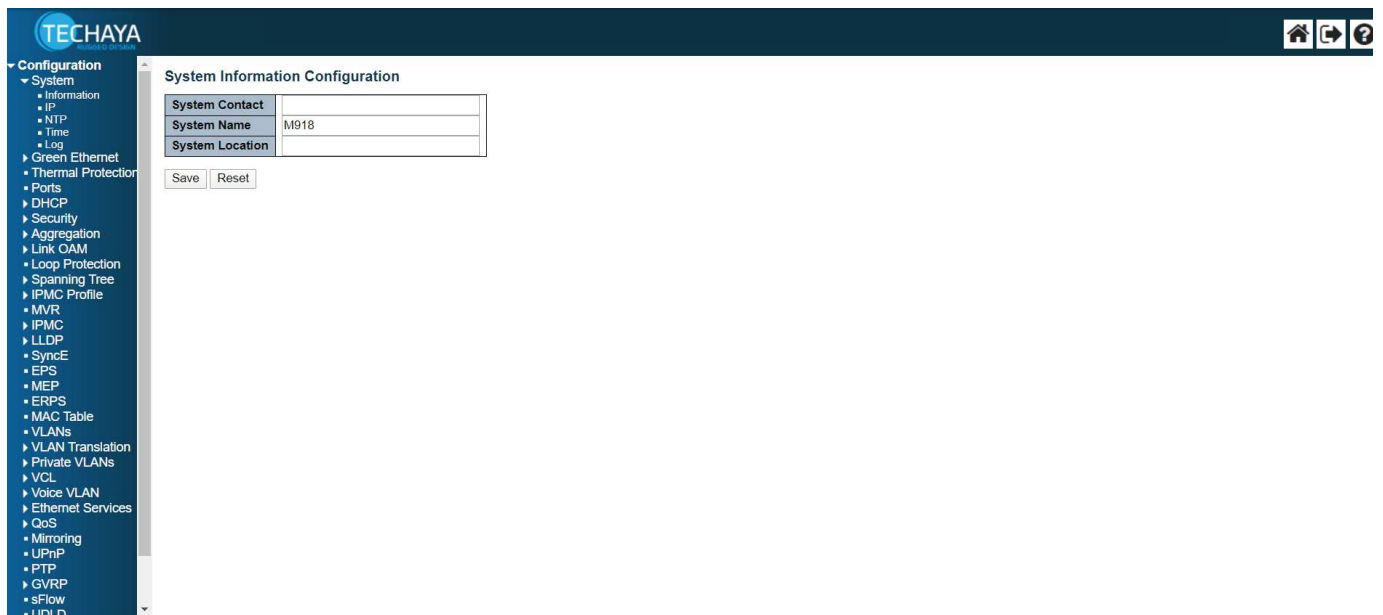
4.1 System Information Configuration

The System Information Configuration page displays and allows updates to the following system details:

- System Contact
- System Name
- System Location

Click **Save** to save all changes.

Click **Reset** to undo any changes made locally and revert to previously saved values.



4.2 System – IP

IP Configuration

The IP Configuration includes IP basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

TECHAYA

Configuration

- System
 - Information
 - IP
 - NTP
 - Time
 - Log
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD

IP Configuration

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		DHCPv6			IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
☐	1	☐	0		192.168.1.111	24	☐	☐			

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN

Add Route

Save Reset

Mode

Configure 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.

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.

System selects the active DNS server from configuration in turn, if the preferred server does not respond in five attempts.

The following modes are supported:

- From any DHCPv4 interfaces - The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.
- 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.

- From this DHCPv4 interface - Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.
- 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 this DHCPv6 interface - Specify from which DHCPv6-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.

DNS Proxy

When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.

Only IPv4 DNS proxy is now supported.

4.2.1

IP Interfaces

Each IP Interface has the following configurable parameters:

Delete

Select this option to delete an existing IP interface.

VLAN

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.

IPv4 DHCP - Enable

- ☒ Enable the DHCP client
- ☐ Disable (default: Disable)

If this option is enabled, the system will configure the IPv4 address and mask of the interface using the Dynamic Host Configuration Protocol (DHCP) protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

IPv4 DHCP - Fallback

The Fallback is the time limit in 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 the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

IPv4 DHCP - Current Lease

For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv4 - Address

Set or show the IPv4 address of the interface in dotted decimal notation.

If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

IPv4 - Mask Length

Set or show the IPv4 network mask, in number of bits (*prefix length*). Valid values are between 0 and 30 bits for an IPv4 address.

If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

DHCPv6 Enable

Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.

DHCPv6 Rapid Commit

Enable the DHCPv6 Rapid-Commit option by checking this box. 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.

DHCPv6 Current Lease

For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.

IPv6 Address

The IPv6 address of the interface. A 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.

System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address.

The field may be left blank if IPv6 operation on the interface is not desired.

IPv6 Mask

The IPv6 network mask, in number of bits (*prefix length*). Valid values are between 1 and 128 bits for a IPv6 address.

The field may be left blank if IPv6 operation on the interface is not desired.

Resolving IPv6 DAD

The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address Detection) detects the address duplication, the operation on the interface SHOULD be disabled.

At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN.

After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface.

4.2.2 IP Routes

Each IP Route has the following configurable parameters:

Delete

Select this option to delete an existing IP route.

Network

Set or show 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 IPv6 notation.

Mask Length

Set or show the 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

Set or show the IP address of the IP 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 (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4094 and 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, system ignores the next hop VLAN for the gateway.

4.2.3 IP Configuration Buttons

Add Interface: Click to add a new IP Interface. A new row opens in the IP Interfaces table. The maximum number of interfaces supported is 8.

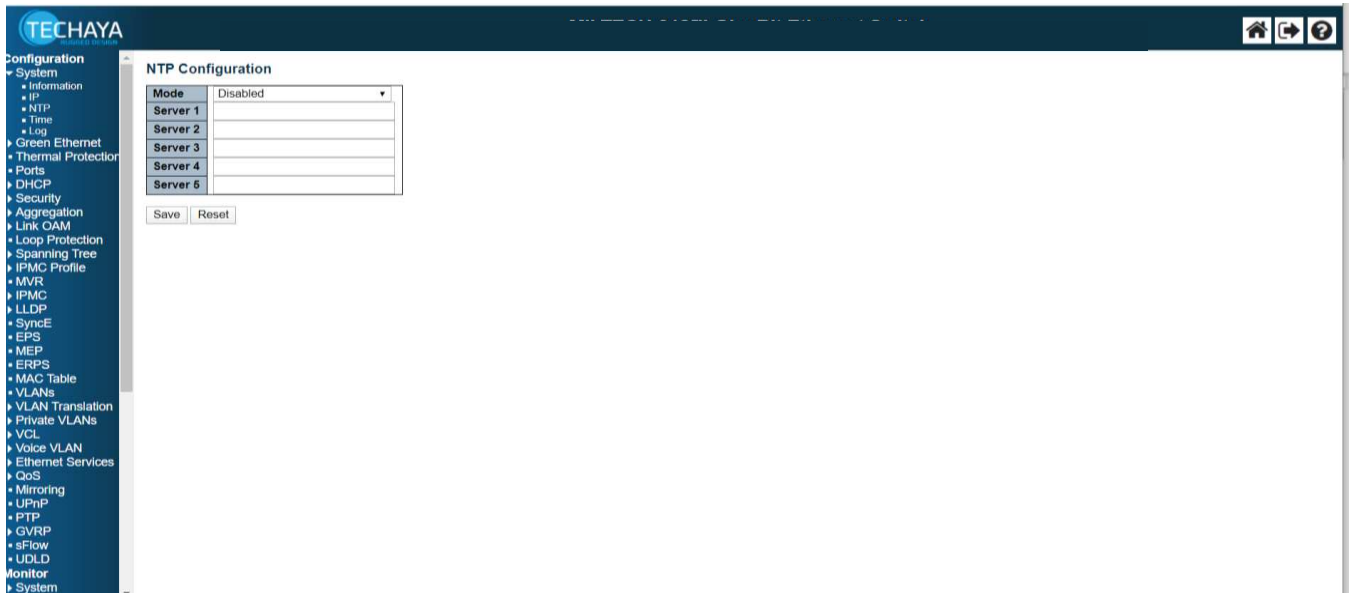
Add Route: Click to add a new IP Route. A new row opens in the IP Routes table. The maximum number of routes is 32.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3 System – NTP

Use the NTP page to configure NTP.



4.3.1 NTP Configuration

Mode

Each Indicates the NTP mode operation. Possible modes are:

Enabled: Enable NTP client mode operation.

Disabled: Disable NTP client mode operation.

Server

Provide the IPv4 or IPv6 address of a 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. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'. In addition, it can also accept a domain name address.

4.3.2 NTP Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.4 System - Time

This page allows you to configure the Time Zone.

4.4.1 Time Zone Configuration

Time zone

Lists various Time Zones world-wide. Select appropriate Time Zone from the drop down and click Save to set.

Acronym

User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 characters).

4.4.2 Daylight Saving Time

This page is used to setup Daylight Saving Time Configuration.

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 : Disabled).

4.4.2.1 Recurring Configurations

Start time settings

Week: Select the starting week number.

Day: Select the starting day.

Month: Select the starting month.

Hours: Select the starting hour.

Minutes: Select the starting minute.

End time settings

Week: Select the ending week number.

Day: Select the ending day.

Month: Select the ending month.

Hours: Select the ending hour.

Minutes: Select the ending minute.

Offset settings

Offset: Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440).

4.4.2.2 Non Recurring Configurations

Start time settings

Week: Select the starting week number.

Day: Select the starting day.

Month: Select the starting month.

Hours: Select the starting hour.

Minutes: Select the starting minute.

End time settings

Week: Select the ending week number.

Day: Select the ending day.

Month: Select the ending month.

Hours: Select the ending hour.

Minutes: Select the ending minute.

Offset settings

Offset: Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440).

4.4.3 Time Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previous values.

4.5 System - Log

System Log Configuration

Use the System Log Configuration page to configure System Log.

The screenshot shows the TECHAYA web interface. On the left is a navigation sidebar with a tree view under 'Configuration' including System, Green Ethernet, Ports, DHCP, Security, Aggregation, Link OAM, Loop Protection, Spanning Tree, IPMC Profile, MVR, IPMC, LLDP, SyncE, EPS, MEP, ERPS, MAC Table, VLANs, VLAN Translation, Private VLANs, VCL, Voice VLAN, Ethernet Services, QoS, Mirroring, URnP, PTP, GVRP, sFlow, UDLD, and Monitor. The main panel is titled 'System Log Configuration' and contains a form with three rows: 'Server Mode' with a dropdown menu showing 'Disabled', 'Server Address' with an empty text input field, and 'Syslog Level' with a dropdown menu showing 'Informational'. At the bottom of the form are 'Save' and 'Reset' buttons.

4.5.1 System Log Configuration

Server Mode

Indicates the server mode operation:

Enabled: Enable server mode operation

Disabled: Disable server mode operation

When the server mode is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and is received on UDP port 514. The syslog server will not send acknowledgments back to 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.

Server Address

Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.

Syslog Level

Indicates the message type to send to syslog server:

Error: Send the specific messages which severity code is less or equal than Error(3).

Warning: Send the specific messages which severity code is less or equal than Warning(4).

Notice: Send the specific messages which severity code is less or equal than Notice(5).

Informational: Send the specific messages which severity code is less or equal than Informational(6).

4.5.2 Log Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previous values.

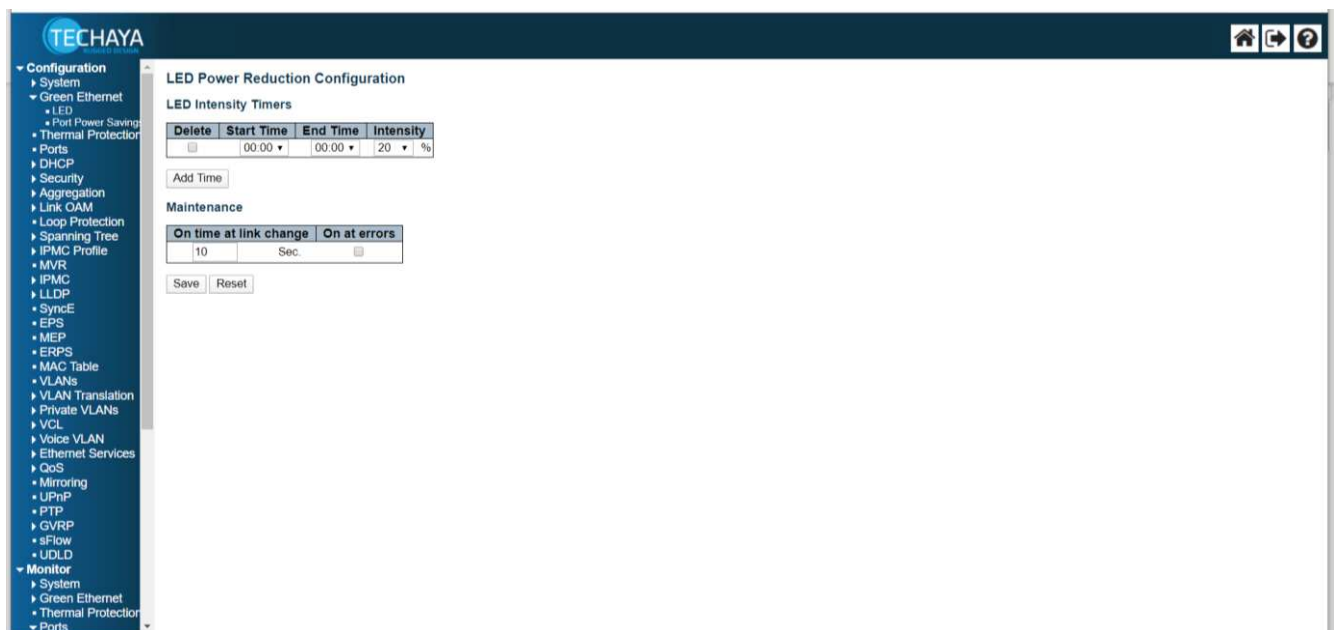
4.6 Green Ethernet – LED

LEDs

4.6.1 Status LED

The system status LED shows whether the system is running. The LED is green when system is running and no errors are detected. If errors has been detected the status LED will indicate this by blinking red.

The LEDs power consumption can be reduced by lowering the LEDs intensity.



4.6.2 Front Ethernet Port LEDs

The front Ethernet ports have a dual color LEDs per port. The port LEDs is placed in a block (1-high for SFPs, 2-high for RJ45s) to the left of the ports.

A pushbutton and a 4-high tower of LEDs is placed next to the front ethernet port LEDs. The pushbutton selects between four different port LED modes, indicated by the 4-high LED mode tower. After 30 seconds the LED mode falls back to mode A. The port LED modes are named A through D and shows the following:

Port LED Indication mode D:

Green (1000Mbit): Solid=Link, Blink=Activity

Orange (10/100Mbit): Solid=Link, Blink=Activity

Port LED Indication mode C:

Green: Solid=Full Duplex Off=No link

Orange: Solid=Half Duplex, Blink: Collisions

Port LED Indication mode B:

Green: Solid = Link, Blink=Activity

Orange: Solid = Port disabled by management, Blink = Errors received

Port LED Indication mode A:

Power save mode - LEDs are off.

4.6.3 LEDs Intensity

The LEDs power consumption can be reduced by lowering the LEDs intensity. LEDs intensity could for example be lowered during night time, or they could be turn completely off. It is possible to configure 24 different hours of the day, at where the LEDs intensity should be set

The LED intensity timer has the following configurable parameters:

Start Time

The time at which the LEDs intensity shall be set to the corresponding intensity.

End Time

The time at which the LEDs intensity shall be set to a new intensity. If no intensity is specified for the next hour, the intensity is set to default intensity.

Intensity

Set or show the LEDs intensity (100% = Full power, 0% = LED off, Default = 100%)

4.6.4 Maintenance

During maintenance of the switch (e.g. adding or moving users), a network administrator might want to have full LED intensity. Therefore, it is possible to specify that the LEDs shall use full intensity at specific period of time. Maintenance Time is the number of seconds that the LEDs will have full intensity after either a port has changed link state, or the LED pushbutton has been pushed.

On Time at Link Change

Set or show the number of seconds for LEDs to be at full intensity during link status change.

On at Errors

☒ Set the LEDs to full intensity on errors

☐ LEDs intensity not affected by errors (Default: this is the default)

4.6.5 Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.7 Green Ethernet - Port Power Savings

Energy Efficient Ethernet (EEE) is a power savings option that reduces the power usage when there is low or no traffic utilization.

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 named 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 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 for EEE.

The EEE port settings relate to the currently selected stack unit, as reflected by the page header.

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.

TECHAYA

Configuration

- System
- Green Ethernet
 - LED
 - Port Power Savings
 - Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD

Monitor

- System
- Green Ethernet
- Thermal Protection
- Ports

Port Power Savings Configuration

Optimize EEE for: Latency

Port Configuration

Port	ActiPHY	PerfectReach	EEE	EEE Urgent Queues									
				1	2	3	4	5	6	7	8		
1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Save Reset

4.7.1 Port Configuration

The Port Power Savings has the following configurable parameters for each port:

Port

This column shows the switch port number of the logical port.

ActiPHY

ActiPHY works by lowering the power for a port when there is no link. To avoid the link being asleep when no data is sent, it activates the circuitry periodically.

- ☒ Link down power savings enabled
- ☐ Link down power savings disabled (default: Disable)

PerfectReach

PerfectReach works by determining the cable length and lowering the power for ports with short cables.

- ☒ Cable length power savings enabled
- ☐ Cable length power savings disabled (default: Disable)

EEE

In order to maximize power savings, the circuit is not started as soon as transmit data is ready for a port. The data is queued until a burst of data is ready to be transmitted. This will give some traffic latency.

- ☒ EEE is enabled for this switch port
- ☐ EEE is disabled for this switch port (default: Disable)

EEE Urgent Queues

If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up immediately and the latency will be reduced to the wakeup time.

- ☒ Queue set as urgent - will activate transmission of frames as soon as data is available
- ☐ Queue in regular mode - will postpone transmission until a burst of frames can be transmitted (default: Queue in regular mode)

4.7.2 Port Power Savings Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.8 Thermal Protection Configuration

This page allows the user to inspect and configure the current setting for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated.

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. Each port is assigned a priority. Each priority is assigned a temperature at which the corresponding ports shall be turned off.

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAG Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD

Monitor

- System
- Green Ethernet
- Thermal Protection
- Ports
- State

Thermal Protection Configuration

Temperature settings for groups

Group	Temperature	
0	255	°C
1	255	°C
2	255	°C
3	255	°C

Port groups

Port	Group
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

Save Reset

4.8.1 Temperature Settings for Priority Groups

Set or show the temperature at which the ports with the corresponding priority will be turned off. Temperatures between 0°C and 255°C are supported.

4.8.2 Port Priorities

The priority the port belongs to. 4 priorities are supported.
(The default priority is 0)

4.8.3 Thermal Protection Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.9 Ports

This page displays the current port configurations.

Port Configuration

Port	Description	Link	Speed		Adv Duplex		Adv speed			Flow Control			Maximum Frame Size	Excessive Collision Mode	Frame Length Check
			Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx			
1		1Gdx	1Gdx	Auto	✓	✓	✓	✓	✓	✓	✓	✓	9600	Discard	✓
2		Down	Down	Auto	✓	✓	✓	✓	✓	✓	✓	✓	9600	Discard	✓
3		Down	Down	Auto	✓	✓	✓	✓	✓	✓	✓	✓	9600	Discard	✓
4		Down	Down	Auto	✓	✓	✓	✓	✓	✓	✓	✓	9600	Discard	✓
5		Down	Down	Auto	✓	✓	✓	✓	✓	✓	✓	✓	9600	Discard	✓
6		Down	Down	Auto	✓	✓	✓	✓	✓	✓	✓	✓	9600	Discard	✓
7		Down	Down	Auto	✓	✓	✓	✓	✓	✓	✓	✓	9600	Discard	✓
8		Down	Down	Auto	✓	✓	✓	✓	✓	✓	✓	✓	9600	Discard	✓

Save Reset

4.9.1 Port Configuration

The user can configure the following port parameters:

Port

This column displays the logical port number for this row.

Description

The description of the port. It is an ASCII string no longer than 256 characters.

Link

The current link state is displayed graphically. Green indicates the link is up and red that it is down.

Speed - Current

This column displays the current link speed of the port.

Speed - Configured

The user can select any available link speed for the given switch port. Only speeds supported by the specific port are shown. Possible speeds are:

Disabled - Disables the switch port operation.

Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.

10Mbps HDX - Forces the cu port in 10Mbps half duplex mode.

10Mbps FDX - Forces the cu port in 10Mbps full duplex mode.

100Mbps HDX - Forces the cu port in 100Mbps half duplex mode.

100Mbps FDX - Forces the cu port in 100Mbps full duplex mode.

1Gbps FDX - Forces the port in 1Gbps full duplex.

Ports in AMS mode with 1000-X speed has Cu port preferred.

Ports in AMS mode with 1000-X speed has fiber port preferred.

Ports in AMS mode with 100-FX speed has fiber port preferred.

Advertise Duplex

When duplex is set as auto i.e auto negotiation, the port will only advertise the specified duplex as either **Fdx** or **Hdx** to the link partner. By default, port will advertise all the supported duplexes if the Duplex is Auto.

Advertise Speed

When Speed is set as auto i.e auto negotiation, the port will only advertise the specified speeds (**10M**, **100M**, **1G**) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto.

Flow Control

When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.

When a fixed-speed setting is selected, that is what is used.

The Rx and Tx settings are determined by the result of the last Auto-Negotiation.

Current Rx

The Current Rx column indicates whether pause frames on the port are obeyed.

Current Tx

The Current Tx column indicates whether pause frames on the port are transmitted

Configured

When flow control is configured, the network element can control the flow of data transmission, to prevent the network from becoming overwhelmed.

☒ Flow control is configured for this port. This setting is related to the setting for Configured Link Speed.

☐ Flow control is **not** configured for this port. (This is the default.)

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, e.g. '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. The range is 1518-9600 bytes.

Excessive Collision Mode

Configure port transmit collision behavior:

Discard: Discard frame after 16 collisions (default)

Restart: Restart backoff algorithm after 16 collisions

Frame Length Check

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

4.9.2 Port Configuration Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page. Any changes made locally will be undone.

4.10 DHCP

DHCP Server

4.10.1 DHCP Server Mode Configuration

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.



4.10.1.1 Global Mode

Configure operation mode to enable/disable DHCP server per system.

Mode

Configure the operation mode per system. Possible modes are:

Enabled: Enable DHCP server per system.

Disabled: Disable DHCP server per system.

4.10.1.2 VLAN Mode

Configure operation mode to enable/disable DHCP server per VLAN.

VLAN Range

Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.

On the other hand, if you want to disable existed VLAN range, then you can follow the steps.

1. press **Add VLAN Range** to add a new VLAN range.
2. input the VLAN range that you want to disable.
3. choose Mode to be Disabled.
4. press **Save** to apply the change.

Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.

Mode

Indicate the operation mode per VLAN. Possible modes are:

Enabled: Enable DHCP server per VLAN.

Disabled: Disable DHCP server per VLAN.

4.10.1.3 DHCP Server Mode Buttons

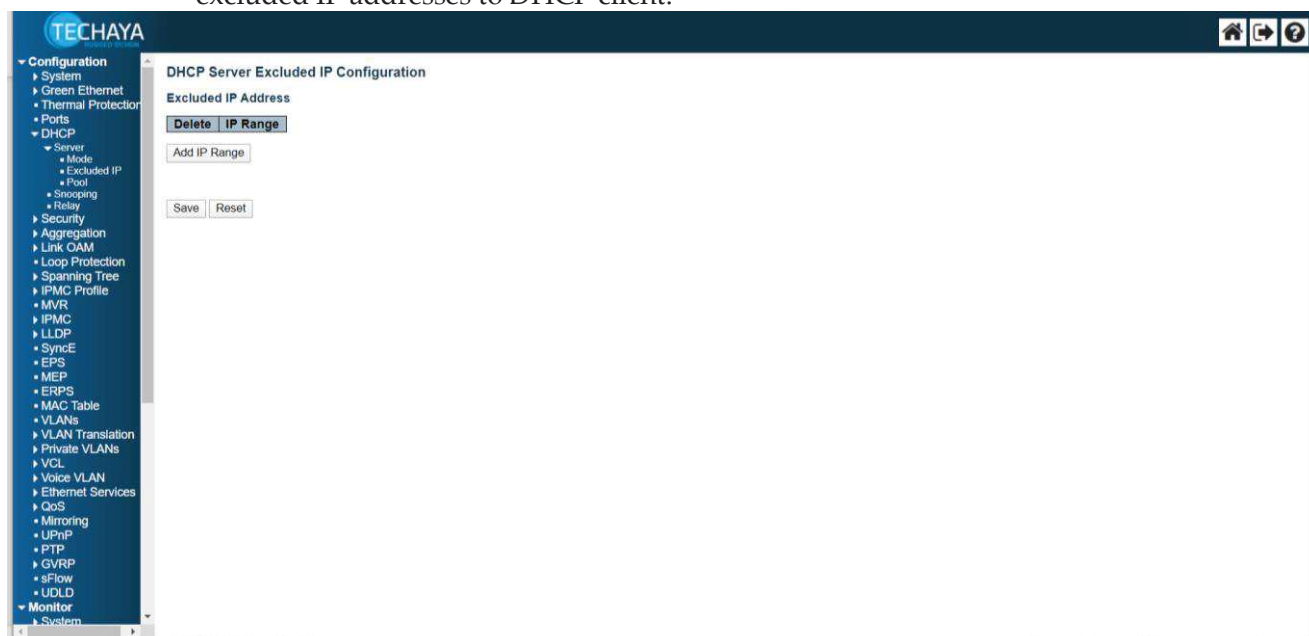
Add VLAN Range: Click to add a new VLAN range.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.10.2 DHCP Server Excluded IP Configuration

This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.



4.10.2.1 Excluded IP Address

Configure excluded IP addresses.

IP Range

Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both.

4.10.2.2 DHCP Server Excluded Buttons

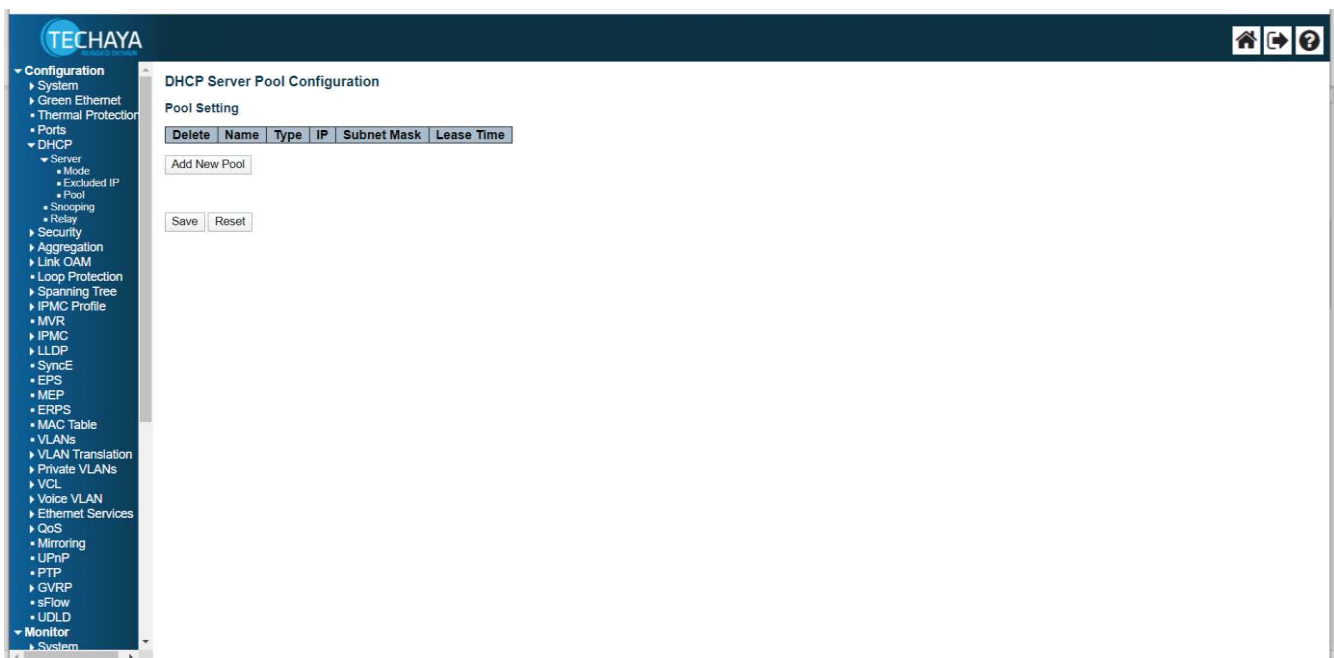
Add IP Range: Click to add a new excluded IP range.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.10.3 DHCP Server Pool Configuration

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.



4.10.3.1 Pool Settings

Add or delete pools.

Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.

Name

Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.

Type

Display which type of the pool is.

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.

If "-" is displayed, it means not defined.

IP

Display network number of the DHCP address pool.

If "-" is displayed, it means not defined.

Subnet Mask

Display subnet mask of the DHCP address pool.

If "-" is displayed, it means not defined.

Lease Time

Display lease time of the pool.

4.10.3.2 DHCP Server Pool Buttons

Add New Pool: Click to add a new DHCP pool.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

DHCP Snooping

Configure DHCP Snooping on this page.



Snooping Mode

Indicates the DHCP snooping mode operation. Possible modes are:

Enabled: Enable DHCP snooping mode operation. 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.

Disabled: Disable DHCP snooping mode operation.

Port Mode Configuration

Indicates the DHCP snooping port mode. Possible port modes are:

Trusted: Configures the port as trusted source of the DHCP messages.

Untrusted: Configures the port as untrusted source of the DHCP messages.

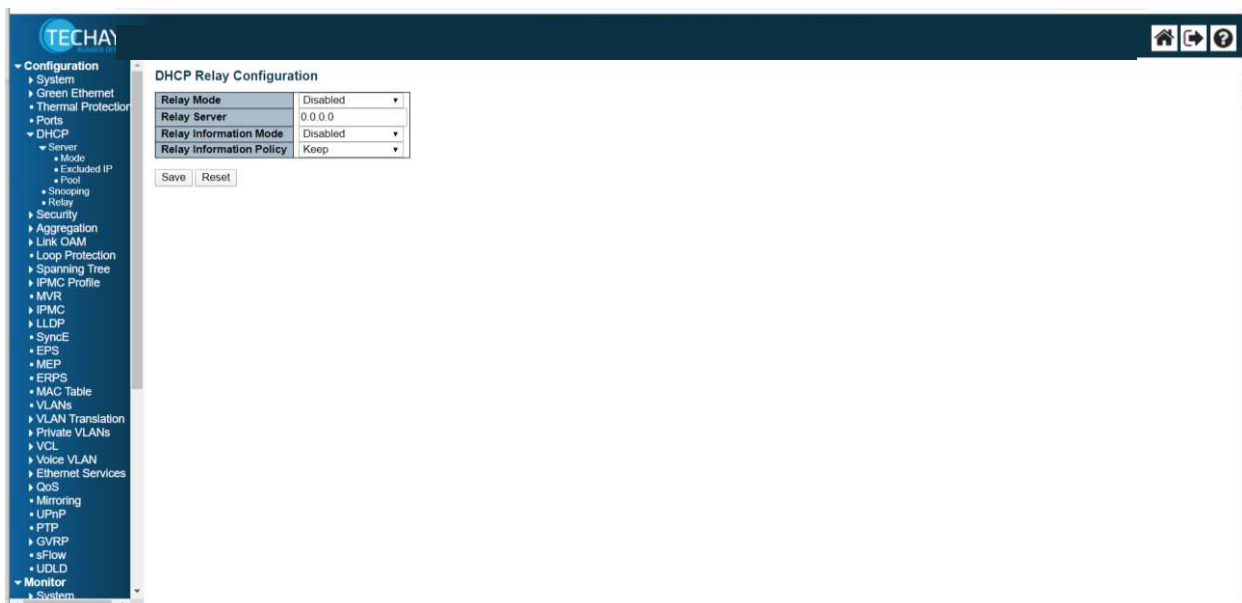
DHCP Snooping Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

DHCP Relay

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID(Port VLAN ID) correctly.



Relay Mode

Indicates the DHCP relay mode operation.

Possible modes are:

Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

Disabled: Disable DHCP relay mode operation.

Relay Server

Indicates the DHCP relay server IP address.

Relay Information Mode

Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive from VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible modes are:

Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

Disabled: Disable DHCP relay information mode operation.

Relay Information Policy

Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:

Replace: Replace the original relay information when a DHCP message that already contains it is received.

Keep: Keep the original relay information when a DHCP message that already contains it is received.

Drop: Drop the package when a DHCP message that already contains relay information is received.

DHCP Relay Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.11 Security – Switch - Users Configurations

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.

The displayed values for each user are:

User Name

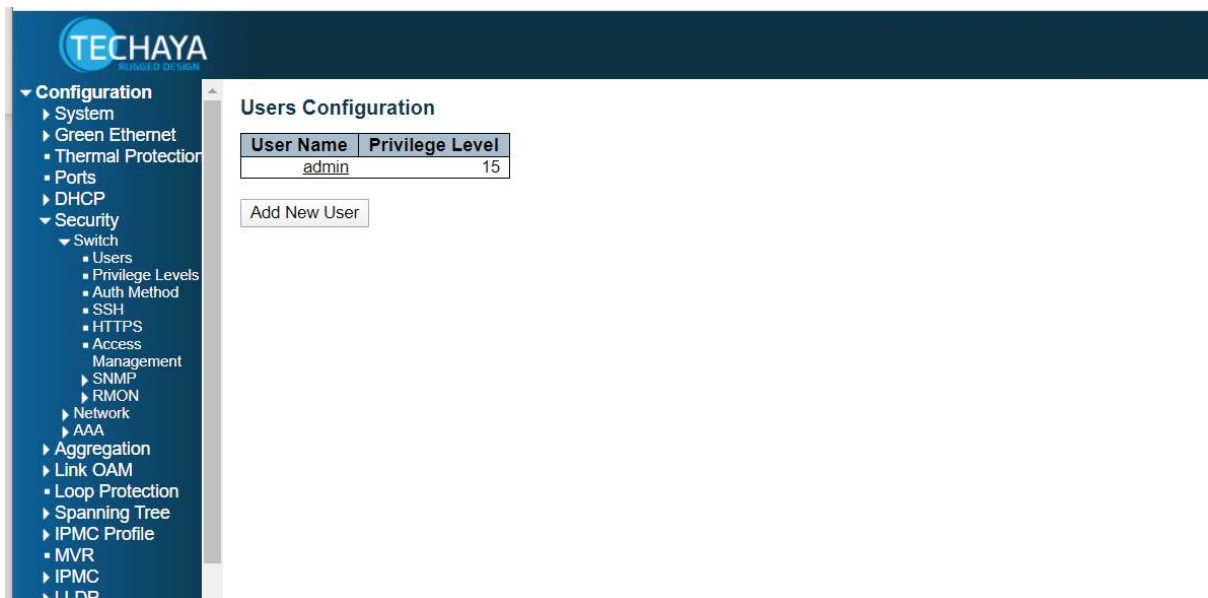
The name identifying the user. This is also a link to Add/Edit User.

Privilege Level

The privilege level of the user. The allowed range is 0 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 others value 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.

Buttons

Add New User: Click to add a new user.



4.12 Security – Switch – Privilege Levels

This page provides an overview of the privilege levels.

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 ▼
EPS	5 ▼	10 ▼	5 ▼	10 ▼
ERPS	5 ▼	10 ▼	5 ▼	10 ▼
ETH_LINK_OAM	5 ▼	10 ▼	5 ▼	10 ▼
EVC	5 ▼	10 ▼	5 ▼	10 ▼
Green_Ethernet	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 ▼
MEP	5 ▼	10 ▼	5 ▼	10 ▼
MVR	5 ▼	10 ▼	5 ▼	10 ▼
NTP	5 ▼	10 ▼	5 ▼	10 ▼
Ports	5 ▼	10 ▼	1 ▼	10 ▼
Private_VLANS	5 ▼	10 ▼	5 ▼	10 ▼
PTP	5 ▼	10 ▼	5 ▼	10 ▼
QoS	5 ▼	10 ▼	5 ▼	10 ▼
RMirror	5 ▼	10 ▼	5 ▼	10 ▼
Security	5 ▼	10 ▼	5 ▼	10 ▼

4.12.1 Group name

The name identifying 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'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

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.

4.12.2 Privilege Level

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 same or greater than the authorization Privilege level to have the access to that group.

Notes that some web pages (for example, MPLS-TP and MEP BFD pages) are based on JSON to transmit dynamic data between the web server and application. These pages require the configuration Read/Write privilege of JSON_RPC group before any operations. This requirement must be met first, then it will evaluate the current privilege level against the required privilege level for the given method. For example, assumes the MPLS-TP page only allows Read-Only attribute under privilege level 5, the privilege configuration should be set as JSON_RPC:[5,5,5,5] and MPLS_TP:[5,10,5,10].

4.12.3 Privilege Levels Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.13 Security – Switch – Auth Method

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
 - Switch
 - Users
 - Privilege Levels
 - Auth Method
 - SSH
 - HTTPS
 - Access Management
 - SNMP
 - RMON
 - Network
 - AAA
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - LLDP
 - SyncE
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLANs
 - VLAN Translation
 - Private VLANs
 - VCL
 - Voice VLAN
 - Ethernet Services
 - QoS
 - Mirroring
 - UPnP
 - PTP

Authentication Method Configuration

Client	Method	no	local	radius	tacacs
console	local	no	no	no	no
telnet	local	no	no	no	no
ssh	local	no	no	no	no
http	local	no	no	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		☐

Save Reset

4.13.1 Authentication Method Configuration

The authentication section allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.

The authentication method configuration has the following parameters:

Client

The management client for which the configuration applies:

- Console
- Telnet
- SSH
- Http

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.

Methods that involve remote servers are timed 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.

Cmd Lvl

Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.

Cfg Cmd

Also authorize configuration commands.

4.13.2 Command Authorization Method Configuration

The command authorization section allows you to limit the CLI commands available to a user.

The authentication method configuration has the following parameters:

Client

The management client for which the configuration applies:

- Console
- Telnet
- SSH

Methods

Method can be set to one of the following values:

no: Command authorization is disabled. User is granted access to CLI commands according to his privilege level.

tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

Cmd Lvl

Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.

Cfg Cmd

Also authorize configuration commands.

4.13.3 Accounting Method Configuration

The accounting section allows you to configure command and exec (login) accounting.

The table has one row for each client type and a number of columns, which are:

Client

The management client for which the configuration applies:

- Console
- Telnet
- SSH

Methods

Method can be set to one of the following values:

no: Accounting is disabled.

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

Enable accounting of all commands with a privilege level higher than or equal to this level.

Cmd Lvl

Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.

Exec

Enable exec (login) accounting.

4.13.4 Authentication Method Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.14 Security – Switch – SSH

Configure SSH on this page.



4.14.1 SSH Configuration

Mode

Indicates the SSH mode operation. Possible modes are:

Enabled: Enable SSH mode operation.

Disabled: Disable SSH mode operation.

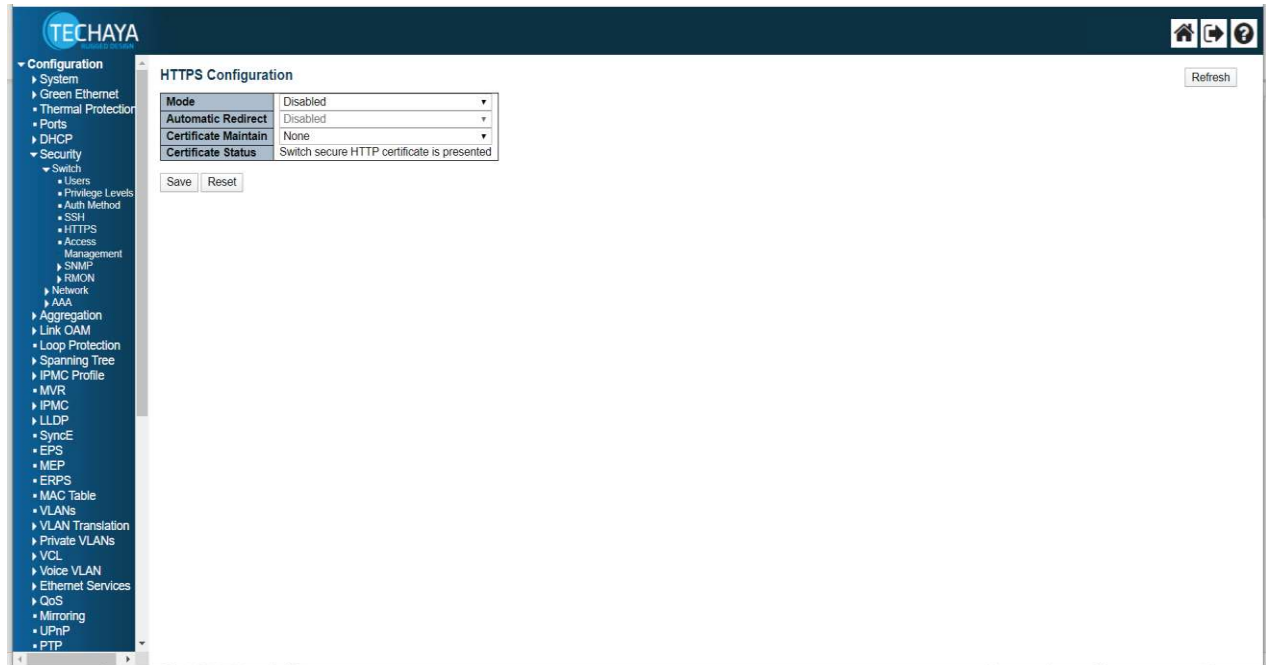
4.14.2 SSH Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.15 Security – Switch – HTTPS

The user can configure HTTPS from this page.



4.15.1 HTTPS Configuration

The HTTPS configuration has the following parameters:

Mode

Set or show the HTTPS operation mode.

This mode allows the user to disable HTTPS even when the current connection is HTTPS. Possible modes are:

Enabled: Enable HTTPS mode operation.

Disabled: Disable HTTPS mode operation.

Automatic Redirect

Set or show the HTTPS redirect operation mode. Automatic Redirect is only available when HTTPS mode is enabled.

Enabled: Enable HTTPS redirect mode operation, to automatically redirect web browser to an HTTPS

Disabled: Disable HTTPS redirect mode operation (This is the default).

Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case.

Certificate Maintain

The operation of certificate maintenance. Possible operations are:

None: No operation.

Delete: Delete the current certificate.

Upload: Upload a certificate PEM file. Possible methods are: Web Browser or URL.

Generate: Generate a new self-signed RSA certificate.

Certificate Pass Phrase

Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.

Certificate Upload

Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem. Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39.

Possible methods are:

Web Browser: Upload a certificate via Web browser.

URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.

Certificate Status

Display the current status of certificate on the switch.

Possible statuses are:

Switch secure HTTP certificate is presented.

Switch secure HTTP certificate is not presented.

Switch secure HTTP certificate is generating

4.15.2 HTTPS Buttons

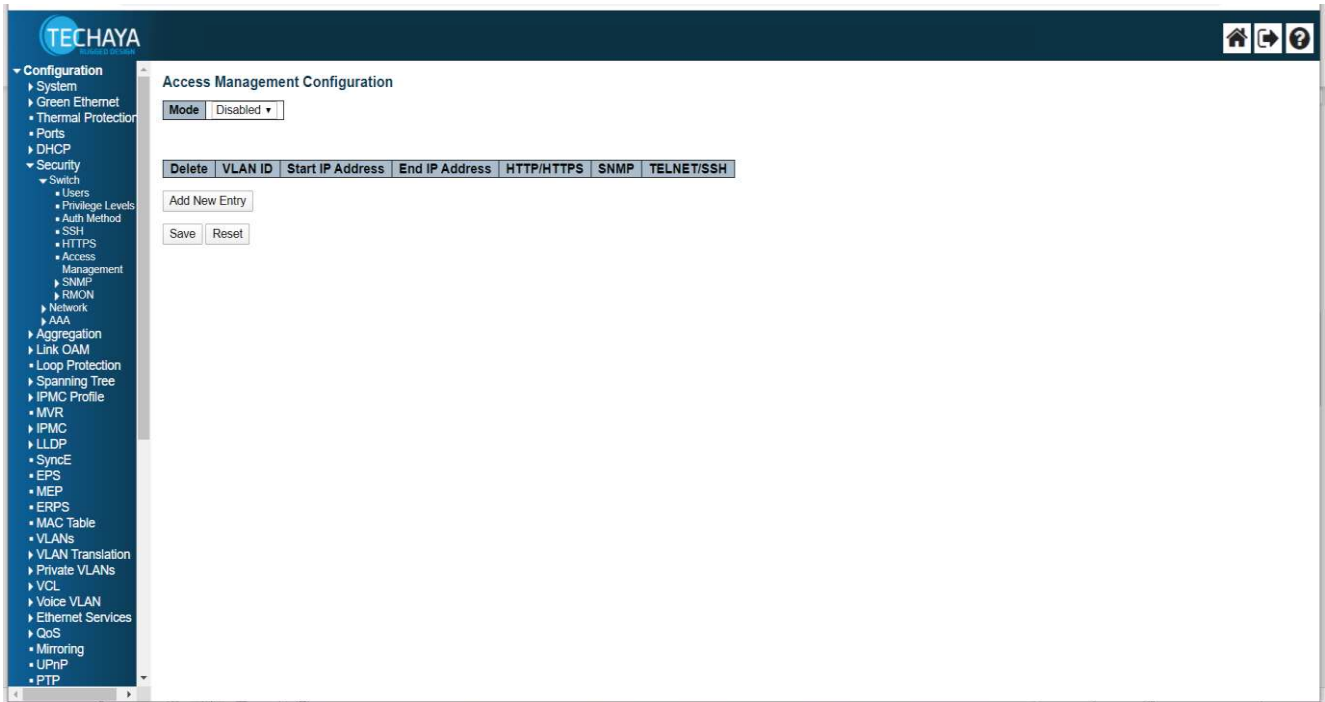
Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

Refresh: Click to refresh the page. Any changes made locally will be undone.

4.16 Security – Switch – Access Management

The user can 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 allow access to the switch.



4.16.1 Access Management Configuration

The access management configuration has the following parameters:

Mode

Set or show the access management mode operation.

Enabled: Enable access management mode operation

Disabled: Disable access management mode operation (This is the default mode.)

Delete

☒ Check to delete the entry. It will be deleted during the next save.

☐ Do not delete the entry. (This is the default.)

VLAN ID

Set or show the VLAN ID for the access management entry.

Start IP Address

Set or show the start IP address for the access management entry.

End IP Address

Set or show the end IP address for the access management entry.

HTTP/HTTPS

Set or show HTTP/HTTPS interface status.

- ☒ Enabled - when the host IP address matches the IP address range provided in the entry, the host can access the switch from HTTP/HTTPS interface
- ☐ Disabled (This is the default.)

SNMP

Set or show SNMP interface status.

- ☒ Enabled - when the host IP address matches the IP address range provided in the entry, the host can access the switch from SNMP interface
- ☐ Disabled (This is the default.)

TELNET/SSH

Set or show TELNET/SSH interface status.

- ☒ Enabled - when the host IP address matches the IP address range provided in the entry, the host can access the switch from TELNET/SSH interface
- ☐ Disabled (This is the default.)

4.16.2 Access Management Buttons

Add New Entry: Click to add a new access management entry.

Save: Click to save all changes.

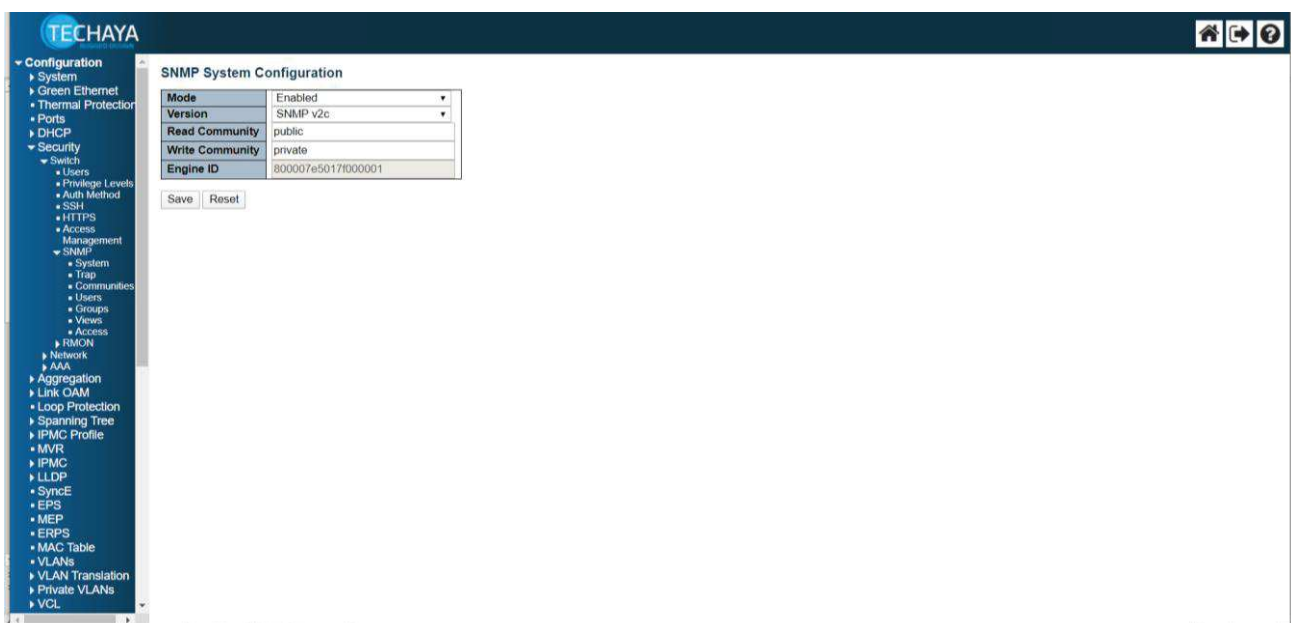
Reset: Click to undo any changes made locally and revert to previously saved values.

4.17 Security – Switch – SNMP– System

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allows diverse network objects to participate in network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

4.17.1 System SNMP System Configuration

The user can configure SNMP from this page.



Mode

Set or show the SNMP mode operation.

Enabled: Enable SNMP mode operation (This is the default mode.)

Disabled: Disable SNMP mode operation

Version

Set or show 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

Set or show the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

Applicable Only to SNMP versions: SNMPv1 or SNMPv2c

If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It 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.

Write Community

Set or show the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

Applicable Only to SNMP versions: SNMPv1 or SNMPv2c

If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It 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

Set or show 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. Change of the Engine ID will clear all original local users.

Applicable Only to SNMP version: SNMPv3

4.17.2 SNMP System Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

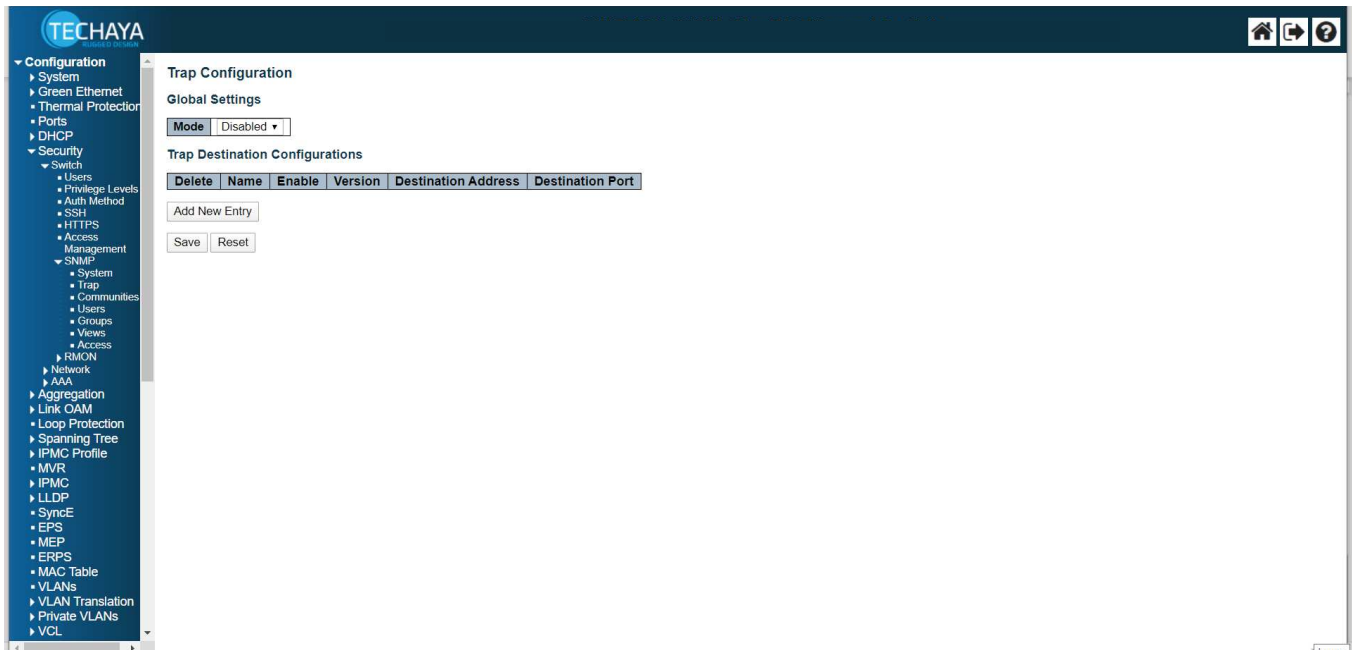
4.18 Security – Switch – SNMP – Trap

The user can enable, disable, and delete SNMP Traps from this page.

Trap Configuration

To create a new trap, click the **Add New Entry** button to open the SNMP Trap Configuration Page.

To edit an existing trap, click on the trap name to open the SNMP Trap



4.18.1 Global Settings

Set or show the SNMP trap mode operation.

Mode

Enabled: Enable SNMP trap mode operation

Disabled: Disable SNMP trap mode operation (This is the default mode.)

4.18.2 Trap Destination Configurations

Except for the “Delete” field parameters in the trap destination configurations table are display only.

Delete

☒ Check to delete the entry. It will be deleted during the next save.

☐ Do not delete the entry. (This is the default.)

Name

Shows the name of the specific trap

Enable

Shows the operation status of the specific trap (enabled/disabled)

Version

Show the SNMP trap supported version.

Destination Address

Show the SNMP trap destination address.

Destination Port

Show the SNMP trap destination port.

4.18.3 **Trap Configuration Buttons**

Add New Entry: Click to add a new trap destination configuration

Save: Click to save all changes

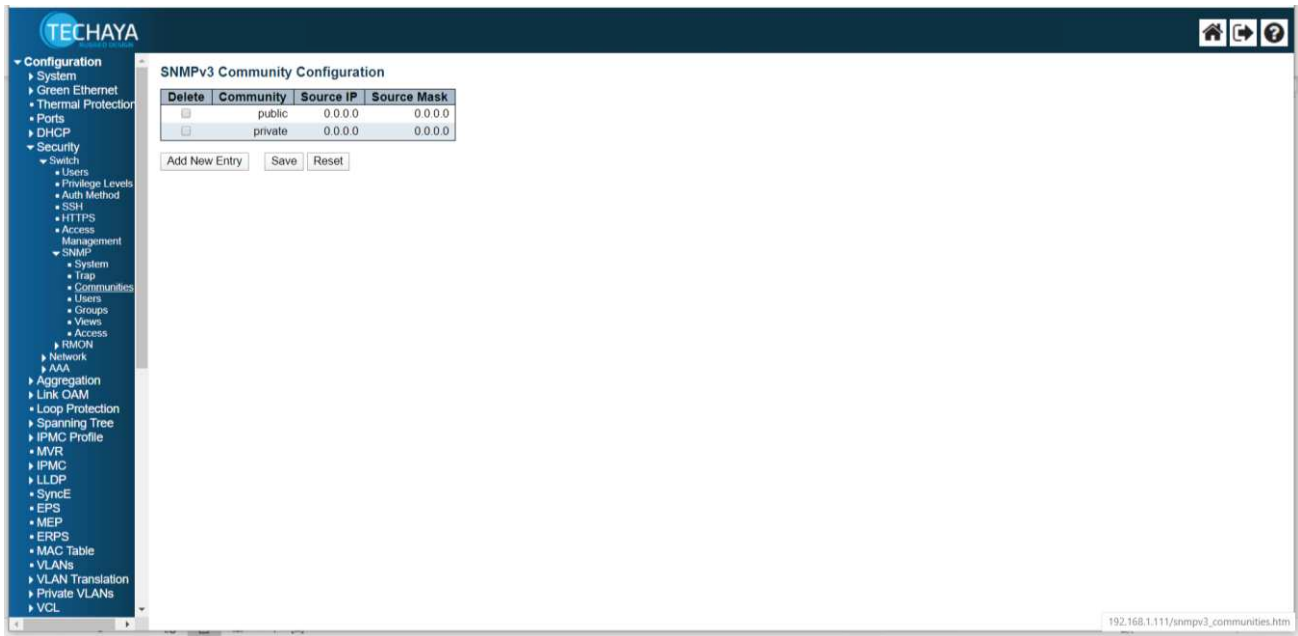
Reset: Click to undo any changes made locally and revert to previously saved values

4.18.3.1 **SNMP Trap Configuration (Add or Reconfigure a Trap)**

The user can create a new SNMP Trap or reconfigure an existing trap from this page. Open this page is by clicking the **Add New Entry** button on the Trap Configuration Page.

4.19 Security – Switch – SNMP – Communities

The user can configure SNMPv3 from this page. The entry index key is Community.



4.19.1 SNMPv3 Community Configuration

The SNMPv3 Community Configuration page has the following parameters:

Delete

- ☒ Check to delete the entry. It will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

Community

Set or show 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 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

Source IP

Set or show 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

Set or show the SNMP access source address mask.

4.19.2 Community Configuration Buttons

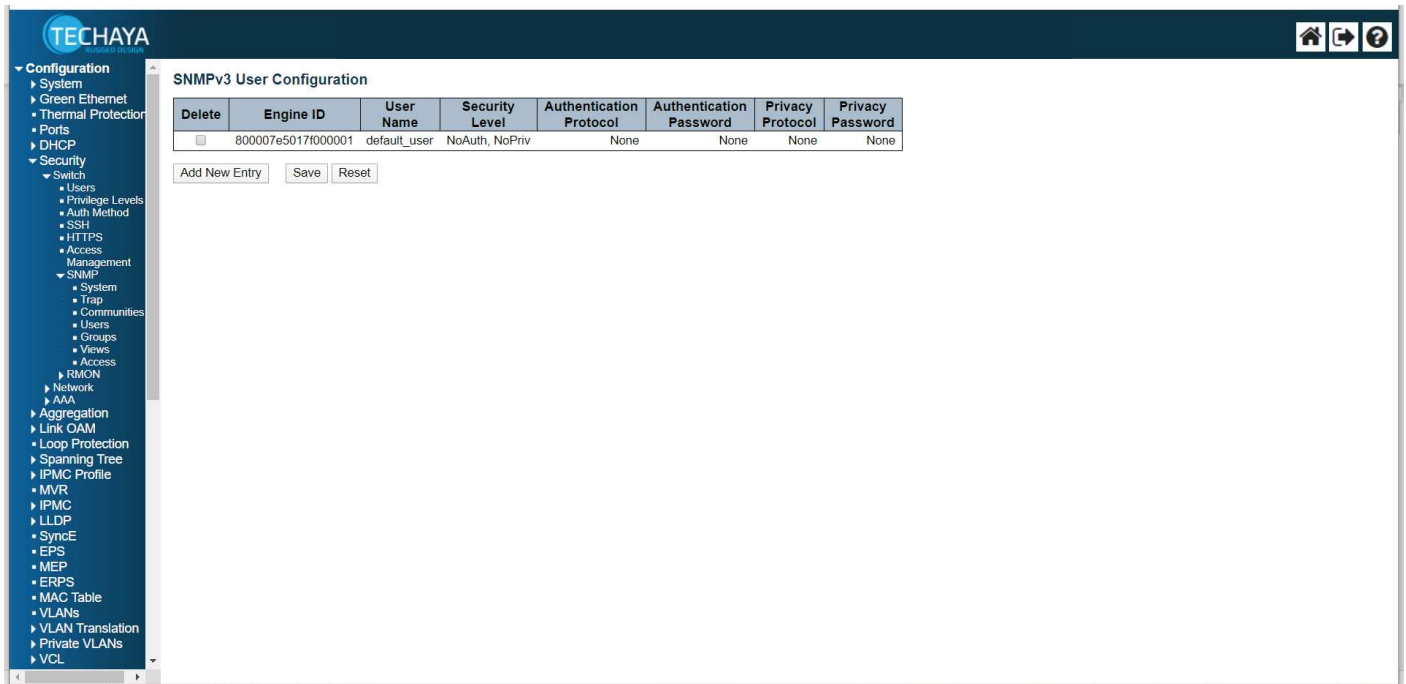
Add New Entry: Click to add a new community configuration

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.20 Security – Switch – SNMP – Users

The user can configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.



4.20.1 SNMPv3 User Configuration

The SNMPv3 User Configuration Page has the following parameters:

Delete

- ☒ Check to delete the entry. It will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

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. If the user engine ID equals the system engine ID then it is local user; otherwise it's 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 33 to 126.

Security Level

Set or show 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

The value of security level cannot be modified if entry already exists. Use care to ensure that the value is set correctly (otherwise the user will need to delete and recreate the entry in order to reset the security level).

Authentication Protocol

Set or show 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. Use care to ensure that the value is set correctly (otherwise the user will need to delete and recreate the entry in order to reset the security level).

Authentication Password

Set or show the string identifying the authentication password phrase. Allowed string length depends on the authentication protocol:

- MD5: string length 8 to 32 characters
- SHA: string length 8 to 40 characters

The allowed content is ASCII characters from 33 to 126.

Privacy Protocol

Set or show 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

Set or show the string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

4.20.2 User Configuration Buttons

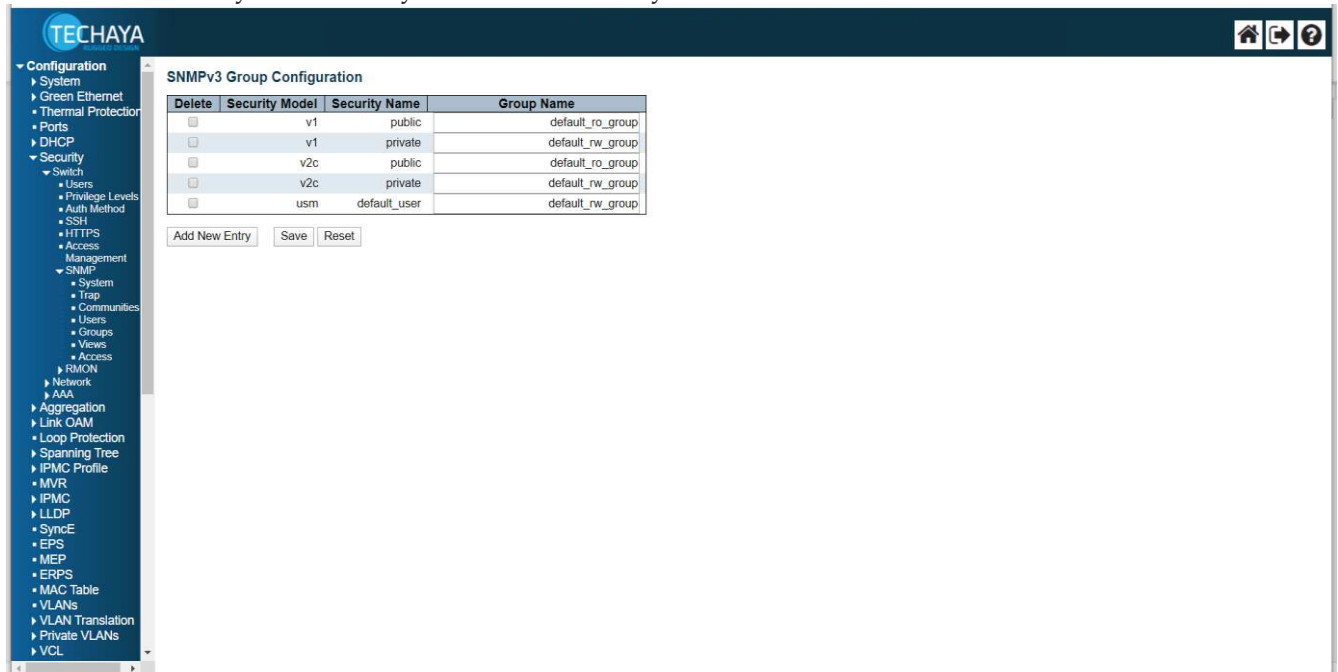
Add New Entry: Click to add a new user configuration.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.21 Security – Switch – SNMP – Groups

The user can configure the SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.



4.21.1 SNMPv3 Group Configuration

The SNMPv3 Group Configuration Page has the following parameters:

Delete

- ☒ Check to delete the entry. It will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

Security Model

Set or show 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)

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 33 to 126.

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 33 to 126.

4.21.2 Group Configuration Buttons**Add New Entry:**

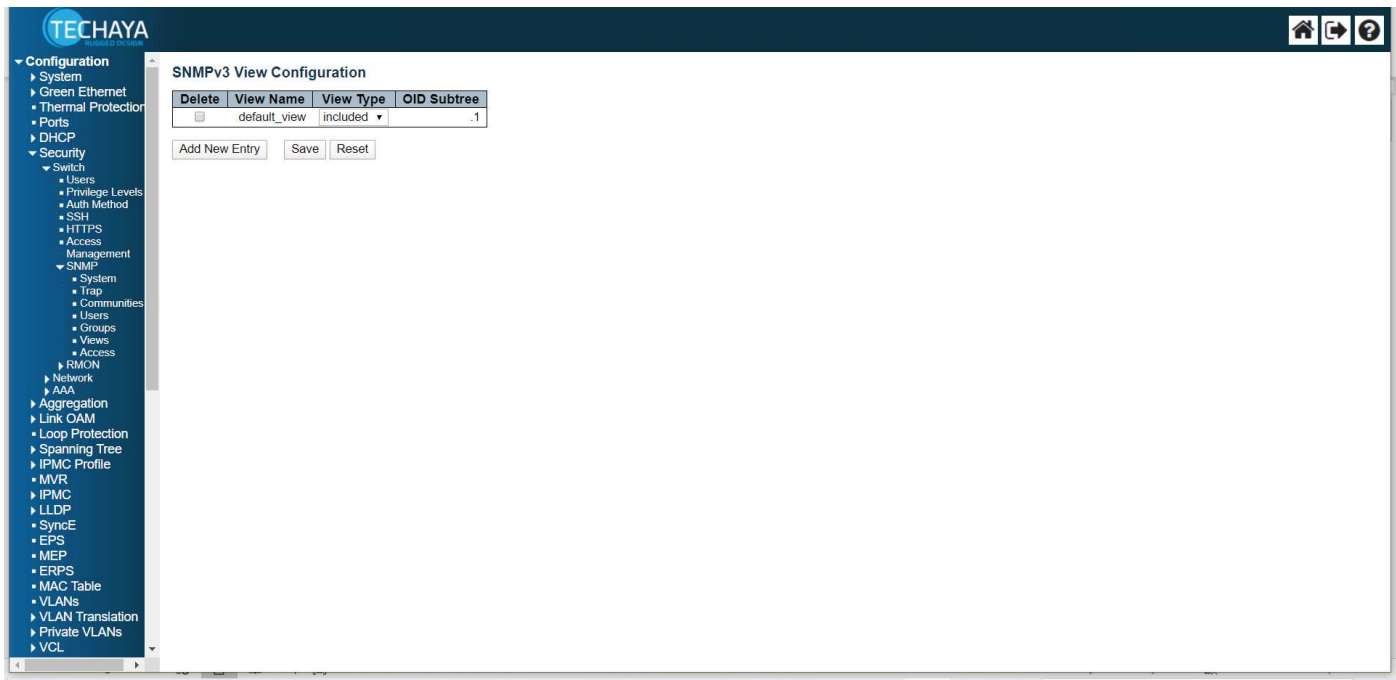
Click to add a new group configuration

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.22 Security – Switch – SNMP – Views

The user can configure the SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.



4.22.1 SNMPv3 View Configuration

The SNMPv3 View Configuration Page has the following parameters:

Delete

- ☒ Check to delete the entry. It will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

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 33 to 126.

View Type

Set or show 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

If a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

OID Subtree

Set or show 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 asterisk (*).

4.22.2 View Configuration Buttons

Add New Entry:

Click to add a new view configuration

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.23 Security – Switch – SNMP – Access

The user can configure the SNMPv3 access table on this page. The entry index keys are Group Name, Security Model and Security Level.

TECHAYA

Configuration

- System
 - Green Ethernet
 - Thermal Protection
- Ports
- DHCP
- Security
 - Switch
 - Users
 - Privilege Levels
 - Auth Method
 - SSH
 - HTTPS
 - Access Management
 - SNMP
 - System
 - Trap
 - Communities
 - Users
 - Groups
 - Views
 - Access
 - RMON
 - Network
 - AAA
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - LLDP
 - SyncE
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLANs
 - VLAN Translation
 - Private VLANs
 - VCL

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

Add New Entry Save Reset

4.23.1 SNMPv3 Access Configuration

The SNMPv3 Access Configuration Page has the following parameters:

Delete



Check to delete the entry. It will be deleted during the next save.



Do not delete the entry. (This is the default.)

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 33 to 126.

Security Model

Set or show 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)

Security Level

Set or show 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

Set or show 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 33 to 126.

Write View Name

Set or show 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 33 to 126.

4.23.2 Access Configuration Buttons

Add New Entry:

Click to add a new access configuration

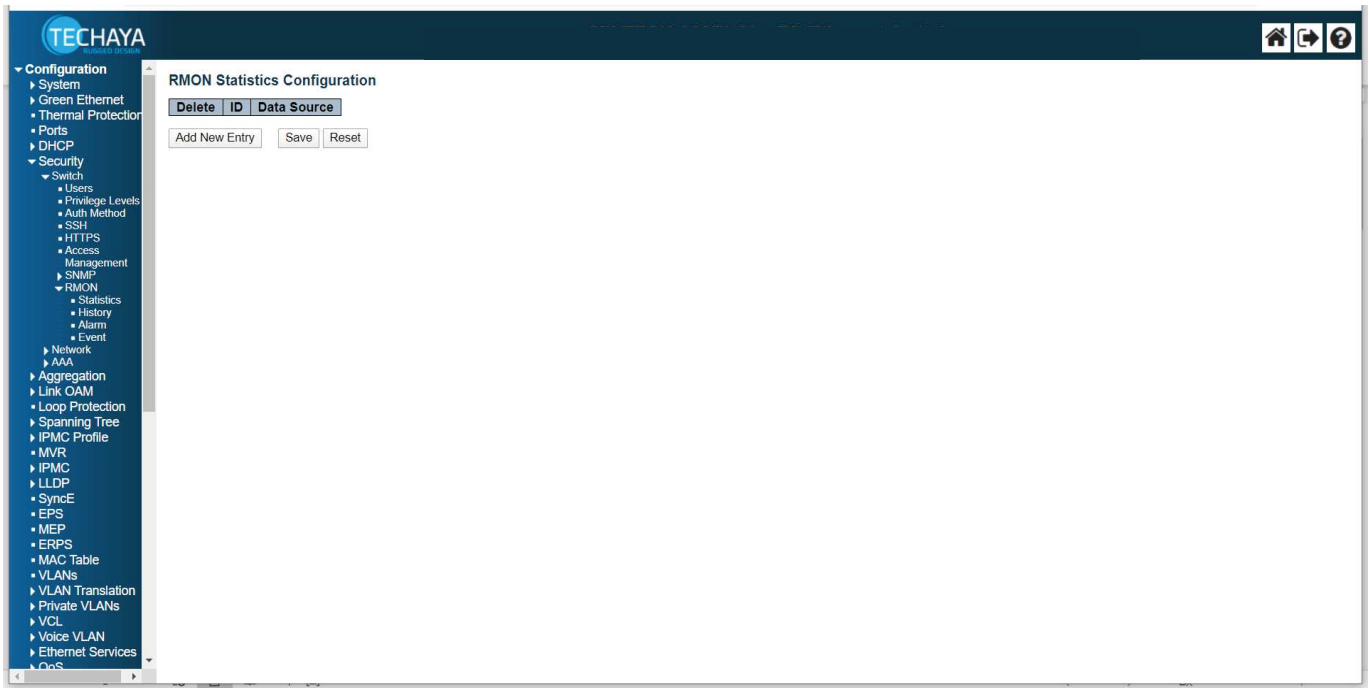
Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.24 Security – Switch – SNMP – RMON

4.24.1 RMON Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is ID.



The RMON Statistics Configuration Page has the following parameters:

Delete

- ☒ Check to delete the entry. It will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

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. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

4.24.2 RMON Statistics Configuration Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.25 Security – Switch – RMON – History

The user can configure the History table on this page.

4.25.1 SNMPv3 Access Configuration

Configure RMON History table on this page. The entry index key is ID.



The History Statistics Configuration Page has the following parameters:

Delete



Check to delete the entry. It will be deleted during the next save.



Do not delete the entry. (This is the default.)

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. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

Interval

Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

Buckets

Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.

Buckets Granted

The number of data shall be saved in the RMON.

4.25.2 RMON History Configuration Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.26 Security – Switch – RMON – Alarm

The user can configure the Alarm table on this page.

4.26.1 Alarm Configuration

Configure RMON Alarm table on this page. The entry index key is ID.

The RMON Alarm Configuration Page has the following parameters:

Delete

- ☒ Check to delete the entry. It will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

ID

Indicates the index of the entry. The range is from 1 to 65535.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to $2^{31}-1$.

Variable

Indicates the particular variable to be sampled, the possible variables are:
InOctets: The total number of octets received on the interface, including framing characters.

InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.

InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

InDiscards: The number of inbound packets that are discarded even the packets are normal.

InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol.

OutOctets: The number of octets transmitted out of the interface, including framing characters.

OutUcastPkts: The number of uni-cast packets that request to transmit.

OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit.

OutDiscards: The number of outbound packets that are discarded event the packets is normal.

OutErrors: The number of outbound packets that could not be transmitted because of errors.

OutQLen: The length of the output packet queue (in packets).

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

Absolute: Get the sample directly.

Delta: Calculate the difference between samples (default).

Value

The value of the statistic during the last sampling period.

Startup Alarm

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

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.

RisingOrFalling Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Rising Threshold

Rising threshold value (-2147483648-2147483647).

Rising Index

Rising event index (1-65535).

Falling Threshold

Falling threshold value (-2147483648-2147483647).

Falling Index

Falling event index (1-65535).

4.26.2 RMON Alarm Configuration Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.27 Security – Switch – RMON – Event

The user can configure the Event table on this page.

4.27.1 RMON Event Configuration

Configure RMON Event table on this page. The entry index key is ID.



The Event Configuration Page has the following parameters:

Delete



Check to delete the entry. It will be deleted during the next save.



Do not delete the entry. (This is the default.)

ID

Indicates the index of the entry. The range is from 1 to 65535.

Desc

Indicates this event, the string length is from 0 to 127, default is a null string.

Type

Indicates the notification of the event, the possible types are:

none: No SNMP log is created, no SNMP trap is sent.

log: Create SNMP log entry when the event is triggered.

snmptrap: Send SNMP trap when the event is triggered.

logandtrap: Create SNMP log entry and sent SNMP trap when the event is triggered.

Community

Specify the community when trap is sent, the string length is from 0 to 127, default is "public".

Event Last Time

Indicates the value of sysUpTime at the time this event entry last generated an event.

4.27.2 RMON Event Configuration Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.28 Security – Network – Limit Control

This page allows you to configure the Port Security Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.

The Limit Control configuration consists of two sections, a system- and a port-wide.

Port Security Limit Control Configuration

System Configuration

Mode: Disabled

Aging Enabled: ☐

Aging Period: 3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
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

Save Reset

4.28.1 System Configuration

Set or show the NAS system configuration parameters.

Mode

Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled

If checked, secured MAC addresses are subject to aging as discussed under Aging Period .

Aging Period

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario:

Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. 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.

4.28.2 Port Configuration

The table has one row for each port on the switch in the stack and a number of columns:

Port

The port number to which the configuration below applies.

Mode

Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Action

If Limit is reached, the switch can take one of the following actions:

- None: Do not allow more than Limit MAC addresses on the port, but take no further action.
- Trap: If Limit + 1 MAC addresses is 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 gets 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 address 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:

- 1) Boot the switch,
- 2) Disable and re-enable Limit Control on the port or the switch,
- 3) 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

This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

- Disabled: Limit Control is either globally disabled or disabled on the port.
- Ready: The limit is not yet reached. This can be shown for all actions.
- Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.
- Shutdown: Indicates that 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 shutdown 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.

4.28.3 Limit Control Configuration Buttons

Refresh: Click to refresh the page. Note that non-committed changes will be lost.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.29 Security – Network – NAS

This page allows the user to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network, by requiring users to first submit credentials for authentication. One or more central servers and the backend servers determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the “Configuration->Security->AAA” page. The IEEE 802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1 X authentications.

The NAS configuration consists of two sections, a system- and a port-wide.

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
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
8	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize

Save Reset

4.29.1 System Configuration

Set or show the NAS system configuration parameters.

Mode

Set or show the NAS mode:

Enabled: NAS is globally enabled on the switchstack

Disabled: NAS is globally disabled on the switchstack (This is the default mode.)

If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled

Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port.

- ☒ Successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period
- ☐ Supplicants/clients are not reauthenticated (This is the default.)

Reauthentication Period

Set or show the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

EAPOL Timeout

Set or show the time for retransmission of Request Identity EAPOL frames.

Valid values are in the range 1 to 65535 seconds. This has no effect on MAC-based ports.

Aging Period

The Port Security module frees resources if no activity within a given period of time. The Aging Period parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

This setting applies to modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module checks the specified MAC address at regular intervals, to see if there is activity.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time

The Hold Time can be set to a number between 10 and 1000000 seconds.

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration->Security->AAA" page - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

The switch will ignore new frames coming from the client during the hold time.

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 (see RADIUS-Assigned VLAN Enabled below for a detailed description).

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 - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. 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 is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].

Max. Reauth. Count

The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.

Valid values are in the range [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.

4.29.2 Port Configuration

The table has one row for each port on the switch in the stack and a number of columns:

Port

The port number for which the configuration below applies.

Admin State

If NAS is enabled globally, this selection controls the port's authentication mode. 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

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. The authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant. (For a more detailed discussion of the Port-based 802.1X Admin State, see the online help.)

- Single 802.1X

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 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.

- Single 802.1X

Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. 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.

- Multi 802.1X

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards

the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **MAC-based Auth.:**

Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. (For a more detailed discussion of the MAC-based authentication Admin State, see the online help.)

RADIUS - Assigned QoS Enabled

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS - Assigned VLAN Enabled

When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID:

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel Private-Group-ID does not need to include a Tag):
 - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
 - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
 - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

Guest VLAN Operation:

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State

Set or show the current state of the port:

- Globally Disabled: NAS is globally disabled.
- Link Down: NAS is globally enabled, but there is no link on the port.
- Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.
- Unauthorized: The port is in Force Unauthorized or a single supplicant mode and the supplicant is not successfully authorized by the RADIUS server.
- X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Restart

Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL based or MAC based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

- **Reauthenticate:**
Schedules a reauthentication 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:**
Forces a 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.

4.29.3 NAS Configuration Buttons

Refresh: Click to refresh the page

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.30 Security – Network – ACL – Ports

ACL is an acronym for Access Control List. It is the list table of ACEs (Access Control Entries), containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL.

4.30.1 ACL Ports Configuration

This page allows the user to configure the ACL Ports parameters (Access Control Entry - ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

Port	Policy ID	Action	Rate Limiter ID	EVC Policer	EVC Policer ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	1	Disabled	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	1	Disabled	Disabled	Disabled	Disabled	Enabled	390
2	0	Permit	Disabled	Disabled	1	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	1	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	1	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	1	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	1	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	1	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	1	Disabled	Disabled	Disabled	Disabled	Enabled	0

Port

Show the logical port for the settings contained in the same row.

Policy ID

Set or show the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.

Action

Set or show the forwarding status of the port:

Permit: Forwarding is permitted (The default value is "Permit".)

Deny: Forwarding is denied

Rate Limiter ID

Set or show the rate limiter to apply on this port. The Rate Limiter can be Disabled or set to a value from 1 through 16. The default value is "Disabled".

EVC Policer

Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that ACL rate limiter and EVC policer can not both be enabled.

EVC Policer ID

Select which EVC policer ID to apply on this port. The allowed values are Disabled or the values 1 through 256.

Port Redirect

Set or show which port frames are redirected on. The Port Redirect can be Disabled or set to a specific port number. It cannot be set when "Action" is permitted. The default value is "Disabled".

Mirror

Set or show the mirror operation of this port:

Enabled: Frames received on the port are mirrored

Disabled: Frames received on the port are not mirrored

The default value is "Disabled".

Logging

Set or show the logging operation of this port:

Enabled: Frames received on the port are stored in the System Log

Disabled: Frames received on the port are not logged (The default value is "Disabled".)

Note:

- The logging message does not include the 4 bytes CRC.
- The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown

Set or show the port shut down operation of this port:

Enabled: If a frame is received on the port, the port will be disabled

Disabled: Port shut down is disabled (The default value is "Disabled".)

Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

State

Set or show the port state of this port.

Enabled: To reopen ports by changing the volatile port configuration of the ACL user module (The default value is "Enabled".)

Disabled: To close ports by changing the volatile port configuration of the ACL user module

Counter

The Counter counts the number of frames that match this ACE.

4.30.2 ACL Ports Configuration Buttons

Refresh: Click to refresh the page, any changes made locally will be undone

Clear: Click to clear the counters

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.31 Security – Network – ACL – Rate Limiters

This page allows the user to configure the rate limiter for the ACL of the switch.

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
 - Switch
 - Network
 - Limit Control
 - NAS
 - ACL
 - Ports
 - Rate Limiters
 - Access Control List
 - IP Source Guard
 - ARP Inspection
 - AAA
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - LLDP
 - SyncE
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLANs
 - VLAN Translation
 - Private VLANs
 - VCL
 - Voice VLAN
 - Ethernet Services
 - QoS
 - Mirroring
 - UPnP
 - PTP

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

Save Reset

4.31.1 ACL Rate Limiter Configuration

The ACL Rate Limiter Configuration Page has the following parameters:

Rate Limiter ID

Shows the Rate Limiter ID for the settings contained in the same row. Its range is 1 to 16.

Rate

The rate range is located 0-3276700 in pps.

- The valid rate is 0 - -1, 0, 0, 0, ..., 3276700 in pps

Or

- 0, 100, 200, 300, ..., 1000000 in kbps

Unit

Set or show the rate unit:

pps: packets per second

kbps: Kbits per second

4.31.2 ACL Rate Limiter Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.32 Security – Network – ACL – Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch.

Click on the lowest plus sign to add a new ACE to the list (the ACE Configuration page opens, see the description below). The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.



4.32.1 Access Control List Configuration

The ACL Access Control List Configuration Page has the following parameters:

ACE

Indicates the ACE ID.

Ingress Report

Display the ingress port of the ACE:

All: The ACE will match all ingress ports

Port: The ACE will match a specific ingress port

Policy/Bitmask

Display the policy number and bitmask of the ACE.

Frame Type

Display the frame type of the ACE:

- 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 are dropped
- Filter: Frames matching the ACE are filtered

Rate Limiter

Display the rate limiter number of the ACE.

The Rate Limiter can be Disabled or set to a value from 1 through 16. The default value is "Disabled".

Port Redirect

Display the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number.

The port redirect operation can be Disabled or set to a specific port number. The default value is "Disabled".

Mirror

Display the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port:

Enabled: Frames received on the port are mirrored

Disabled: Frames received on the port are not mirrored (The default value is "Disabled".)

Counter

The counter indicates the number of times the ACE was hit by a frame.

Modification Buttons

The user can modify each ACE (Access Control Entry) in the table using the following buttons:

- : Inserts a new ACE before the current row
- : Edits the ACE row
- : Moves the ACE up the list
- : Moves the ACE down the list
- : Deletes the ACE
- : The lowest plus sign adds a new entry at the bottom of the ACE listings

4.32.2 Access Control List Configuration Buttons

☐ Auto-refresh – Click this box to refresh the page automatically (every three seconds)

Refresh: Click to refresh the page, any changes made locally will be undone

Clear: Click to clear the counters

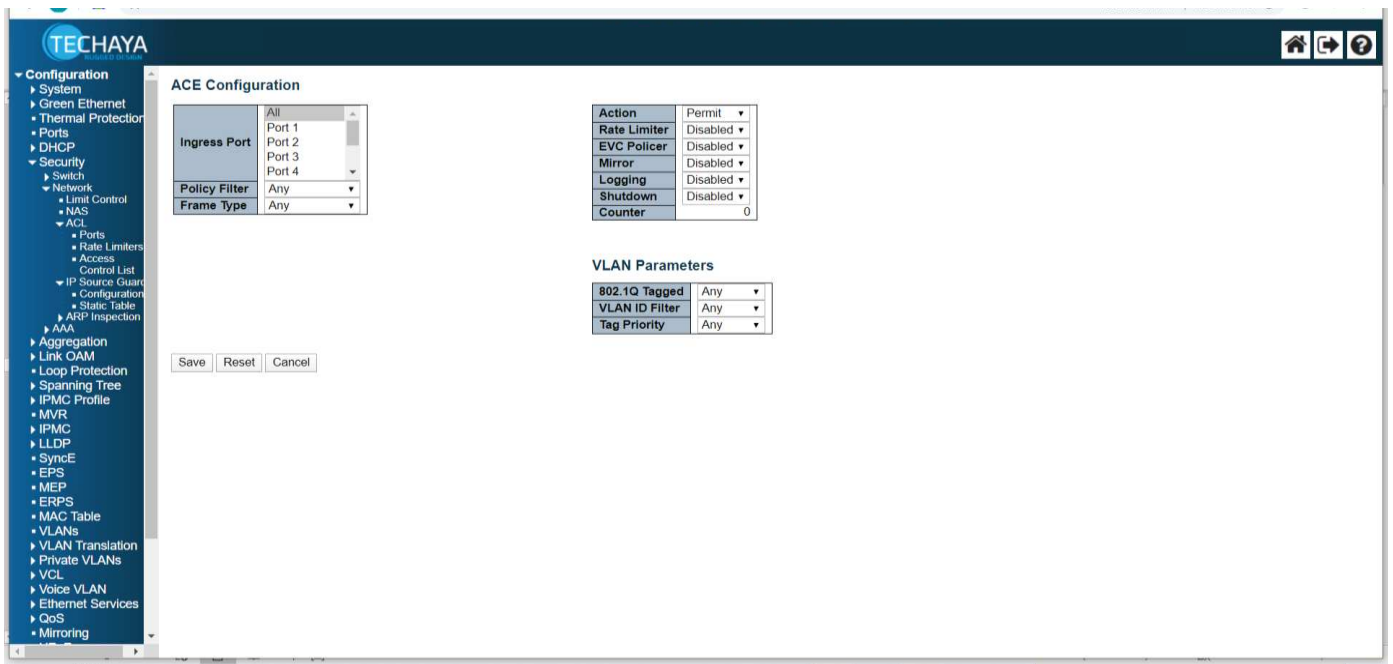
Remove All: Click to remove all ACEs

4.32.2.1 ACE Configuration

This page allows the user to configure an Access Control Entry (ACE). Open this page by clicking add () or edit () from the Access Control List Configuration table (see section 4.32 above).

An ACE consists of several parameters. These parameters vary according to the frame type that the user selects. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here.



ACE Configuration

Ingress Port: All, Port 1, Port 2, Port 3, Port 4

Policy Filter: Any

Frame Type: Any

Action	Permit
Rate Limiter	Disabled
EVC Policer	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

802.1Q Tagged	VLAN ID Filter	Tag Priority
Any	Any	Any

Save Reset Cancel

Ingress Report

Set or show the ingress port for which this ACE applies:

- All: The ACE applies to all port
- Port n: The ACE applies to this port number, where n is the number of the switch port.

Policy Filter

Set or show the policy number filter for this ACE.

- Any: No policy filter is specified. (policy filter status is “don’t-care”.)
- Specific: Filter a specific policy with this ACE. Two fields for entering a Policy Value and Policy Bitmask appear.

ACE Configuration	
Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0xff
Frame Type	Any

Policy Value

Displayed only when Policy Filter = Specific.

The user can enter a specific policy value. The allowed range is 0 to 255.

Policy Bitmask

Displayed only when Policy Filter = Specific.

The user can enter a specific policy bitmask. The allowed range is 0x0 to 0xff.

Note: The usage of bitmask, if the binary bit value is “0”, it means this bit is “don’t-care”. The real matched pattern is [Policy Value and Policy Bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is “don’t-care” bit), then policy 2 and 3 are applied to this rule.

Frame Type

Set or show the frame type for this ACE. These frame types are mutually exclusive.

- Any: Any frame can match this ACE
- Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal)
- ARP: Only ARP frames can match this ACE.

Note: The ARP frames won't match the ACE with Ethernet type.

IPv4: Only IPv4 frames can match this ACE.

Note: The IPv4 frames won't match the ACE with Ethernet type.

IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

Action

Set or show the action to take with a frame that hits this ACE.

Permit: The frame that hits this ACE is granted permission for the ACE operation

Deny: The frame that hits this ACE is dropped

Filter: Frames matching the ACE are filtered

Rate Limiter

Set or show the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.

EVC Policer

Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that the ACL rate limiter and EVC policer can not both be enabled.

EVC Policer ID

Select which EVC policer ID to apply on this ACE. The allowed values are Disabled or the values 1 through 256.

Port Redirect

Set or show the destination port number. Frames that hit the ACE are redirected to the port number specified here.

The rate limiter will affect these ports. The allowable values for port redirect are:

- "Disabled"
- A valid port number

When the Port Redirect is "Disabled" the Port Redirect operation is disabled and the specific port number of 'Port Redirect' cannot be set when the action is permitted.

Mirror

Set or show the mirror operation of this port.

Enabled: Frames received on the port are mirrored

Disabled: Frames received on the port are not mirrored (The default value is "Disabled".)

Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port.

Logging

Set or show the logging operation of the ACE:

Enabled: Frames matching the ACE are stored in the System Log

Disabled: Frames matching the ACE are not logged.

Note:

- The logging message doesn't include the 4 bytes CRC information.
- The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown

Set or show the port shut down operation of the ACE:

Enabled: If a frame matches the ACE, the ingress port will be disabled

Disabled: Port shut down is disabled for the ACE

Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

Counter

The counter indicates the number of times the ACE was hit by a frame.

4.32.2.2 MAC Parameters

MAC Parameters	
SMAC Filter	Specific ▼
SMAC Value	00-00-00-00-00-01
DMAC Filter	Specific ▼
DMAC Value	00-00-00-00-00-02

SMAC Filter

SMAC Filter is displayed only when the Frame Type is Ethernet Type or ARP.

Set or show the source MAC filter for this ACE.

Any: No SMAC filter is specified (SMAC filter status is "don't care".)

Specific: Filter a specific source MAC address with this ACE. A field for entering a SMAC value appears.

SMAC Value

When "Specific" is selected for the SMAC filter, the user can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

DMAC Filter

Set or show the destination MAC filter for this ACE.

- Any: No DMAC filter is specified (DMAC filter status is “don’t care”.)
- MC: Frame must be multicast
- BC: Frame must be broadcast
- UC: Frame must be unicast
- Specific: Filter a specific destination MAC address with this ACE. A field for entering a DMAC value appears.

DMAC Value

When “Specific” is selected for the DMAC filter, the user can enter a specific destination MAC address. The legal format is “xx-xx-xx-xx-xx-xx” or “xx.xx.xx.xx.xx.xx” or “xxxxxxxxxxxx” (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

4.32.2.3 VLAN Parameters

VLAN Parameters	
802.1Q Tagged	Enabled ▾
VLAN ID Filter	Specific ▾
VLAN ID	1
Tag Priority	Any ▾

802.1Q tagged

Set or show 802.1Q Tagged operation status. The status determines whether or not frames can hit the action according to the 802.1Q Tagged:

- Any: Any value is allowed (“don’t care”) (The default value is “Any”.)
- Enabled: Tagged frame only
- Disabled: Untagged frame only

VLAN ID Filter

Set or show the VLAN ID filter for this ACE.

- Any: No VLAN ID filter is specified. (VLAN ID filter status is “don’t care”.)
- Specific: Filter a specific VLAN ID with this ACE. A field for entering a VLAN ID number appears.

VLAN ID

When “Specific” is selected for the VLAN ID filter, the user can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.

Tag priority

Set or show the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value "Any" means that no tag priority is specified (tag priority is "don't care".)

4.32.2.4 ARP Parameters

The ARP parameters can be configured when Frame Type “ARP” is selected.

ARP Parameters	
ARP/RARP	Any ▼
Request/Reply	Any ▼
Sender IP Filter	Network ▼
Sender IP Address	0.0.0.0
Sender IP Mask	255.255.255.0
Target IP Filter	Network ▼
Target IP Address	0.0.0.0
Target IP Mask	255.255.255.0

ARP Sender MAC Match	Any ▼
RARP Target MAC Match	Any ▼
IP/Ethernet Length	Any ▼
IP	Any ▼
Ethernet	Any ▼

ARP/RARP

Set or show the available ARP/RARP opcode (OP) flag for this ACE

- Any: No ARP/RARP OP flag is specified. (OP is “don’t-care”.)
- ARP: Frame must have ARP opcode set to ARP
- RARP: Frame must have RARP opcode set to RARP
- Other: Frame has unknown ARP/RARP Opcode flag

Request/Reply

Set or show the available Request/Reply opcode (OP) flag for this ACE

- Any: No Request/Reply OP flag is specified. (OP is “don’t-care”.)
- Request: Frame must have ARP Request or RARP Request OP flag set
- Reply: Frame must have ARP Reply or RARP Reply OP flag

Sender IP Filter

Set or show the sender IP filter for this ACE.

- Any: No sender IP filter is specified. (Sender IP filter is “don’t care”.)
- Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears
- Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

Sender IP Address

When “Host” or “Network” is selected for the sender IP filter, the user can enter a specific sender IP address in dotted decimal notation.

Sender IP Mask

When “Network” is selected for the sender IP filter, the user can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter

Set or show the target IP filter for this specific ACE.

- Any: No target IP filter is specified. (Target IP filter is “don’t-care”.)
- Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears
- Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear

Target IP Address

When “Host” or “Network” is selected for the target IP filter, the user can enter a specific target IP address in dotted decimal notation.

Target IP Mask

When “Network” is selected for the target IP filter, the user can enter a specific target IP mask in dotted decimal notation.

ARP Sender MAC Match

Specify whether frames can hit the action according to their Sender Hardware Address field (SHA) settings.

- 0: Not a Match
ARP frames where SHA is **not** equal to the SMAC address
- 1: Match
ARP frames where SHA is equal to the SMAC address
- Any: Any value is allowed (“don’t care”).

RARP Target MAC Match

Specify whether frames can hit the action according to their target hardware address field (THA) settings.

- 0: Not a Match
RARP frames where THA is **not** equal to the target MAC address
- 1: Match
RARP frames where THA is equal to the target MAC address
- Any: Any value is allowed (“don’t-care”)

IP/Ethernet Length

Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

- 0: Not a Match
ARP/RARP frames where the HLN is **not** equal to Ethernet (0x06) or the (PLN) is **not** equal to IPv4 (0x04)
- 1: Match

ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04)

Any: Any value is allowed ("don't-care")

IP

Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

0: Not a Match

ARP/RARP frames where the HLD is **not** equal to Ethernet (1)

1: Match

ARP/RARP frames where the HLD is equal to Ethernet (1)

Any: Any value is allowed ("don't-care")

Ethernet

Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

0: Not a Match

ARP/RARP frames where the PRO is **not** equal to IP (0x800)

1: Match

ARP/RARP frames where the PRO is equal to IP (0x800)

Any: Any value is allowed ("don't-care")

4.32.2.5 IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

IP Parameters	
IP Protocol Filter	ICMP ▼
IP TTL	Any ▼
IP Fragment	Any ▼
IP Option	Any ▼
SIP Filter	Network ▼
SIP Address	0.0.0.0
SIP Mask	255.255.255.0
DIP Filter	Network ▼
DIP Address	0.0.0.0
DIP Mask	255.255.255.0

IP Protocol Filter

Set or show the IP protocol filter for this ACE.

Any: No IP protocol filter is specified ("don't care")

Specific: Filter a specific IP protocol filter with this ACE. A field for entering an IP protocol filter appears

- ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.
- UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.
- TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

IP Protocol Value

When "Specific" is selected for the IP protocol value, the user can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.

IP TTL

Set or show the Time-to-Live settings for this ACE.

- zero: IPv4 frames with a Time-to-Live field greater than zero must **not** be able to match this entry
- non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry
- Any: Any value is allowed ("don't care")

IP Fragment

Set or show the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

- No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must **not** be able to match this entry
- Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry
- Any: Any value is allowed ("don't care")

IP Option

Set or show the options flag setting for this ACE.

- No: IPv4 frames where the options flag is set must **not** be able to match this entry
- Yes: IPv4 frames where the options flag is set must be able to match this entry
- Any: Any value is allowed ("don't care")

SIP Filter

Set or show the source IP filter for this ACE.

- Any: No source IP filter is specified. (Source IP filter is “don’t care”.)
- Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.
- Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

SIP Address

When “Host” or “Network” is selected for the source IP filter, the user can enter a specific SIP address in dotted decimal notation.

SIP Mask

When “Network” is selected for the source IP filter, the user can enter a specific SIP mask in dotted decimal notation.

DIP Filter

Set or show the destination IP filter for this ACE.

- Any: No destination IP filter is specified. (Destination IP filter is “don’t care”.)
- Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.
- Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

DIP Address

When “Host” or “Network” is selected for the destination IP filter, the user can enter a specific DIP address in dotted decimal notation.

DIP Mask

When “Network” is selected for the destination IP filter, the user can enter a specific DIP mask in dotted decimal notation.

4.32.2.6 IPv6 Parameters

The IPv6 parameters can be configured when Frame Type “IPv6” is selected.

IPv6 Parameters	
Next Header Filter	Other
Next Header Value	255
SIP Filter	Specific
SIP Address (32 bits)	::
SIP Bitmask (32 bits)	0x FFFFFFFF
Hop Limit	Any

Next Header Filter

Set or show the IPv6 next header filter for this ACE.

- Any: No IPv6 next header filter is specified ("don't-care")
- Specific: Filter a specific IPv6 next header filter with this ACE. A field for entering an IPv6 next header filter appears.
- ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.
- UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.
- TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

Next Header Value

When "Other" is selected for the IPv6 Next Header Filter, the user can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.

SIP Filter

Set or show the source IPv6 filter for this ACE.

- Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't care".)
- Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.

SIP Address

When "Specific" is selected for the source IPv6 filter, the user can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.

SIP BitMask

When "Specific" is selected for the source IPv6 filter, the user can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address.

Note: The usage of bitmask, if the binary bit value is "0", it means this bit is "don't care". The real matched pattern is [sipv6_address and sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFF0 (bit 0 is "don't care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

Hop Limit

Set or show the hop limit settings for this ACE.

- zero: IPv6 frames with a hop limit field greater than zero must **not** be able to match this entry
- non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry
- Any: Any value is allowed ("don't care").

4.32.2.7 ICMPV6 Parameters

The ICMPV6 parameters can be configured when the Frame Type is "IPv6" and the Next Header Filter is "ICMP".

ICMPv6 Parameters	
ICMP Type Filter	Specific ▼
ICMP Type Value	255
ICMP Code Filter	Specific ▼
ICMP Code Value	255

ICMP Type Filter

Set or show the ICMP filter for this ACE.

- Any: No ICMP filter is specified (ICMP filter status is "don't care")
- Specific: To filter a specific ICMP filter with this ACE, the user can enter a specific ICMP value. A field for entering an ICMP value appears.

ICMP Type Value

When "Specific" is selected for the ICMP Type Filter, the user can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.

ICMP Code Filter

Set or show the ICMP code filter for this ACE.

- Any: No ICMP code filter is specified (ICMP code filter status is "don't care").
- Specific: To filter a specific ICMP code filter with this ACE, the user can enter a specific ICMP code value. A field for entering an ICMP code value appears.

ICMP Code Value

When "Specific" is selected for the ICMP Code Filter, you can enter a specific ICMP Code Value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.

4.32.2.8 TCPv6/UDPv6 Parameters

The TCPv6/UDPv6 parameters can be configured when the Frame Type is "IPv6" and the Next Header Filter is "TCP" or "UDP".

UDIPv6 Parameters	
Source Port Filter	Specific ▼
Source Port No.	0
Dest. Port Filter	Specific ▼
Dest. Port No.	0

Source Filter: "Specific"

Destination Filter: "Specific"

UDIPv6 Parameters	
Source Port Filter	Range ▼
Source Port Range	0 - 65535
Dest. Port Filter	Range ▼
Dest. Port Range	0 - 65535

Source Filter: "Range"

Destination Filter: "Range"

TCP/UDP Source Port Filter

Set or show the TCP/UDP source filter for this ACE.

- Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't care")
- Specific: To filter a specific TCP/UDP source filter with this ACE, the user can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.
- Range: To filter a specific TCP/UDP source range filter with this ACE, the user can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP/UDP Source Port Number

When "Specific" is selected for the TCP/UDP source filter, the user can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Port Range

When "Range" is selected for the TCP/UDP source filter, the user can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Destination Port Filter

Set or show the TCP/UDP destination filter for this ACE.

- Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't care").
- Specific: To filter a specific TCP/UDP destination filter with this ACE, the user can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.
- Range: To filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

TCP/UDP Destination Port Number

When "Specific" is selected for the TCP/UDP destination filter, the user can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Destination Port Range

When "Range" is selected for the TCP/UDP destination filter, the user can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP FIN

Set or show the TCP "No more data from sender" (FIN) value for this ACE.

- 0: TCP frames where the FIN field is set must **not** be able to match this entry
- 1: TCP frames where the FIN field is set must be able to match this entry
- Any: Any value is allowed ("don't care")

TCPv6 Parameters	
Source Port Filter	Any ▼
Dest. Port Filter	Any ▼
TCP FIN	Any ▼
TCP SYN	Any ▼
TCP RST	Any ▼
TCP PSH	Any ▼
TCP ACK	Any ▼
TCP URG	Any ▼

TCP SYN

Set or show the TCP "Synchronize Sequence Numbers" (SYN) value for this ACE.

- 0: TCP frames where the SYN field is set must **not** be able to match this entry
- 1: TCP frames where the SYN field is set must be able to match this entry
- Any: Any value is allowed ("don't care")

TCP RST

Set or show the TCP "Reset the connection" (RST) value for this ACE.

- 0: TCP frames where the RST field is set must **not** be able to match this entry
- 1: TCP frames where the RST field is set must be able to match this entry
- Any: Any value is allowed ("don't care")

TCP PSH

Set or show the TCP "Push Function" (PSH) value for this ACE.

- 0: TCP frames where the PSH field is set must **not** be able to match this entry

- 1: TCP frames where the PSH field is set must be able to match this entry
 Any: Any value is allowed ("don't-care")

TCP ACK

Set or show the TCP "Acknowledgment field significant" (ACK) value for this ACE.

- 0: TCP frames where the ACK field is set must **not** be able to match this entry
 1: TCP frames where the ACK field is set must be able to match this entry
 Any: Any value is allowed ("don't care")

TCP URG

Set or show the TCP "Urgent Pointer field significant" (URG) value for this ACE.

- 0: TCP frames where the URG field is set must **not** be able to match this entry
 1: TCP frames where the URG field is set must be able to match this entry
 Any: Any value is allowed ("don't care")

4.32.2.9 Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

Ethernet Type Parameters	
EtherType Filter	Specific ▼
Ethernet Type Value	0xFFFF

EtherType Filter

Set or show the Ethernet type filter for this ACE.

- Any: No EtherType filter is specified (EtherType filter status is "don't care")
 Specific: To filter a specific EtherType filter with this ACE, the user can enter a specific EtherType value. A field for entering an EtherType value appears.

Ethernet Type Value

When "Specific" is selected for the EtherType filter, the user can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

4.32.2.10 ACE Configuration Buttons

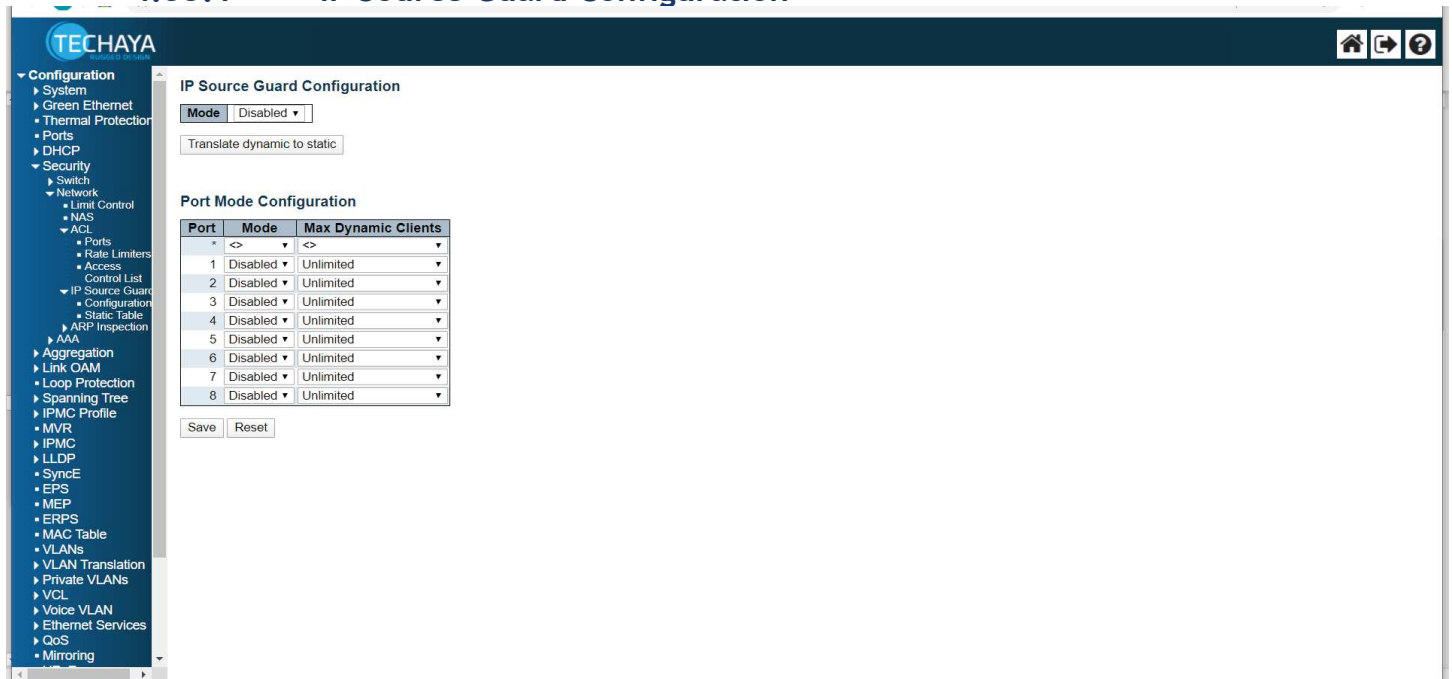
Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

Cancel: Return to the previous page

4.33 Security – Network – IP Source Guard Configuration

4.33.1 IP Source Guard Configuration



Mode of IP Source Guard Configuration

Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

4.33.2 Port Mode Configuration

Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

Max Dynamic Clients

Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

4.33.3 IP Source Buttons

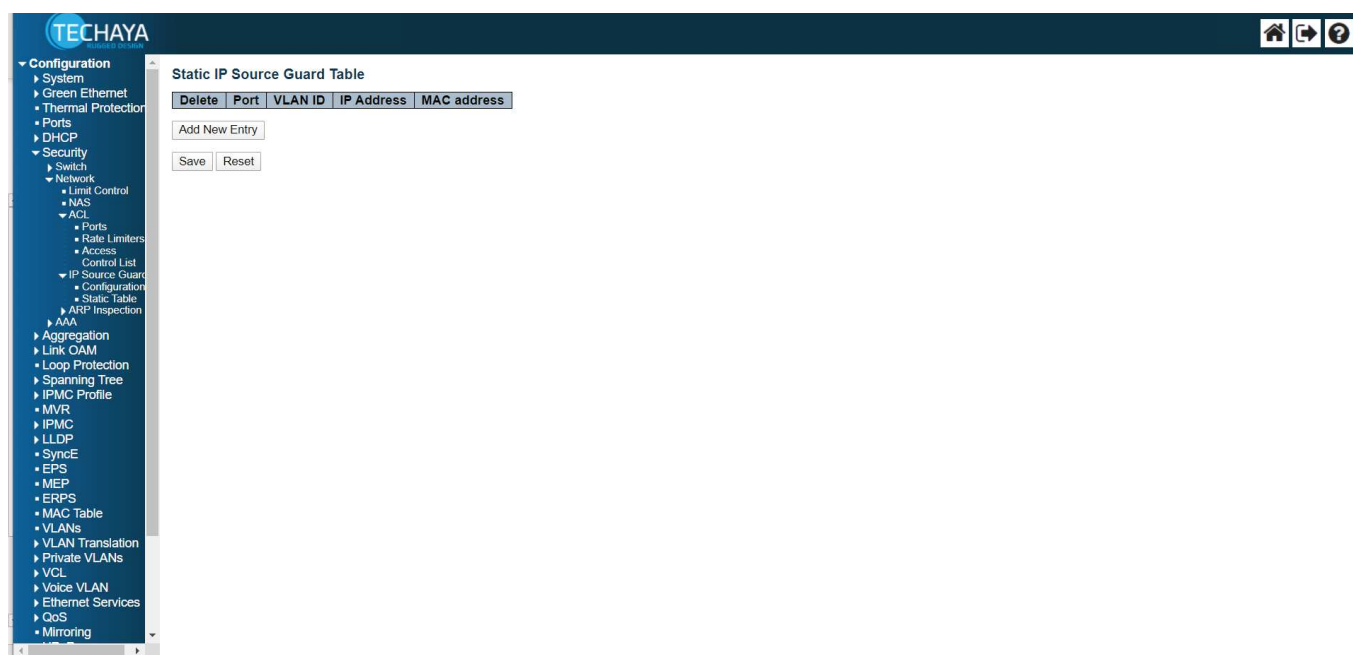
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Translate dynamic to static: Click to translate all dynamic entries to static entries.

Static Table

This page shows the static IP Source Guard rules. The maximum number of rules is 112 on the switch.



Delete

Check to delete the entry. It will be deleted during the next save.

Port

The logical port for the settings.

VLAN ID

The vlan id for the settings.

IP Address

Allowed Source IP address.

MAC Address

Allowed Source MAC address.

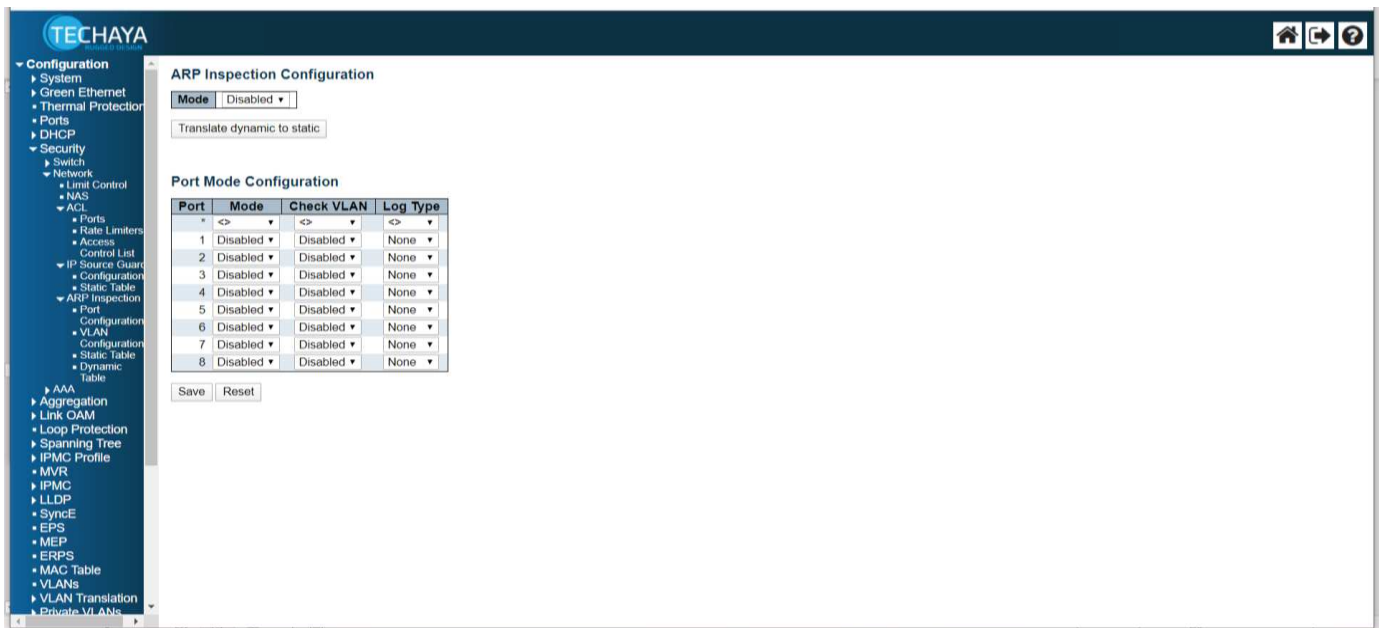
4.33.4 Static Table Buttons

Add new entry: Click to add a new entry to the Static IP Source Guard table.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.34 Security – Network – ARP Inspection – Port



This page provides ARP Inspection related configuration

4.34.1 Mode of ARP Inspection Configuration

Enable the Global ARP Inspection or disable the Global ARP Inspection.

4.34.2 Port Mode Configuration

Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:

Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.

If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:

Enabled: Enable check VLAN operation.

Disabled: Disable check VLAN operation.

Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

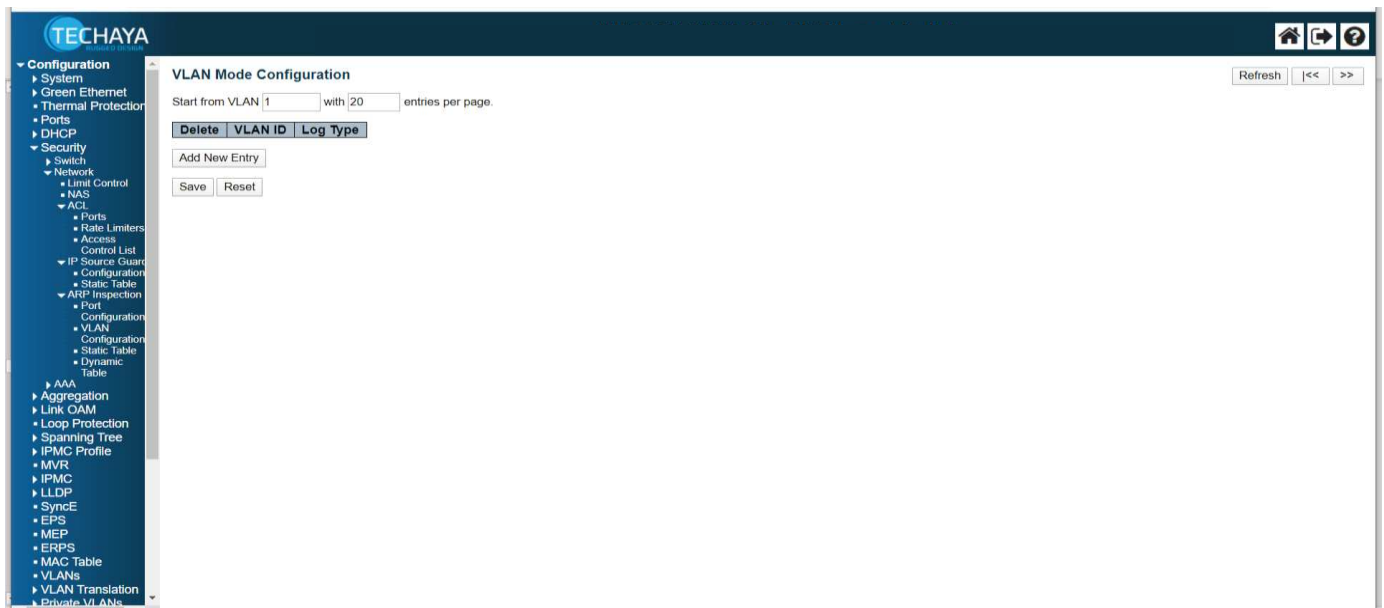
4.34.3 **ARP Inspection Port Buttons**

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Translate dynamic to static: Click to translate all dynamic entries to static entries.

4.35 Security – Network – ARP Inspection – VLAN



Navigating the VLAN Configuration

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next VLAN Table match. The >> will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the << button to start over.

4.35.1 VLAN Mode Configuration

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.

Possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

4.35.2 ARP Inspection VLAN Buttons

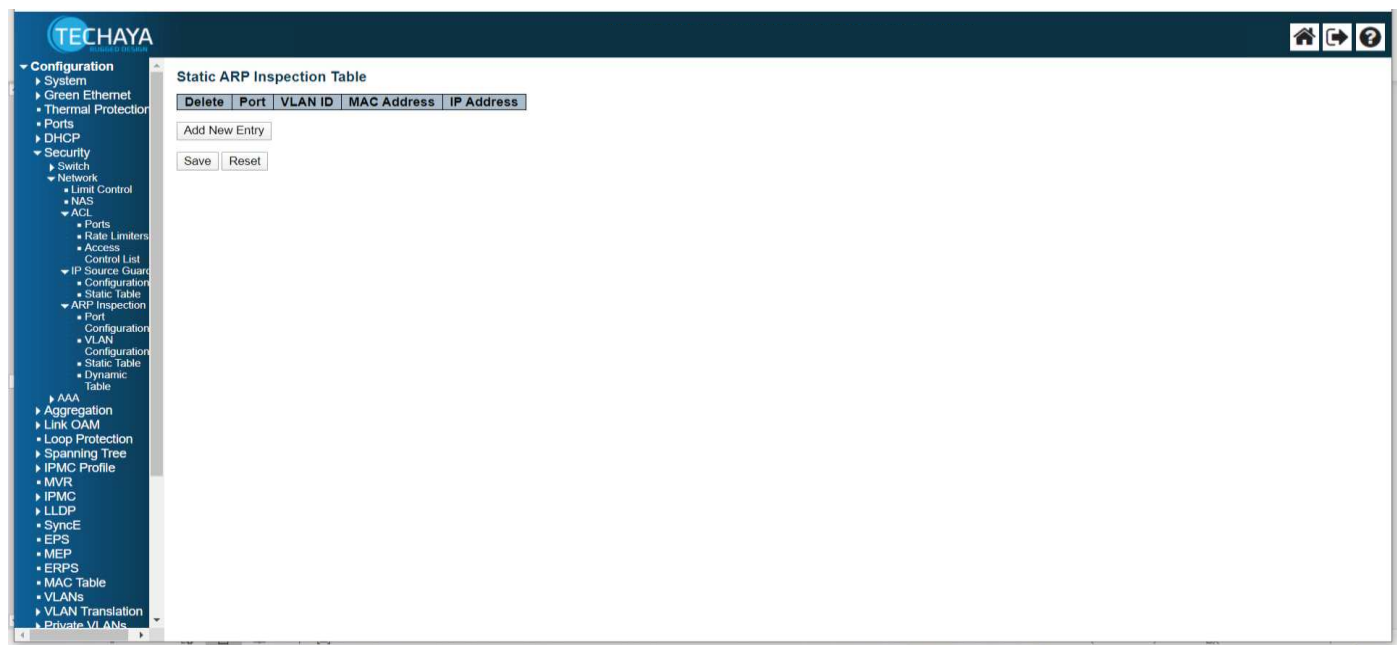
Add new entry: Click to add a new VLAN to the ARP Inspection VLAN table.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.36 Security – Network – ARP Inspection – Static Table

This page shows the static ARP Inspection rules. The maximum number of rules is 256 on the switch.



Delete

Check to delete the entry. It will be deleted during the next save.

Port

The logical port for the settings.

VLAN ID

The vlan id for the settings.

MAC Address

Allowed Source MAC address in ARP request packets.

IP Address

Allowed Source IP address in ARP request packets.

Static Table Buttons

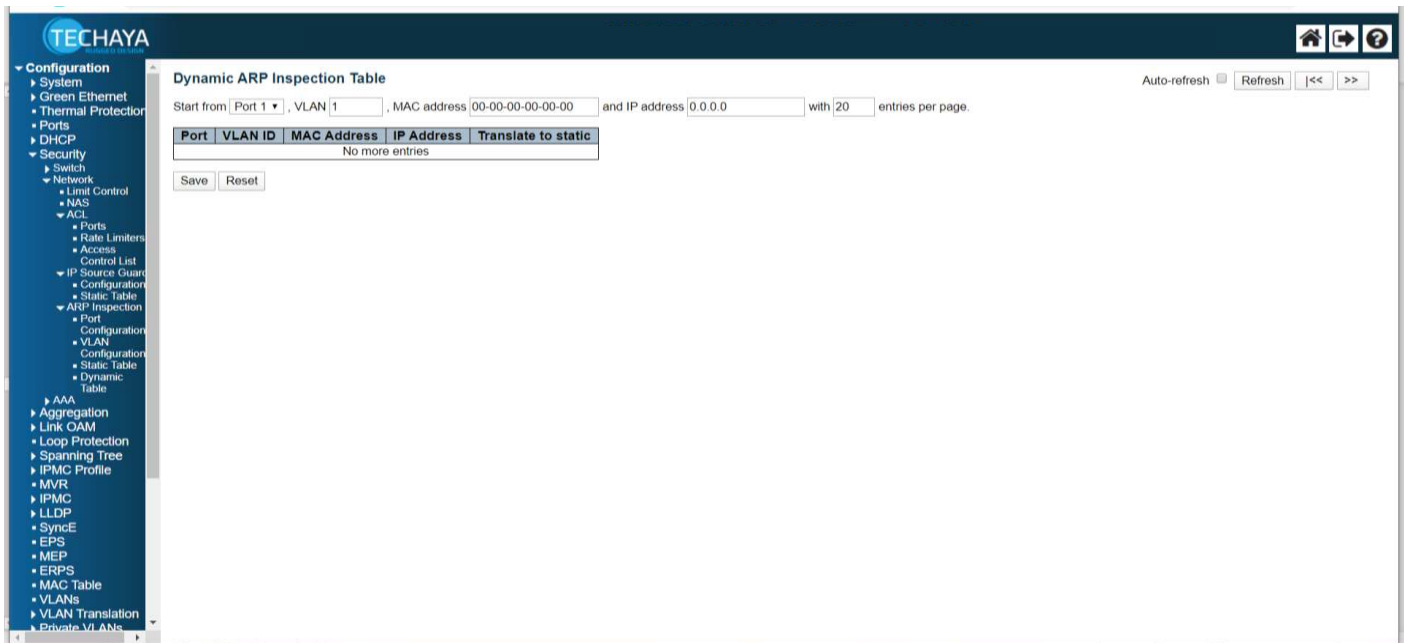
Add new entry: Click to add a new entry to the Static ARP Inspection table.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.37 Security – Network – ARP Inspection – Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.



Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

ARP Inspection Table Columns

Port

Switch Port Number for which the entries are displayed.

VLAV ID

The vlan id in which the ARP traffic is permitted

MAC Address

User MAC address of the entry.

IP Address

User IP address of the entry.

Translate to static

Select the checkbox to translate the entry to static entry.

Dynamic Table Buttons

Refresh: Click to refresh the page, any changes made locally will be undone.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

|<<: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.38 Security – AAA – Radius

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RADIUS Server Configuration

This page allows the user to configure RADIUS Server parameters.

TECHAYA

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						

4.38.1 Global Configuration

These settings are common for all of the RADIUS servers.

Timeout

Set or show the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit

Set or show the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit, it is considered to be dead.

Deadtime

Set or show the period, a number between 0 to 1440 minutes, 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.

Key

Set or show secret key - up to 63 characters long - shared between the RADIUS server and the switch.

NAS-IP-Address

IPv4 (Attribute 4)

Set or show the IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

IPv6 (Attribute 95)

Set or show the IPv6 address to be 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 (Attribute 32)

Set or show the identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

4.38.2 Server Configuration

The table has one row for each RADIUS server and a number of columns, with the following parameters:

Delete

☒ Check to delete a RADIUS server entry. The entry will be deleted during the next save.

☐ Do not delete the entry. (This is the default.)

Hostname

Set or show the IP address or hostname of the RADIUS server.

Auth Port

The UDP port to use on the RADIUS server for authentication.

Acct Port

Set or show the UDP port to use on the RADIUS server for accounting.

Timeout

Set or show this optional setting that overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit

Set or show this optional setting that overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Key

Set or show this optional setting that overrides the global key. Leaving it blank will use the global key.

4.38.3 RADIUS Server Configuration Buttons**Add New Server:**

Click to add a new RADIUS Server entry. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.

Delete: Click to undo the addition of the new server.

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.39 Security – AAA – TACACS+

These settings are common for all of the TACACS+ servers.

TACACS+ Server Configuration

TACACS+ Server Configuration

Global Configuration

Timeout: 5 seconds
 Deadtime: 0 minutes
 Key:

Server Configuration

Delete	Hostname	Port	Timeout	Key
Add New Server				

Save Reset

4.39.1 Global Configuration

This page allows the user to configure TACACS+ Server parameters

Timeout

Set or show the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

Deadtime

Set or show the period, a number between 0 to 1440 minutes, 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.

Key

Set or show secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

4.39.2 Server Configuration

The table has one row for each TACACS+ server and a number of columns, with the following parameters:

Delete

☒ Check to delete a TACACS+ server entry. The entry will be deleted during the next save.

☐ Do not delete the entry. (This is the default.)

Hostname

Set or show the IP address or hostname of the TACACS+ server.

Port

The TCP port to use on the TACACS+ server for authentication.

Timeout

Set or show this optional setting that overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Key

This optional setting overrides the global key. Leaving it blank will use the global key.

4.39.3 TACACS+ Server Configuration Buttons

Add New Server:

Click to add a new TACACS+ Server entry. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

Delete: Click to undo the addition of the new server.

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.40 Aggregation – Static

Aggregation mode uses multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability. This page allows the user to configure Aggregation Mode parameters.

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation**
 - Static
 - LACP
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD
- Monitor
- Diagnostics

Aggregation Mode Configuration

Hash Code Contributors

Source MAC Address ☒

Destination MAC Address ☐

IP Address ☒

TCP/UDP Port Number ☒

Aggregation Group Configuration

Group ID	Port Members							
	1	2	3	4	5	6	7	8
Normal	☒	☒	☒	☒	☒	☒	☒	☒
1	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐

Save Reset

4.40.1 Aggregation Mode Configuration Hash Code Contributors

This section allows the user to configure Hash Code Contributors:

Source MAC Address

The Source MAC address can be used to calculate the destination port for the frame. By default, Source MAC Address is enabled.

- ☒ Check to enable the use of the Source MAC address (This is the default.)
- ☐ Uncheck to disable the use of the Source MAC address

Destination MAC Address

The Destination MAC Address can be used to calculate the destination port for the frame. By default, Destination MAC Address is disabled.

- ☒ Check to enable the use of the Destination MAC Address
- ☐ Uncheck to disable the use of the Destination MAC Address (This is the default.)

IP Address

The IP address can be used to calculate the destination port for the frame. By default, IP Address is enabled.

- ☒ Check to enable the use of the IP Address (This is the default.)
- ☐ Uncheck to disable the use of the IP Address

TCP/UDP Port Number

The TCP/UDP port number can be used to calculate the destination port for the frame. By default, TCP/UDP Port Number is enabled.

- ☒ Check to enable the use of the TCP/UDP Port Number (This is the default.)
- ☐ Uncheck to disable the use of the TCP/UDP Port Number

4.40.2 Aggregation Group Configuration

This section allows the user to configure aggregation groups.

Group ID

Set or show the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

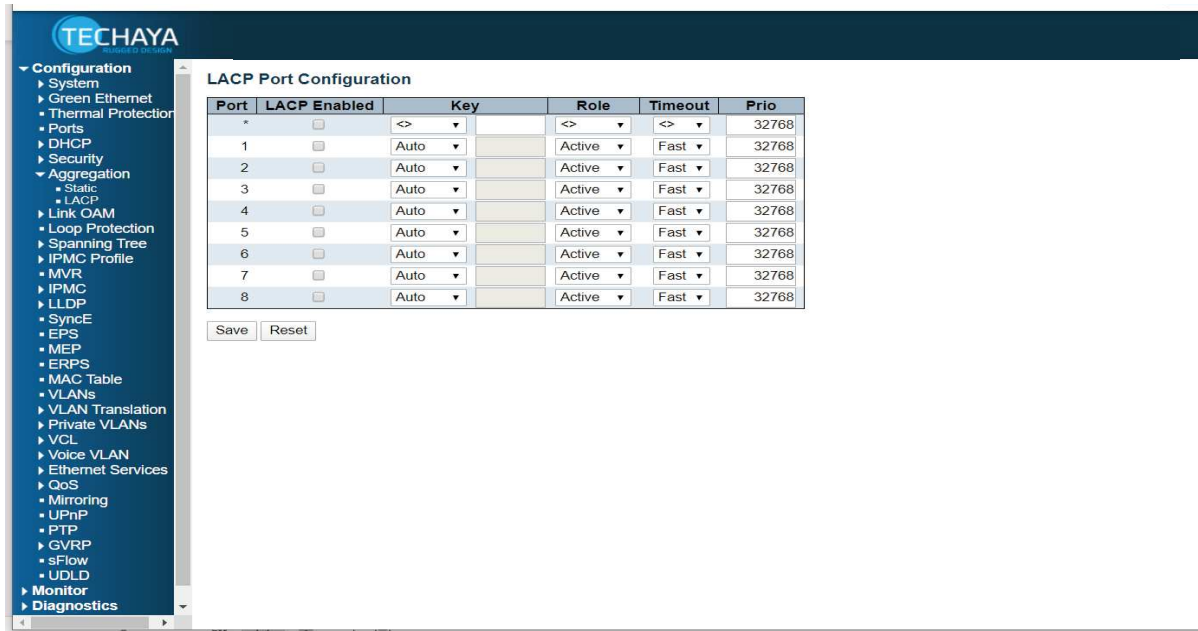
4.40.3 Aggregation Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.41 Aggregation – LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.



4.41.1 LACP Port Configuration

This page allows the user to inspect and change LACP Port configurations:

Port

This column displays the switch port number.

LACP Enabled

Set or show whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.

- ☒ LACP is enabled on this switch port
- ☐ LACP is disabled on this switch port (This is the default.)

Up to 32 aggregations are supported (if stackable).

Key

Set or show the Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.

Role

Set or show the LACP activity status:

Active: Transmit LACP packets each second

Passive Wait for an LACP packet from a partner (speak if spoken to)

Timeout

Set or show the period between BPDU transmissions.

Fast Transmit LACP packets each second

Slow Wait for 30 seconds before sending a LACP packet

Prio

Set or show the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

4.41.2 LACP Port Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.42 Link OAM – Port

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD
- Monitor
- Diagnostics

Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	☐	<>	☐	☒	☐	☐
1	☐	Passive	☐	☒	☐	☐
2	☐	Passive	☐	☒	☐	☐
3	☐	Passive	☐	☒	☐	☐
4	☐	Passive	☐	☒	☐	☐
5	☐	Passive	☐	☒	☐	☐
6	☐	Passive	☐	☒	☐	☐
7	☐	Passive	☐	☒	☐	☐
8	☐	Passive	☐	☒	☐	☐

Save Reset

4.42.1 Link OAM Port Configuration

This page allows the user to inspect and change Link OAM Port configurations:

Port

This column displays the switch port number.

OAM Enabled

Controls whether Link OAM is enabled on this switch port. Enabling Link OAM provides the network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

OAM Mode

Configures the OAM Mode as Active or Passive. The default mode is Passive.

Active mode

DTE's configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.

Passive mode

DTE's configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDUs.

Set or show the LACP activity status:

Active: Transmit LACP packets each second

Passive Wait for an LACP packet from a partner (speak if spoken to)

Lookback Support

Controls whether the loopback support is enabled for the switch port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.

Link Monitor Support

Controls whether the Link Monitor support is enabled for the switch port. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.

MIB Retrieval Support

Controls whether the MIB Retrieval Support is enabled for the switch port. On enabling the MIB retrieval support, the DTE supports polling of various Link OAM based MIB variables' contents.

Loopback Operation

If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

4.42.2 Link OAM Port Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.43 Link OAM – Event

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
 - Port Settings
 - Event Settings
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD
- Monitor
- Diagnostics

Link Event Configuration for Port 1

Port 1

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

Save Reset

4.43.1 Link Event Configuration

This page allows the user to inspect the current Link OAM Link Event configurations and change them as well.

Event Name

Name of the Link Event which is being configured.

Error Window

Represents the window period in the order of 1 sec for the observation of various link events.

Error Threshold

Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

Error Frame Event

The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '0'.

Symbol Period Error Event

The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '0'.

Seconds Summary Event

The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be between 0-65535 and its default value is '1'.

4.43.2 Link Event Configuration Buttons

The **port** select box determines which port is affected by clicking the buttons.

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.44 Loop Protection (Configuration)

When loop protection is enabled, the spanning-tree topology detects root ports and blocked ports and makes sure both keep receiving BPDUs.

This page allows the user to inspect and change the Loop Protection Configuration.

TECHAYA
Simplified Design

▼ Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD
- Monitor
- Diagnostics
- Maintenance

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 ▼

Save Reset

4.44.1 General Settings

This section allows the user to configure the Global Configuration settings:

Enable Loop Protection

Set or show the global Loop Protection status:

Enabled: Loop Protection is enabled (globally)

Disabled: Loop Protection is disabled (globally)(This is the default.)

Transmission Time

Set or show the interval between each loop protection PDU sent on each port.

Valid values are 1 to 10 seconds. Default value is 5 seconds.

Shutdown Time

The period (in seconds) for which a port will be kept disabled in the event a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800

seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds.

4.44.2 Port Configuration

Port

This column displays the switch port number.

Enable

Set or show whether Loop Protection is enabled on this switch port.

☒ Loop Protection is enabled on this switch port (This is the default.)

☐ Loop Protection is disabled on this switch

Action

Set or show the action to perform when a loop is detected on a port. Valid values are:

- Shutdown Port
- Shutdown Port and Log
- Log Only.

Tx Mode

Set or show whether the port is actively generating loop protection PDUs

Enabled: Port is actively generating loop protection PDUs

Disabled: Port is passively looking for looped PDUs

4.44.3 Loop Protection Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.45 Spanning Tree – Bridge Settings

This page allows the user to configure Spanning Tree Protocol (STP) system settings. The settings are used by all STP Bridge instances in the Switch.

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - CIST Ports
 - MSTI Ports
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD

STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	128
Hello Time	2
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

4.45.1 STP Bridge Configuration - Basic Settings

This section allows the user to configure the Bridge Configuration Basic settings:

Protocol Version

Set or show the MSTP/ RSTP/ STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority

Set or show the Bridge priority. Lower numeric values have higher priority. The Bridge Priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP Bridge.

Hello Time

The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds.

Note: Changing this parameter from the default value is not recommended, and may have adverse effects on your network.

Forward Delay

Set or show the delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age

Set or show the maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range from 6 to 40 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1)*2$.

Maximum Hop Count

Set or show the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count

Set or show the number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDUs per second.

4.45.2 STP Bridge Configuration - Advanced Settings

This section allows the user to configure the Bridge Configuration Advanced settings:

Edge Port BPDU Filtering

Set or show Edge Port BPDU Filtering status.

When Edge Port BPDU Filtering is enabled, a port explicitly configured as Edge will transmit and receive BPDUs.

- ☒ Edge Port BPDU Filtering is enabled
- ☐ Edge Port BPDU Filtering is disabled (This is the default.)

Edge Port BPDU Guard

Set or show Edge Port BPDU Guard status.

When Edge Port BPDU Guard is enabled, a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

- ☒ Edge Port BPDU Guard is enabled
- ☐ Edge Port BPDU Guard is disabled (This is the default.)

Port Error Recovery

Set or show Port Error Recovery status.

When Port Error Recovery is enabled, a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

- ☒ Port Error Recovery is enabled
- ☐ Port Error Recovery is disabled (This is the default.)

Port Error Recovery Timeout

Set or show the time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

4.45.3 STP Bridge Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.46 Spanning Tree – MSTI Mapping

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

TECHAYA
PROVIDER DESIGN

▼ Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- ▼ Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - CIST Ports
 - MSTI Ports
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name: 02-00-c1-93-4a-5f

Configuration Revision: 0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Save Reset

4.46.1 MSTI Configuration Identification

This section allows the user to configure the MSTI settings

Configuration Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

4.46.2 MSTI Mapping

MSTI

The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped

The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2,5,20-40.

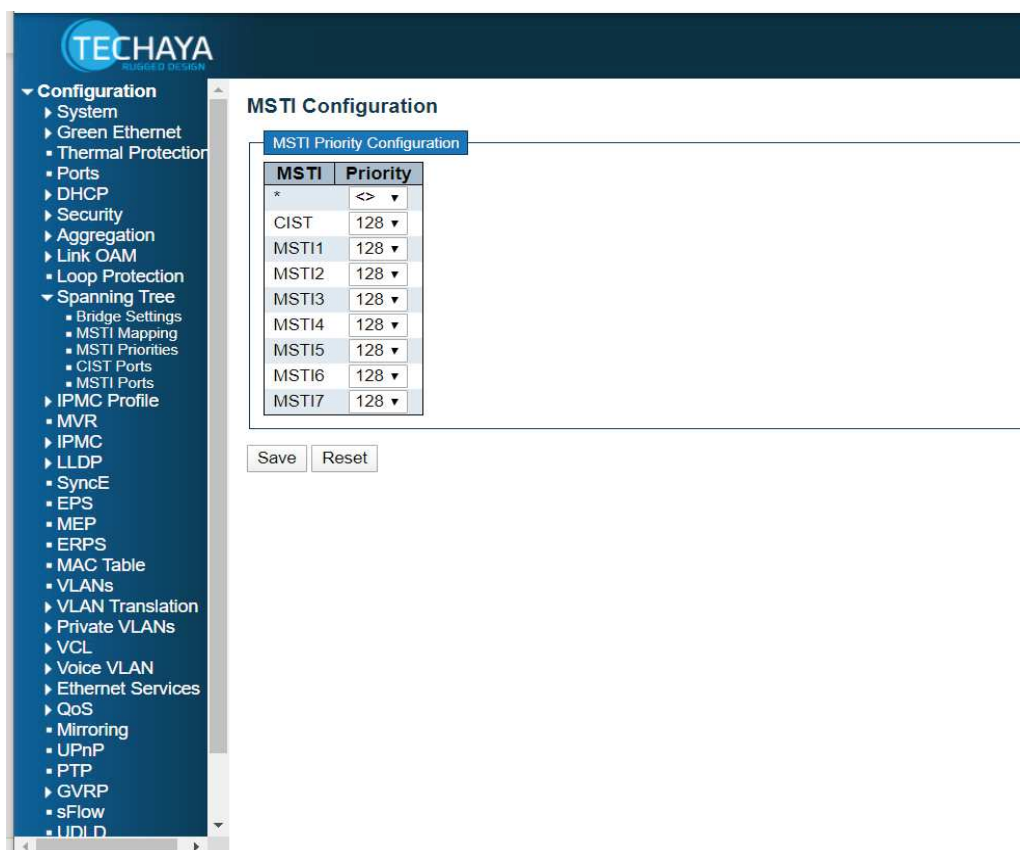
4.46.3 MSTI Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.47 Spanning Tree – MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



4.47.1 STP MSTI Priority Configuration

The bridge instance. The CIST is the default instance, which is always active.

Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

4.47.2 STP MSTI Priority Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.48 Spanning Tree – Bridge CIST Ports

This page allows the user to inspect and change the current Spanning Tree Protocol (STP) Common Internal Spanning Tree (CIST) port configurations.

This page contains settings for physical and aggregated 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

Save Reset

4.48.1 STP CIST Port Configuration

This section allows the user to configure the Bridge Configuration Basic settings (the parameters are the same for aggregated and normal ports):

Port

This column displays the switch port number of the logical STP port.

STP Enabled

Set or show the STP status for this switch port.

☒ STP is enabled on this switch port (This is the default.)

☐ STP is disabled on this switch port

Path Cost

Set or show the path cost incurred by the port.

Auto: Sets the path cost as appropriately, for the physical link speed, using the 802.1D recommended values.

Specific: The user enters a value to define the path cost.

The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200,000,000.

Priority

Set or show the port priority. This can be used to control priority of ports having identical port cost. (See above).

operEdge (state flag)

Displays the operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

AdminEdge

Set or show whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

Edge: operEdge flag should start as set

Non- Edge: operEdge flag is not set

AutoEdge

Set or show the AutoEdge status for this bridge port.

☒ Enable automatic edge detection on the bridge port (This is the default.)

☐ Disable automatic edge detection on the bridge port

This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role

Set or show the Restricted Role status for this bridge port.

☒ Enabled – port will **not** be selected as a Root Port for the CIST or any MSTI

☐ Disabled – port may be selected as a Root Port for the CIST or any MSTI (This is the default.)

If enabled, the port will not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If enabled, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN

Set or show the Restricted TCN (Topology Change Notification) status for this bridge port.

- ☒ Enabled – port will **not** propagate received topology change notifications and topology changes to other ports
- ☐ Disabled – port may propagate received topology change notifications and topology changes to other ports (This is the default.)

If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard

Set or show the BPDU Guard status for this bridge port.

- ☒ Enabled – The Port will disable itself upon receiving valid BPDUs
- ☐ Disabled – The Port will **not** disable itself upon receiving valid BPDUs (This is the default.)

Contrary to the similar bridge setting, the port Edge status does not affect this setting.

A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery (shown on page 253) setting as well.

Point-to-Point

Set or show whether the port connects to a point-to-point LAN rather than to a shared medium.

Auto:	Determine automatically
Forced True	Force to true
Forced False	Force to false

Transition to the forwarding state is faster for point-to-point LANs than for shared media.

4.48.2 STP CIST Port Configuration Buttons

Save: Click to save all changes

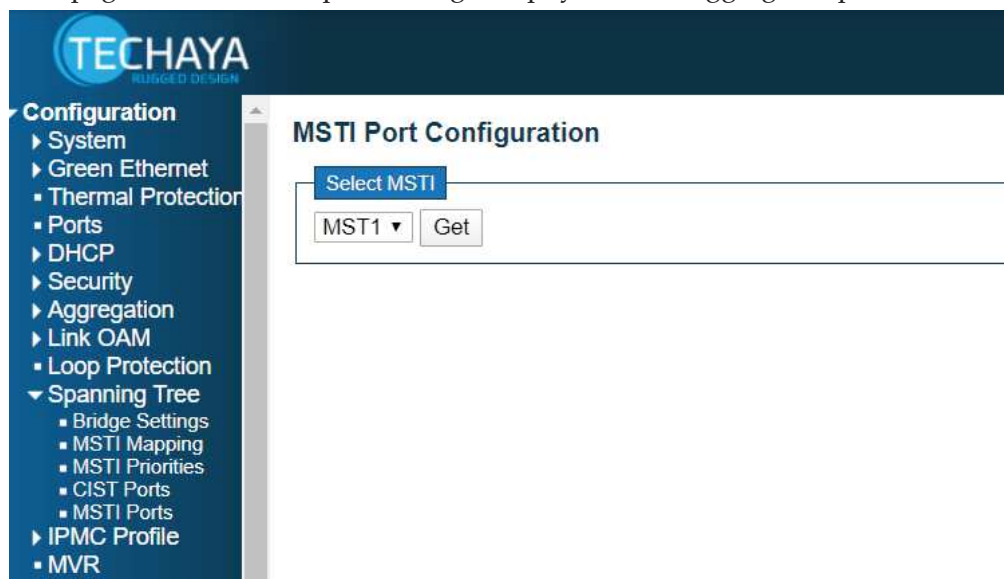
Reset: Click to undo any changes made locally and revert to previously saved values

4.49 Spanning Tree – MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports.



The screenshot displays the TECHAYA web interface. On the left, a dark blue sidebar contains a 'Configuration' menu with the following items: System, Green Ethernet, Thermal Protection, Ports, DHCP, Security, Aggregation, Link OAM, Loop Protection, Spanning Tree (expanded), IPMC Profile, and MVR. Under 'Spanning Tree', the sub-items are Bridge Settings, MSTI Mapping, MSTI Priorities, CIST Ports, and MSTI Ports. The main content area has a title 'MSTI Port Configuration'. Below the title is a 'Select MSTI' dropdown menu with 'MST1' selected and a 'Get' button.

4.49.1 STP MSTI Port Configuration

Port

The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost

Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

4.49.2 STP MSTI Port Buttons

Get: Click to retrieve settings for a specific MSTI.

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.49.3 MSTI Port Configuration - Get

Allow to retrieve settings for a specific MSTI.

TECHAYA
SERVICIOS DE SUMIN

▼ Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- ▼ Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - CIST Ports
 - MSTI Ports
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto	128

MSTI Normal Ports Configuration

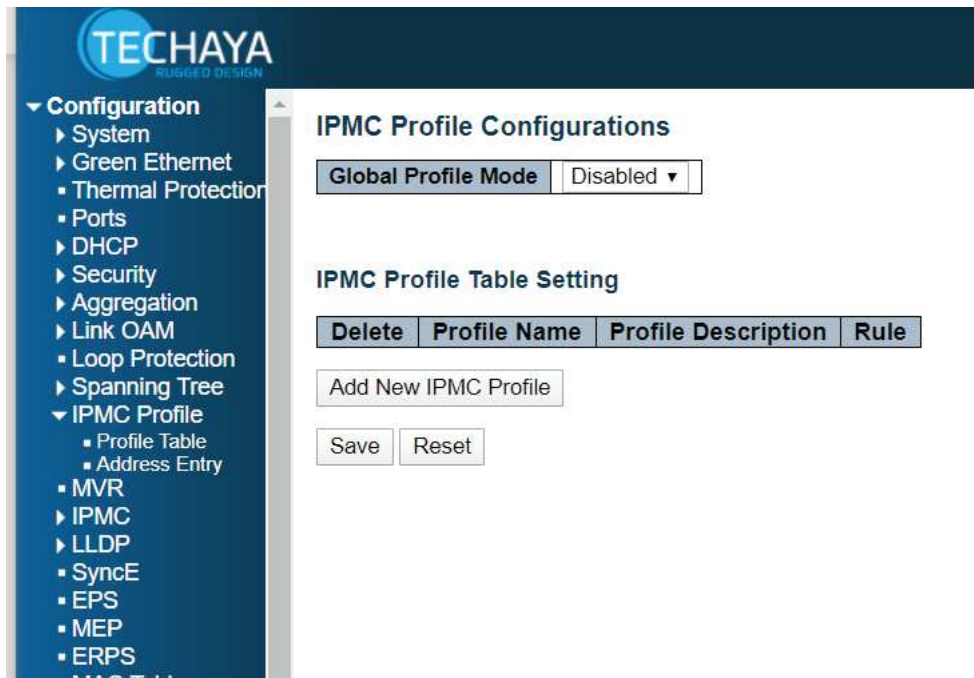
Port	Path Cost	Priority
*	<>	<>
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128
5	Auto	128
6	Auto	128
7	Auto	128
8	Auto	128

Save Reset

4.50 IPMC – Profile Table

This page provides IPMC Profile related configurations.

The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.



4.50.1 IPMC Profile Configurations

Global Profile Mode

Set or show Global IPMC profile.

- ☒ Enable the Global IPMC Profile.
- ☐ Disable the Global IPMC Profile (This is the default.)

System starts to do filtering based on profile settings only when the global profile mode is enabled.

Delete

Check to delete the entry.

The designated entry will be deleted during the next save.

The name used for indexing the profile table.

Profile Name

Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

Profile Description

Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.

No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.

Rule

When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:

: List the rules associated with the designated profile.

: Adjust the rules associated with the designated profile.

4.50.2 IPMC Profile Buttons

Add New IPMC Profile:

Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save".

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.51 IPMC – Address Entry

This page provides address range settings used in IPMC profile.

The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system.

4.51.1 IPMC Profile Address Entry Table

Delete

Check to delete the entry.

The designated entry will be deleted during the next save.

The name used for indexing the profile table.

Entry Name

The name used for indexing the address entry table.

Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

Start Address

The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

End Address

The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

4.51.2 IPMC Profile Buttons**Add New IPMC Profile:**

Click to add new address range. Specify the name and configure the addresses. Click "Save".

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the IPMC Profile Address Configuration.

>>: Updates the table starting with the entry after the last entry currently displayed.

4.52 MVR

This page provides MVR related configurations.

TECHAYA
RUGGED DESIGN

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - GIST Ports
 - MSTI Ports
- IPMC Profile
 - MVR
 - IPMC
 - LLDP
 - SyncE
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLANs
 - VLAN Translation
 - Private VLANs
 - VCL
 - Voice VLAN
 - Ethernet Services
 - QoS
 - Mirroring
 - UPnP
 - PTP
 - GVRP
 - sFlow
 - UDLD

MVR Configurations

MVR Mode: Disabled ▼

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
Add New MVR VLAN								

Immediate Leave Setting

Port	Immediate Leave
*	<> ▼
1	Disabled ▼
2	Disabled ▼
3	Disabled ▼
4	Disabled ▼
5	Disabled ▼
6	Disabled ▼
7	Disabled ▼
8	Disabled ▼

Save Reset

4.52.1 MVR Configurations

The MVR feature enables multicast traffic forwarding on the Multicast VLANs.

In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

It is allowed to create at maximum 4 MVR VLANs with corresponding channel profile for each Multicast VLAN.

The channel profile is defined by the IPMC Profile which provides the filtering conditions.

Mode

Enable/Disable the Global MVR.

The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping.

It is suggested to enable Unregistered Flooding control when the MVR group table is full.

Delete

Check to delete the entry.

The designated entry will be deleted during the next save.

MVR ID

Specify the Multicast VLAN ID.

Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name

MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

IGMP Address

Define the IPv4 address as source address used in IP header for IGMP control frames.

The default IGMP address is not set (0.0.0.0).

When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Mode

Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

Targeting

Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.

Priority

Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

LLQI

Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

Interface Channel Profile

When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:



: List the rules associated with the designated profile.

Port

The logical port for the settings.

Configure an MVR port of the designated MVR VLAN as one of the following roles.

Port Role

Inactive: The designated port does not participate MVR operations.

Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.

Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

Select the port role by clicking the Role symbol to switch the setting.

I indicates Inactive; S indicates Source; R indicates Receiver

The default Role is Inactive.

Immediate Leave

Enable the fast leave on the port.

4.52.2 MVR Buttons

Add New MVR VLAN:

Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save".

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.53 IPMC – IGMP Snooping - Basic Configuration

4.53.1 IGMP Snooping Configuration

This page provides IGMP Snooping related configuration.

TECHAYA
RUGGED DESIGN

- Configuration
 - System
 - Green Ethernet
 - Thermal Protection
 - Ports
 - DHCP
 - Security
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - CIST Ports
 - MSTI Ports
 - IPMC Profile
 - MVR
 - IPMC
 - IGMP Snooping
 - Basic Configuration
 - VLAN Configuration
 - Port Filtering Profile
 - MLD Snooping
 - LLDP
 - SyncE
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLANs
 - VLAN Translation
 - Private VLANs
 - VCL
 - Voice VLAN
 - Ethernet Services

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

Save Reset

Snooping Enabled

Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled

Enable unregistered IPMCv4 traffic flooding.

The flooding control takes effect only when IGMP Snooping is enabled.

When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

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.

Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.

Leave Proxy Enabled

Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

4.53.2 IGMP Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.54 IPMC – IGMP Snooping - VLAN Configuration

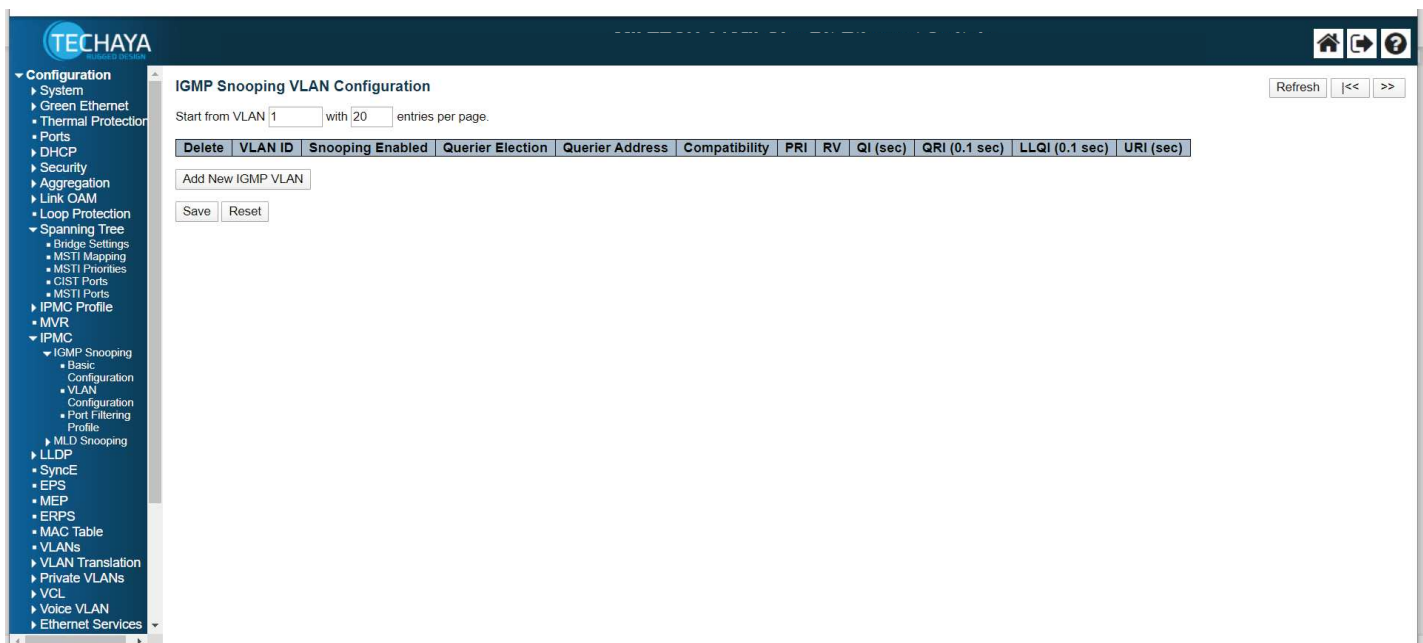
Navigating the IGMP Snooping VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The “VLAN” input fields allow the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match.

The **Forward Arrows** () button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the

Back Arrows button () to start over.



4.54.1 IGMP Snooping VLAN Configuration

This page allows the user to configure the IGMP Snooping VLAN parameters:

Delete

- ☒ Check to delete a VLAN entry. The entry will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

VLAN ID

Set or show the VLAN ID of the entry.

IGMP Snooping Enabled

Set or show the per VLAN IGMP Snooping status.

- ☒ Enable the Global IGMP Snooping
- ☐ Disable the Global IGMP Snooping (This is the default.)

Up to 32 VLANs can be selected for IGMP Snooping.

Querier Election

- ☒ Enable this entry to join IGMP Querier election in the VLAN (This is the default.)
- ☐ Disable this entry to act as an IGMP Non-Querier

Querier election is used to dedicate the Querier. This is the only Querier to which the sends Query messages, on a particular link.

Querier election rule determines that IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

Querier Address

Set or show the IPv4 address as source address used in IP header for IGMP IGMP Querier election.

When the Querier address is not set, the system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

This column displays the switch port number of the logical STP port.

Compatibility

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.

The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

PRI

Priority of Interface.

It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

RV

Robustness Variable.

The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2.

QI

Query Interval.

The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI

Query Response Interval.

The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.

The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP)

Last Member Query Interval.

The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count.

The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).

The logical port for the settings. Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group.

The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

4.54.2 IGMP Snooping VLAN Configuration Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

Back Arrows (): Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

Forward Arrows (): Updates the table, starting with the entry after the last entry currently displayed.

Add a New IGMP VLAN:

Click to add new IGMP VLAN. Specify the VID and configure the new entry. After creation of the new entry the user must click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

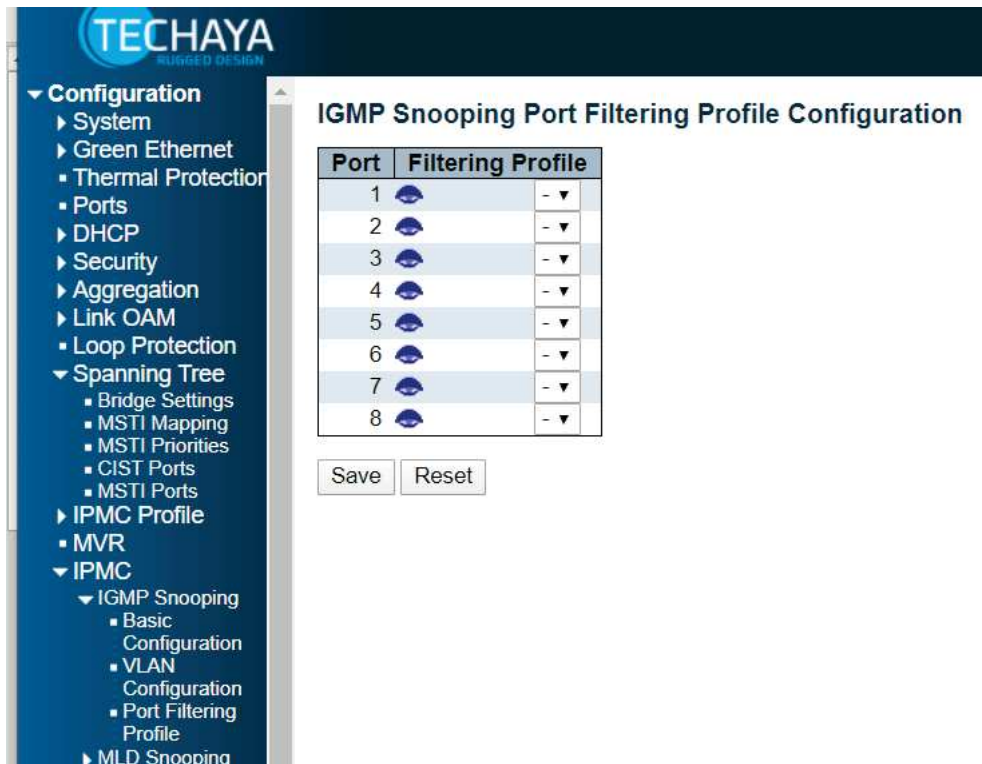
Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.55 IPMC – IGMP Snooping - Port Filtering Profile

4.55.1 Port Filtering Profile Configuration

This page provides Port Filtering Profile related configuration.



Port

The logical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port.

Summary about the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:



: List the rules associated with the designated profile.

4.55.2 Port Filtering Profile Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.56 IPMC – MLD Snooping - Basic Configuration

4.56.1 MLD Snooping Configuration

This page provides MLD Snooping related configuration.

TECHAYA
MULTI-GEAR DESIGN

- Configuration
 - System
 - Green Ethernet
 - Thermal Protection
 - Ports
 - DHCP
 - Security
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - CIST Ports
 - MSTI Ports
 - IPMC Profile
 - MVR
 - IPMC
 - IGMP Snooping
 - MLD Snooping
 - Basic Configuration
 - VLAN Configuration
 - Port Filtering Profile
 - LLDP
 - SyncE
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLANs

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 ▼

Save Reset

Snooping Enabled

Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding Enabled

Enable unregistered IPMCv6 traffic flooding.

The flooding control takes effect only when MLD Snooping is enabled.

When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

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.

Assign valid IPv6 multicast address as prefix with a prefix length (from 8 to 128) for the range.

Leave Proxy Enabled

Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

4.56.2 MLD Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.57 IPMC – MLD Snooping - VLAN Configuration

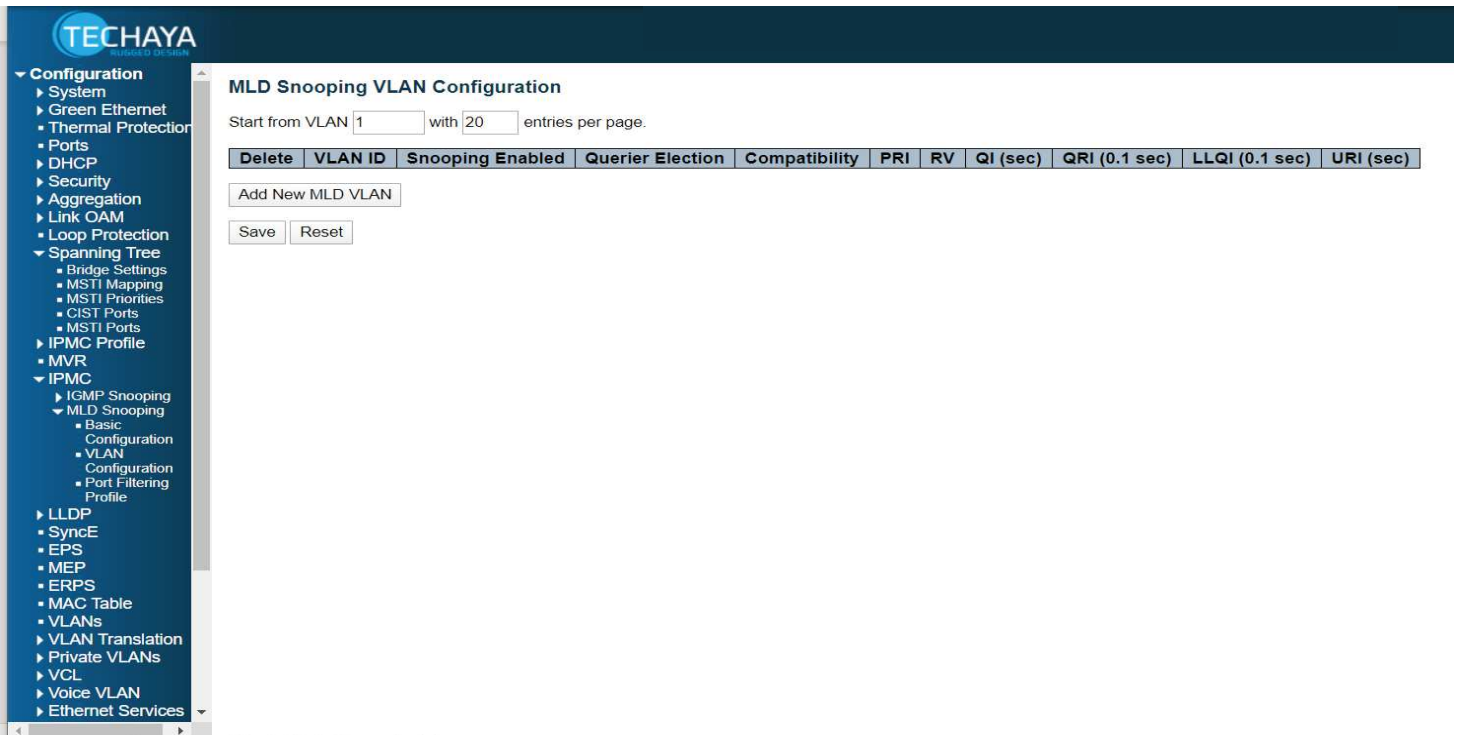
Navigating the MLD Snooping VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The “VLAN” input fields allow the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match.

The **Forward Arrows** () button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the

Back Arrows button () to start over.



TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - CI ST Ports
 - MSTI Ports
- IPMC Profile
- MVR
- IPMC
 - IGMP Snooping
 - MLD Snooping
 - Basic
 - Configuration
 - VLAN
 - Configuration
 - Port Filtering
 - Profile
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services

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)
Add New MLD VLAN										
Save Reset										

4.57.1 MLD Snooping VLAN Configuration

This page allows the user to configure the IGMP Snooping VLAN parameters:

Delete

- ☒ Check to delete a VLAN entry. The entry will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

VLAN ID

Set or show the VLAN ID of the entry.

MLD Snooping Enabled

Set or show the per VLAN MLD Snooping status.

- ☒ Enable the Global MLD Snooping
- ☐ Disable the Global MLD Snooping (This is the default.)

Up to 32 VLANs can be selected for MLD Snooping.

Querier Election

- ☒ Enable this entry to join MLD Querier election in the VLAN (This is the default.)
- ☐ Disable this entry to act as an MLD Non-Querier

Querier election is used to dedicate the Querier. This is the only Querier to which the sends Query messages, on a particular link.

Querier election rule determines that MLD Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

Compatibility

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network.

The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto.

PRI

Priority of Interface.

It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

RV

Robustness Variable.

The Robustness Variable allows tuning for the expected packet loss on a network.

The allowed range is 1 to 255, default robustness variable value is 2.

QI

Query Interval.

The Query Interval is the interval between General Queries sent by the Querier.

The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI

Query Response Interval.

The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.

The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP)

Last Member Query Interval.

The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count.

The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).

The logical port for the settings. Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group.

The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

4.57.2 MLD Snooping VLAN Configuration Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

Back Arrows (): Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

Forward Arrows (): Updates the table, starting with the entry after the last entry currently displayed.

Add a New IGMP VLAN:

Click to add new MLD VLAN. Specify the VID and configure the new entry. After creation of the new entry the user must click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.

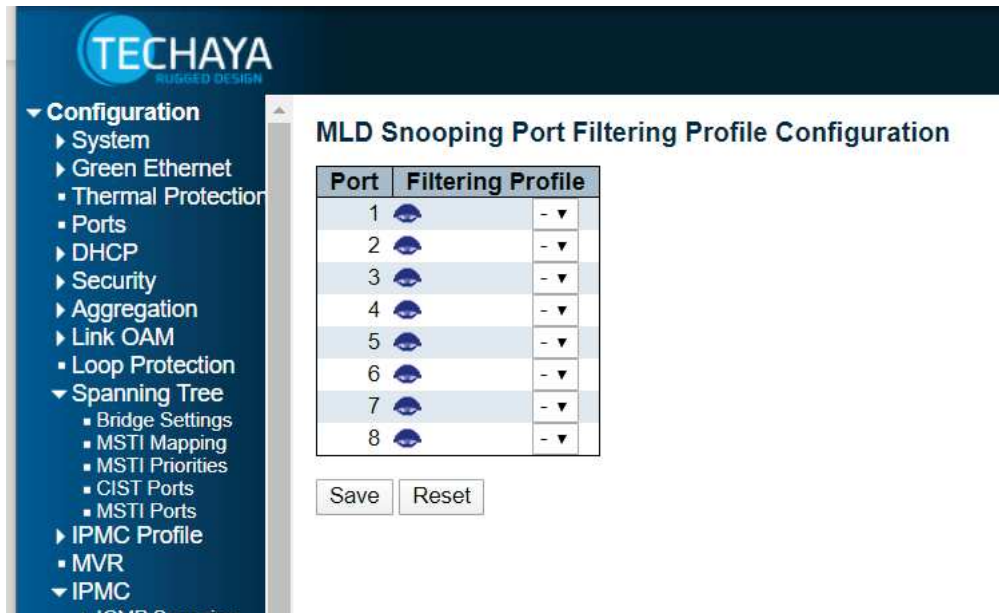
Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.58 IPMC – MLD Snooping - Port Filtering Profile

4.58.1 Port Filtering Profile Configuration

This page provides Port Filtering Profile related configuration.



Port

The logical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port.

Summary about the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:



: List the rules associated with the designated profile.

4.58.2 Port Filtering Profile Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.59 LLDP – LLDP Configuration

The Link Layer Discovery Protocol (LLDP) is an IEEE 802.1ab standard protocol. The LLDP specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN (for a more detailed explanation of this protocol, see the online help).

This page is divided into a global section and a per-port configuration section.

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - CIST Ports
 - MSTI Ports
- IPMC Profile
- MVR
- IPMC
 - IGMP Snooping
 - MLD Snooping
- LLDP
 - LLDP
 - LLDP-MED
 - SymE
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLANs
 - VLAN Translation
 - Private VLANs
 - VCL
 - Voice VLAN
 - Ethernet Services
 - QoS
 - Mirroring
 - UPnP
 - DDP

LLDP Configuration

LLDP Parameters

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	☐	☒	☒	☒	☒	☒

Save Reset

4.59.1 LLDP Parameters

This section allows the user to configure the LLDP Parameters per port:

Tx Interval

Set or show the Tx Interval. Valid values are restricted to 5 - 32768 seconds.

The switch periodically transmits LLDP frames to its neighbors to keep the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value.

Tx Hold

Set or show the Tx Hold value which is used to determine how long the information in the LLDP frame remains valid (the valid period). Values are restricted to 2 - 10 times.

The valid period equals Tx Hold multiplied by Tx Interval seconds. Each LLDP frame stores the valid period to know how long the information in the LLDP frame shall be considered valid.

Tx Delay

Set or show the Tx Delay value. Values are restricted to 1 - 8192 seconds.

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value.

Tx Reinit

Set or show the Tx Reinit value. Values are restricted to 1 - 10 seconds

When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information is not valid anymore. Tx Reinit controls the number of seconds between the shutdown frame and a new LLDP initialization.

4.59.2 LLDP Port Configuration

This section allows the user to configure the LLDP Port Configuration Parameters:

Interface

The switch interface name of the logical LLDP interface.

Mode

Set or show the LLDP mode:

Rx only	The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed
Tx only	The switch will drop LLDP information received from neighbors, but will send out LLDP information
Disabled	The switch will not send out LLDP information, and will drop LLDP information received from neighbors
Enabled	The switch will send out LLDP information, and will analyze LLDP information received from neighbors

CDP Aware

Select CDP awareness.

The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

If all interfaces have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one interface has CDP awareness enabled all CDP frames are terminated by the switch.

Note: When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.

Port Descr

Set or show whether or not the "Port Description" is included in the LLDP information transmitted.

☒ "Port Description" is included (This is the default.)

☐ "Port Description" is **not** included

(This is an optional TLV. For an explanation, see What is an optional TLV below.)

Sys Name

Set or show whether or not the "System Name" is included in the LLDP information transmitted.

☒ "System Name" is included (This is the default.)

☐ "System Name" is **not** included

(This is an optional TLV. For an explanation, see What is an optional TLV below.)

Sys Descr

Set or show whether or not the "System Description" is included in the LLDP information transmitted.

☒ "System Description" is included (This is the default.)

☐ "System Description" is **not** included

(This is an optional TLV. For an explanation, see What is an optional TLV below.)

Sys Capa

Set or show whether or not the "System Capability" is included in the LLDP information transmitted.

☒ "System Capability" is included (This is the default.)

☐ “System Capability” is **not** included

(This is an optional TLV. For an explanation, see What is an optional TLV below.)

Mgmt Addr

Set or show whether or not the “Management Address” is included in the LLDP information transmitted.

☒ “Management Address” is included (This is the default.)

☐ “Management Address” is **not** included

(This is an optional TLV. For an explanation, see What is an optional TLV below.)

What is an optional TLV

TLV is an acronym for Type Length Value. An LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

An LLDP frame contains multiple TLVs.

Optional TLVs are configurable; they can be enabled or disabled. If an optional TLV is disabled the corresponding information is not included in the LLDP frame.

4.59.3 LLDP Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.60 LLDP – LLDP-MED

This page allows you to configure the LLDP-Media. This function applies to VoIP devices which support LLDP-MED.

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
 - Bridge Settings
 - MSTI Mapping
 - MSTI Priorities
 - CIST Ports
 - MSTI Ports
- IPMC Profile
- MVR
- IPMC
 - IGMP Snooping
 - MLD Snooping
- LLDP
 - LLDP
 - LLDP-MED
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring
- UPnP
- PTP

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count: 4

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	☒	☒	☒

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

4.60.1 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 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. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated interface. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an 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 Network Connectivity Devices, or other types of links.

4.60.2 Transmit TLVs

It is possible to 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.

Interface

The interface name to which the configuration applies.

Capabilities

When checked the switch's capabilities is included in LLDP-MED information transmitted.

Policies

When checked the configured policies for the interface is included in LLDP-MED information transmitted.

Location

When checked the configured location information for the switch is included in LLDP-MED information transmitted.

PoE

When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted.

4.60.3 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 -2097151.9 to 2097151.9 with a maximum of 1 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.

4.60.4 Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters.

A couple of notes to the limitation of 250 characters.

- 1) A non empty civic address location will use 2 extra characters in addition to the civic address location text.
- 2) The 2 letter country code is not part of the 250 characters limitation.

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).

Country

County, parish, gun (Japan), district.

City

City, township, shi (Japan) - Example: Copenhagen.

City District

City division, borough, city district, ward, chou (Japan).

Block

Neighborhood, block.

Street

Street - Example: Poppelvej.

Leading street direction

Leading street direction - Example: N.

Trailing street suffix

Trailing street suffix - Example: SW.

Street suffix

Street suffix - Example: Ave, Platz.

House no. suffix

House number suffix - Example: A, 1/2.

Landmark

Landmark or vanity address - Example: Columbia University.

Additional location info

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

Floor - Example: 4.

Room no.

Room number - Example: 450F.

Place type

Place type - Example: Office.

Postal community name

Postal community name - Example: Leonia.

P.O. Box

Post office box (P.O. BOX) - Example: 12345.

Additional code

Additional code - Example: 1320300003.

4.60.5 **Emergency Call Service**

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service

Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

4.60.6 **Policies**

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing

5. Streaming Video

6. Control / Signalling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Delete

- ☒ Check to delete a Policy. The entry will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

Policy ID

ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific interfaces.

Application Type

Intended use of the application types:

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.

5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

Tag

Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID

VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003.

L2 Priority

L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP

DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Adding a new policy

Click **Add New Policy** to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save".

The number of policies supported is 32.

4.60.7 Policies Interface Configuration

Every interface may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or interface configuration.

Interface

The interface name to which the configuration applies.

Policy ID

The set of policies that shall apply to a given interface. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

4.60.8 LLDP-MED Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.61 SyncE

This page allows the user to inspect and configure the current SyncE (Synchronous Ethernet) port settings.

TECHAYA SyncE Configuration

Clock Source Nomination and State

Clock Source	Nominated	Port	Priority	SSM Overwrite	Hold Off	ANEG mode	LOCS	SSM	WTR	Clear WTR
1	☐	1	0	Disabled	Disabled	None	☒	☒	☒	none
2	☐	1	0	Disabled	Disabled	None	☒	☒	☒	none

Clock Selection Mode and State

Mode	Source	WTR Time	SSM Hold Over	SSM Free Run	EEC Option	State	Clock Source	LOL	DHOLD
Auto Revertive	1	5M	Default	Default	None	Free Run		☒	☒

Station Clock Configuration

Clock input frequency: Disabled
Clock output frequency: Disabled

Save Reset

SyncE Ports

Port	SSM Enable	Tx SSM	Rx SSM	1000BaseT Mode
1	☐			Master
2	☐			Master
3	☐			Master
4	☐			Master
5	☐			Master
6	☐			Master
7	☐			Master
8	☐			Master

PTP Ports (8265.1)

Instance	Rx SSM	PTSF
0	QL FAIL	LossAnn

4.61.1 Clock Source Nomination and State

For each possible clock source the following can be configured.

Clock Source

This is the instance number of the clock source. This has to be referenced when selecting 'Manual' Mode.

Nominated

When a clock source is nominated, the clock output from the related PHY (Port) is enabled against the clock controller. This makes it available as a possible source in the clock selection process. If it is supported by the actual HW configuration, The Station clock input can be nominated as a Clock Source.

Port

In this drop down box, the ports that are possible to select for this clock source, is presented. The PCB104 Sync module supports 10MHz station clock input. The station clock input is indicated by a port name = 'S-CLK'. The serval has a limitation that chip port 1 cannot be nominated as source 1. On the Vitesse boards this is port 7 (interface gi 1/7).

Serval2 NID board limitations: Port 5-12 can be configured for 100M, 1G or 2.5G speed. In 2.5G speed mode the SyncE hardware is not able to lock, because the recovered clock output frequency does not match the SyncE hardware's frequency options.

Priority

The priority for this clock source. Lowest number (0) is the highest priority. If two clock sources has the same priority, the lowest clock source number gets the highest priority in the clock selection process.

SSM Overwrite

A selectable clock source Quality Level (QL) to overwrite any QL received in a SSM. If QL is not Received in a SSM (SSM is not enabled on this port), the SSM Overwrite QL is used as if received. The SSM Overwrite can be set to QL_NONE, indicating that the clock source is without any know quality (Lowest compared to clock source with known quality).

Hold Off

The Hold Off timer value. Active loss of clock Source will be delayed the selected amount of time. The clock selector will not change clock source if the loss of clock condition is cleared within this time.

ANEG Mode

This is relevant for 1000BaseT ports only. In order to recover clock from port it must be negotiated to 'Slave' mode. In order to distribute clock the port must be negotiated to 'Master' mode.

This different ANEG modes can be activated on a Clock Source port:

Prefer Slave: The Port will be negotiated to 'Slave' mode if possible.

Prefer Master: The Port will be negotiated to 'Master' mode if possible.

Forced Slave: The Port will be forced to 'Slave' mode.

The selected port in 'Locked' state will always be negotiated to 'Slave' if possible.

LOCS

Signal is lost on this clock source.

SSM

If SSM is enabled and not received properly. Type of SSM fail will be indicated in the 'Rx SSM' field.

WTR

Wait To Restore timer is active.

Clear WTR

Clears the WTR timer and makes this clock source available to the clock selection process.

4.61.2 Clock Selection Mode and State

The Clock Selector is only in one instance - the one who selects between the nominated clock sources.

Mode

The definition of the 'best' clock source is firstly the one with the highest (QL) and secondly (the ones with equal QL) the highest priority.

Clock Selector can be in different modes:

Manual: Clock selector will select the clock source stated in Source (see below). If this manually selected clock source is failing, the clock selector will go into holdover state.

Manual To Selected: Same as Manual mode where the pt. selected clock source will become Source.

Auto NonRevertive: Clock Selection of the best clock source is only done when the selected clock fails.

Auto Revertive: Clock Selection of the best clock source is constantly done.

Force Hold Over: Clock Selector is forced to Hold Over State.

Force Free Run: Clock Selector is forced to Free Run State.

Source

Only relevant if Manual mode is selected (see above).

WTR Time

WTR is the Wait To Restore timer value in minutes. The WTR time is activated on the falling edge of a clock source failure (in Revertive mode). This means that the clock source is first available for clock selection after WTR Time (can be cleared).

SSM Hold Over

This is the transmitted SSM QL value when clock selector is in Hold Over State.

SSM Free Run

This is the transmitted SSM QL value when clock selector is in Free Run State.

EEC Option

The ZL30xxx based Synce modules support both EEC1 and EEC2 option. The difference is: EEC1=> DPLL bandwidth=3,5 Hz, EEC2=> DPLL bandwidth = 0,1 Hz.

State

This is indicating the state of the clock selector. Possible states are:

Free Run: There is no external clock sources to lock to (unlocked state). The Clock Selector has never been locked to a clock source long enough to calculate the hold over frequency offset to local oscillator. The frequency of this node is the frequency of the local oscillator.

Hold Over: There is no external clock sources to lock to (unlocked state). The Clock Selector has calculate the holdover frequency offset to local oscillator. The frequency of this node is hold to the frequency of the clock source previous locked to.

Locked: Clock selector is locked to the clock source indicated (See next).

Top: Clock selector is locked to Time over packets, e.g. PTP (See next).

Clock Source

The clock source locked to when clock selector is in locked state.

LOL

Clock selector has raised the Los Of Lock alarm.

DHOLD

Clock selector has not yet calculated the holdover frequency offset to local oscillator. This becomes active for about 10 s. when a new clock source is selected.

4.61.3 Station Clock Configuration

The Synce module may have a Station clock input and/or a Station clock output.

Clock input frequency

If supported by the Synce HW, the station clock input frequency can be configured, the possible frequencies are:

1,544 MHz, 2,048 MHz or 10 MHz

Clock output frequency

If supported by the Synce HW, the station clock output frequency can be configured, the possible frequencies are:

1,544 MHz, 2,048 MHz or 10 MHz

4.61.4 SyncE Ports

For each possible port on switch.

Port

The port number to configure.

SSM Enable

Enable and disable of SSM functionality on this port.

Tx SSM

Monitoring of the transmitted SSM QL on this port. Transmitted QL should be the Quality Level of the clock generated by this node. This means the QL of the clock source this node is locked to.

Rx SSM

Monitoring of the received SSM QL on this port. If link is down on port, QL_LINK is indicated. If no SSM is received, QL_FAIL is indicated.

1000BaseT Mode

If PHY is in 1000BaseT Mode then this is monitoring the master/slave mode. In order to receive clock on a port, it has to be in slave mode. In order to transmit clock on a port, it has to be in master mode.

4.61.5 SyncE Buttons

Refresh: Click to refresh the page immediately.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.62 EPS

The Ethernet (Linear) Protection Switch instances are configured here.



4.62.1 Ethernet Protection Switching

Mode

This box is used to mark an EPS for deletion in next Save operation.

EPS ID

The ID of the EPS. Click on the ID of an EPS to enter the configuration page. The range is 1-100.

Domain

Port: This will create a EPS in the Port Domain. 'W/P Flow' is a Port.

Architecture

Port: This will create a 1+1 EPS.

Port: This will create a 1:1 EPS.

W Flow

The working flow for the EPS - See 'Domain'.

P Flow

The protecting flow for the EPS - See 'Domain'.

W SF MEP

The working Signal Fail reporting MEP.

P SF MEP

The protecting Signal Fail reporting MEP.

APS MEP

The APS PDU handling MEP.

Alarm

There is an active alarm on the EPS.

4.62.2 EPS Buttons

Add New APS: Click to add a new EPS entry.

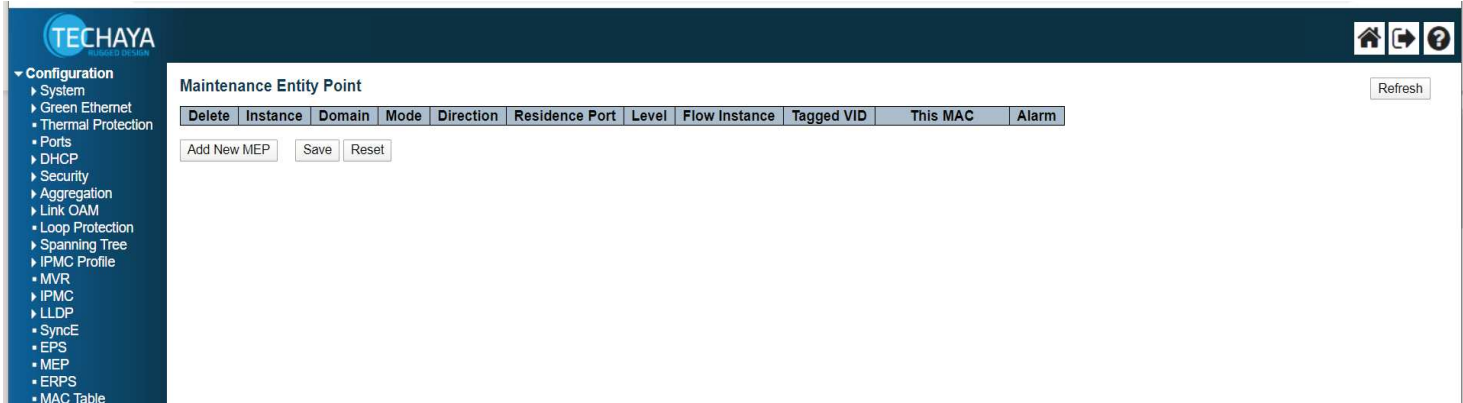
Refresh: Click to refresh the page immediately.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.63 MEP

The Maintenance Entity Point instances are configured here.



4.63.1 Maintenance Entity Point

Delete

- ☒ Check to delete a MEP. The entry will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

Instance

The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from 1 through 100.

Domain

Port: This is a MEP in the Port Domain.

EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created.

Mode

MEP: This is a Maintenance Entity End Point.

MIP: This is a Maintenance Entity Intermediate Point.

Direction

Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port

The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Level

The MEG level of this MEP.

Flow Instance

The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MEP: This is not used.

VLAN MEP: This is not used.

EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.

This MAC

The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Alarm

There is an active alarm on the MEP.

4.63.2 MEP Buttons

Add New MEP: Click to add a new MEP entry.

Refresh: Click to refresh the page immediately.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.64 ERPS

The ERPS instances are configured here.



4.64.1 ERPS Configuration

Delete

- ☒ Check to delete a ERPS. The entry will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

ERPS ID

The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum number of ERPS Protection Groups that can be created are 64. Click on the ID of an Protection group to enter the configuration page.

Port 0

This will create a Port 0 of the switch in the ring.

Port 1

This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance.

Port 0 SF MEP

The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP

The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

Port 0 APS MEP

The Port 0 APS PDU handling MEP.

Port 1 APS MEP

The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type

Type of Protecting ring. It can be either major ring or sub-ring.

Interconnected Node

Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

Virtual Channel

Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

Major Ring ID

Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

Alarm

There is an active alarm on the ERPS.

4.64.2 ERPS Buttons

Add New Protection Group: Click to add a new Protection group entry.

Refresh: Click to refresh the page immediately.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.65 MAC Table – MAC Address Table Configuration

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC Table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

On this page, the user can configure the MAC Address Table, set timeouts for entries in the dynamic MAC Table, and configure the static MAC table here.

TECHAYA
RUGGED DESIGN

- Configuration
 - System
 - Green Ethernet
 - Thermal Protection
 - Ports
 - DHCP
 - Security
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - LLDP
 - SyncE
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLANs
 - VLAN Translation
 - Private VLANs
 - VCL
 - Voice VLAN
 - Ethernet Services
 - QoS
 - Mirroring
 - UPnP
 - PTP
 - GVRP
 - sFlow
 - UDLD
- Monitor
- Diagnostics
- Maintenance

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging ☐

Aging Time seconds

MAC Table Learning

	Port Members							
	1	2	3	4	5	6	7	8
Auto	☒	☒	☒	☒	☒	☒	☒	☒
Disable	☐	☐	☐	☐	☐	☐	☐	☐
Secure	☐	☐	☐	☐	☐	☐	☐	☐

Static MAC Table Configuration

			Port Members							
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8
Add New Static Entry										

Save Reset

4.65.1 Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is called aging.

Disable Automatic Aging

To disable the automatic aging of dynamic entries, check the box:

- ☒ Automatic aging disabled
- ☐ Automatic aging enabled (This is the default.)

Aging Time

To configure aging time, enter a value in the box. The allowed range is 10 to 1,000,000 seconds.

4.65.2 MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:

Port Members

This column displays the switch port number of the logical LLDP port.

Learning Mode

Set or show the Learning mode per switch:

Auto	Learning is done automatically as soon as a frame with unknown SMAC is received
Disable	No learning is done
Secure	Only static MAC entries are learned, all other frames are 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.

4.65.3 Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

Delete

- ☒ Check to delete the entry. The entry will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

VLAN ID

Set or show the VLAN ID of the entry.

MAC Address

Set or show the MAC address of the entry.

Port Members

- ☒ Checkmark indicates the corresponding port is a member of the entry
- ☐ Unchecked box indicates the corresponding port is not a member of the entry
(This is the default.)

4.65.4 MAC Configuration Buttons

Add a New Static Entry Click to add a new entry to the static MAC table.
Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.66 VLANs –VLAN Configuration

This page allows the user to control the VLAN configuration on the switch stack. It is divided into a global section and a per-port configuration section.

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD
- Monitor
- Diagnostics
- Maintenance

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
1	Access	1	C-Port	☒	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☒	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☒	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☒	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☒	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☒	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☒	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☒	Tagged and Untagged	Untag All	1	

Save Reset

4.66.1 Global VLAN Configuration

Allowed Access VLANs

Set or show the allowed Access VLANs. “Allowed Access VLANs” only affect ports configured as Access Ports (for an explanation of Access Ports see the online help). Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be added by using list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will add VLANs 1, 10, 11, 12, 13, 200, and 300 to the list of Allowed Access VLANs:

1, 10-13,200,300. Spaces are allowed in between the delimiters.

Ethertype for Custom S-ports

Set or show the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

4.66.2 Port VLAN Configuration

This section allows the user to configure the VLAN Parameters per port:

Port

This field displays the logical port number of this row.

Mode

Set or show the port mode (default is Access) to determine the fundamental behavior of the port in question. The remaining fields in that row will be either grayed out or made changeable depending on the mode selected.

The grayed out fields show the value that the port will get when the mode is applied to the port.

A port can have one of three modes:

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 a 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 – except 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, but they have 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
 - S-custom-tag aware
- Ingress filtering can be controlled

- Ingress acceptance of frames and configuration of egress tagging can be configured independently

Port VLAN

Set or show the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095 (the default is 1).

On ingress, frames get classified to the Port VLAN if:

- The port is configured as VLAN "Unaware"
- The frame is untagged
- VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0)

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to "Untag Port VLAN".

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

Ports in hybrid mode allow for changing the port type, so that the frame's VLAN tag can be used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. There are four Port Types:

Unaware: On ingress, all frames whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

C-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.

S-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

S-Custom-Port: On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom S-ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

- ☒ Enabled – frames classified to a VLAN of which the port is not a member get discarded (This is the default.)
- ☐ Disabled – frames classified to a VLAN of which the port is not a member are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs of which it is not a member.

Ingress Acceptance

Set or show Ingress Acceptance type.

Tagged and Untagged:	Both tagged and untagged frames are accepted
Tagged Only:	Only tagged frames are accepted on ingress. Untagged frames are discarded.
Untagged Only:	Only untagged frames are accepted on ingress. Tagged frames are discarded.

Hybrid ports allow for changing the type of frames that are accepted on ingress.

Egress Tagging

Set or show Egress Tagging type.

Untag Port VLAN:	Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag
Tag All:	All frames, whether classified to the Port VLAN or not, are transmitted with a tag
Untag All:	All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.

Allowed VLANs

Ports in Trunk and Hybrid mode can control which VLANs they are allowed to join as members. Access ports can be members of only 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.

A list of specific VLANs may be created by using list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will allow the port to become a member of VLANs 1, 10, 11, 12, 13, 200, and 300:

1, 10-13,200,300. Spaces are allowed in between the delimiters.

The field may be left empty, which means that the port will not become member of any VLAN.

Forbidden VLANs

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.

A list of specific VLANs may be created by using list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will forbid the port from becoming a member of VLANs 1, 10, 11, 12, 13, 200, and 300:

1, 10-13,200,300. Spaces are allowed in between the delimiters.

4.66.3 Global VLAN Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.67 Private VLANs – Membership

In a private VLAN, PVLANS provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This 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.

TECHAYA
RUGGED DESIGN

▼ Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- ▼ Private VLANs
 - Membership
 - Port Isolation
- VCL

Private VLAN Membership Configuration

Delete	PVLAN ID	Port Members							
		1	2	3	4	5	6	7	8
☐	1	☒	☒	☒	☒	☒	☒	☒	☒

4.67.1 Private VLAN Membership Configuration

From this page the user can:

- Configure, monitor, and modify Private VLAN membership configurations for the switch
- Add or delete Private VLANs

- Add or remove port members of each Private VLAN

Delete

- ☒ Check to delete a Private VLAN entry. It will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

Private VLAN ID

Set or show ID of this particular private VLAN.

Port Members

A row of check boxes for each port is displayed for each private VLAN ID.

- ☒ Include this port in the Private VLAN (configured in this row)
- ☐ Remove or exclude this port from the Private VLAN (configured in this row)

By default, no ports are members, and all boxes are unchecked.

4.67.2 Private VLAN Membership Configuration Buttons

Auto-refresh:

- ☒ Enable Auto-refresh - refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Add a New Private VLAN Click to add a new Private VLAN ID.

An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.

Click the "Delete" button to undo the addition of a new Private VLAN. The Private VLAN is enabled when you click "Save".

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.68 Private VLANs – Port Isolation

In a private VLAN, PVLANS provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.



4.68.1 Port Isolation Configuration

From this page the user can enable or disable port isolation on ports in a Private VLAN.

A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Port Number

A check box is provided for each port of a private VLAN.

☒ Port Isolation is enabled on that port

☐ Port Isolation is disabled on that port

By default, port isolation is disabled on all ports.

4.68.2 Port Isolation Configuration Buttons

Auto-refresh:

- ☒ Enable Auto-refresh - refresh the page automatically every 3 seconds
☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.69 VCL – Mac-Based VLAN

The MAC address to VLAN ID mappings can be configured here. This page allows adding and deleting MAC-based VLAN Classification List entries and assigning the entries to different ports.

The screenshot shows the 'MAC-based VLAN Membership Configuration' page. On the left is a sidebar with a 'Configuration' menu containing links to System, Green Ethernet, Thermal Protection, Ports, DHCP, Security, Aggregation, Link OAM, Loop Protection, Spanning Tree, and IPMC Profile. The main content area has a title 'MAC-based VLAN Membership Configuration' and an 'Auto-refresh' checkbox. Below the title is a table with columns 'Delete', 'MAC Address', 'VLAN ID', and 'Port Members'. The 'Port Members' column has sub-columns for ports 1 through 8. The table currently shows 'Currently no entries present'. Below the table are buttons for 'Add New Entry', 'Save', and 'Reset'.

4.69.1 VCL Mac-Based VLAN Configuration

Delete

☒ Check to delete a MAC to VLAN ID mapping entry. It will be deleted during the next save.

☐ Do not delete the entry. (This is the default.)

Mac Address

Indicates the MAC address of the mapping.

VLAN ID

Indicates the VLAN ID the above MAC will be mapped to.

Port Members

A row of check boxes for each port is displayed for each MAC to VLAN ID mapping entry. To include a port in the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

4.69.2 VCL Mac-Based VLAN Configuration Buttons

Auto-refresh:

☒ Enable Auto-refresh - refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Add a New Private VLAN Click to add a new MAC to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any unicast MAC address can be used to configure the mapping. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.

The MAC to VLAN ID entry is enabled when you click on "Save". A mapping without any port members will not be added when you click "Save". The "Delete" button can be used to undo the addition of new mappings. The maximum possible MAC to VLAN ID mapping entries are limited to 256.

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.70 VCL – Protocol-Based VLAN – Protocol to Group Mapping

This page allows you to add new Protocol to Group Name (each protocol can be part of only one Group) mapping entries as well as allow you to see and delete already mapped entries for the switch.

TECHAYA
RUGGED DESIGN

- ▼ Configuration
 - ▶ System
 - ▶ Green Ethernet
 - Thermal Protection
 - Ports
 - ▶ DHCP
 - ▶ Security
 - ▶ Aggregation
 - ▶ Link OAM
 - Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - MVR
 - ▶ IPMC

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
No Group entry found!			

Add New Entry

Save Reset

4.70.1 Protocol to Group Mapping Configuration

Delete

- ☒ Check to delete a Protocol to Group Name map entry. It will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

Frame Type

Frame Type can have one of the following values:

- 1.Ethernet
- 2.LLC
- 3.SNAP

Note: When changing the Frame type field, the valid value of the following text field will vary depending on the new frame type you selected.

Value

Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.

Below are the criteria for the three different Frame Types:

1. Ethernet: Value in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range between 0x0600 and 0xffff
2. LLC: Valid value in this case is comprised of two different sub-values.

- a. DSAP: 1-byte long string (0x00-0xff)
 - b. SSAP: 1-byte long string (0x00-0xff)
 - 3. SNAP: Valid value in this case is also comprised of two different sub-values.
 - a. OUI: OUI (Organizationally Unique Identifier) is a parameter in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value ranging between 0x00 and 0xff.
 - b. PID: PID (Protocol ID). If OUI is hexadecimal 000000, then the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if OUI is an OUI for 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 the value of OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff) and if the value of OUI is other than 00-00-00 then valid values of PID will be any value between 0x0000 and 0xffff.

Group Name

A valid Group Name is a 16-character long string, unique for every entry, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).

Note: Special characters and underscores (_) are not allowed.

4.70.2 VCL Group Mapping Configuration Buttons

Auto-refresh:

- ☒ Enable Auto-refresh - refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.).

Refresh: Click to refresh the page immediately.

Add a New Group Mapping: Click to add a new entry in the mapping table. An empty row is added to the table, where Frame Type, Value and the Group Name can be configured as needed.

The "Delete" button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.71 VCL – Protocol-Based VLAN – Group to VLAN

This page allows you to map a Group Name (already configured or to be configured in the future) to a VLAN for the switch.

TECHAYA
REDUCED DESIGN

- Configuration
 - System
 - Green Ethernet
 - Thermal Protection
 - Ports
 - DHCP
 - Security
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC

Group Name to VLAN mapping Table

Delete	Group Name	VLAN ID	Port Members							
			1	2	3	4	5	6	7	8
Currently no entries present in the switch										

4.71.1 Group Name to VLAN Mapping Configuration

Delete

- ☒ Check to delete a Group Name to VLAN mapping entry. It will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

Group Name

A valid Group Name is a string, at the most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings), or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g. Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2).

VLAN ID

Indicates the VLAN ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1 to 4095.

Port Members

A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in the mapping, check the box. To remove or exclude

the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

4.71.2 Group Name to VLAN Mapping Buttons

Auto-refresh:

- ☒ Enable Auto-refresh - refresh the page automatically every 3 seconds
☐ Disable Auto-refresh (This is the default.).

Refresh: Click to refresh the page immediately.

Add a New Group to VLAN Mapping: Click to add a new entry in the mapping table. An empty row is added to the table and the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

The "Delete" button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 128.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.72 VCL – IP Subnet-based VLAN Membership

The IP subnet to VLAN ID mappings can be configured here. This page allows adding, updating and deleting IP subnet to VLAN ID mapping entries and assigning them to different ports.

TECHAYA
Network Design

- ▼ Configuration
 - ▶ System
 - ▶ Green Ethernet
 - ▶ Thermal Protection
 - ▶ Ports
 - ▶ DHCP
 - ▶ Security
 - ▶ Aggregation
 - ▶ Link OAM
 - ▶ Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - ▶ MVR
 - ▶ IPMC
 - ▶ LLDP
 - ▶ SyncE
 - ▶ EPS
 - ▶ MEP
 - ▶ ERPS

IP Subnet-based VLAN Membership Configuration

Delete	IP Address	Mask Length	VLAN ID	Port Members							
				1	2	3	4	5	6	7	8
Currently no entries present											

4.72.1 IP Subnet-based VLAN Membership Configuration

Delete

- ☒ Check to delete a mapping entry. It will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

IP Address

Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically).

Mask Length

Indicates the subnet's mask length.

VLAN ID

Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching.

Port Members

A row of check boxes for each port is displayed for each IP subnet to VLAN ID mapping entry. To include a port in a mapping, simply check the box. To remove

or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

4.72.2 VCL IP Subnet-Based VLAN Configuration Buttons

Auto-refresh:

- ☒ Enable Auto-refresh - refresh the page automatically every 3 seconds
☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Add a New IP subnet-based VLAN: Click to add a new IP subnet to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any IP address/mask can be configured for the mapping. Legal values for the VLAN ID are 1 to 4095.

The IP subnet to VLAN ID mapping entry is enabled when you click on "Save". The "Delete" button can be used to undo the addition of new mappings. The maximum possible IP subnet to VLAN ID mappings are limited to 128.

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.73 Voice VLAN - Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

The screenshot shows the Techaya Web Interface. On the left is a navigation menu with categories like Configuration, System, Green Ethernet, Thermal Protection, Ports, DHCP, Security, Aggregation, Link OAM, Loop Protection, Spanning Tree, IPMC Profile, MVR, IPMC, LLDP, SyncE, EPS, MEP, ERPS, MAC Table, VLANs, VLAN Translation, Private VLANs, VCL, Voice VLAN, Ethernet Services, QoS, Mirroring, UPnP, PTP, GVRP, sFlow, UDLD, and Monitor. The main content area is titled 'Voice VLAN Configuration' and contains the following fields:

- Mode:** Disabled (dropdown)
- VLAN ID:** 1000 (text input)
- Aging Time:** 86400 (text input) seconds
- Traffic Class:** 7 (High) (dropdown)

Below these fields is the 'Port Configuration' section, which is a table with 4 columns: Port, Mode, Security, and Discovery Protocol. The table has 8 rows, numbered 1 to 8. Each row has dropdown menus for Mode, Security, and Discovery Protocol. The Discovery Protocol dropdowns are all set to 'OUI'. At the bottom of the Port Configuration section are 'Save' and 'Reset' buttons.

Port	Mode	Security	Discovery Protocol
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

4.73.1 Voice VLAN Configuration

Mode

Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

Enabled: Enable Voice VLAN mode operation.

Disabled: Disable Voice VLAN mode operation.

VLAN ID

Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.

Aging Time

Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

Traffic Class

Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Port Mode

Indicates the Voice VLAN port mode. Possible port modes are:

Disabled: Disjoin from Voice VLAN.

Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.

Forced: Force join to Voice VLAN.

Port Security

Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

Port Discovery Protocol

Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

OUI: Detect telephony device by OUI address.

LLDP: Detect telephony device by LLDP.

Both: Both OUI and LLDP.

4.73.2 Voice VLAN Configuration Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.74 Voice VLAN - OUI

TECHAYA
SUGGESTED DESIGN

▼ Configuration

- ▶ System
- ▶ Green Ethernet
- Thermal Protection
- Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
- ▶ Link OAM
- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table

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

Add New Entry

Save Reset

4.74.1 Voice VLAN OUI Configuration

Configure VOICE VLAN OUI table on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of OUI process.

Delete

- ☒ Check to delete entry. It will be deleted during the next save.
- ☐ Do not delete the entry. (This is the default.)

Telephony OUI

A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

Description

The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

4.74.2 Voice VLAN OUI Buttons

Add New Entry: Click to add a new access management entry.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.75 Ethernet Services - Ports

This page displays current EVC port configurations. The settings can also be configured here.

TECHAYA
RUGGED DESIGN

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS

Port Configuration

Port	DEI Mode	Tag Mode	Address Mode
*	<>	<>	<>
1	Fixed	Outer	Source
2	Fixed	Outer	Source
3	Fixed	Outer	Source
4	Fixed	Outer	Source
5	Fixed	Outer	Source
6	Fixed	Outer	Source
7	Fixed	Outer	Source
8	Fixed	Outer	Source

Save Reset

4.75.1 EVC Port Configuration

Port

The logical port for the settings contained in the same row.

DEI Mode

The DEI mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the colour of the frame. The allowed values are:

Coloured: The DEI is 1 for yellow frames and 0 for green frames.

Fixed: The DEI value is determined by ECE rules.

Tag Mode

The tag mode specifying whether the EVC classification must be based on the outer or inner tag. This can be used on NNI ports connected to another service provider, where an outer "tunnel" tag is added together with the inner tag identifying the EVC. The allowed values are:

Inner: Enable inner tag in EVC classification.

Outer: Enable outer tag in EVC classification.

Address Mode

The IP/MAC address mode specifying whether the EVC classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses. The allowed values are:

Source: Enable SMAC/SIP matching.

Destination: Enable DMAC/DIP matching.

4.75.2 EVC Port Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.76 Ethernet Services – L2CP

This page displays current EVC L2CP configurations. The settings can also be configured here.



- ▼ Configuration
 - ▶ System
 - ▶ Green Ethernet
 - Thermal Protection
 - Ports
 - ▶ DHCP
 - ▶ Security
 - ▶ Aggregation
 - ▶ Link OAM
 - Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - MVR
 - ▶ IPMC
 - ▶ LLDP
 - SyncE
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLANs
 - ▶ VLAN Translation
 - ▶ Private VLANs
 - ▶ VCL
 - ▶ Voice VLAN
 - ▼ Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs
 - ECEs
 - ▶ QoS
 - Mirroring
 - UPnP
 - PTP
 - ▶ GVRP
 - sFlow
 - UDLD
 - ▶ Monitor
 - ▶ Diagnostics
 - ▶ Maintenance

L2CP Port Configuration

DMAC	L2CP Mode
*	
01-80-C2-00-00-00	Peer ▼
01-80-C2-00-00-01	Peer ▼
01-80-C2-00-00-02	Peer ▼
01-80-C2-00-00-03	Peer ▼
01-80-C2-00-00-04	Peer ▼
01-80-C2-00-00-05	Peer ▼
01-80-C2-00-00-06	Peer ▼
01-80-C2-00-00-07	Peer ▼
01-80-C2-00-00-08	Peer ▼
01-80-C2-00-00-09	Peer ▼
01-80-C2-00-00-0A	Peer ▼
01-80-C2-00-00-0B	Peer ▼
01-80-C2-00-00-0C	Peer ▼
01-80-C2-00-00-0D	Peer ▼
01-80-C2-00-00-0E	Peer ▼
01-80-C2-00-00-0F	Peer ▼
01-80-C2-00-00-20	Forward ▼
01-80-C2-00-00-21	Forward ▼
01-80-C2-00-00-22	Forward ▼
01-80-C2-00-00-23	Forward ▼
01-80-C2-00-00-24	Forward ▼
01-80-C2-00-00-25	Forward ▼
01-80-C2-00-00-26	Forward ▼
01-80-C2-00-00-27	Forward ▼
01-80-C2-00-00-28	Forward ▼
01-80-C2-00-00-29	Forward ▼
01-80-C2-00-00-2A	Forward ▼
01-80-C2-00-00-2B	Forward ▼
01-80-C2-00-00-2C	Forward ▼
01-80-C2-00-00-2D	Forward ▼

4.76.1 L2CP Configuration

DMAC

The destination BPDU MAC addresses (01-80-C2-00-00-0X) and GARP (01-80-C2-00-00-2X) MAC addresses for the settings contained in the same row.

L2CP Mode

The L2CP mode for the specific port. The possible values are:

Peer: Allow to peer L2CP frames.

Forward: Allow to forward L2CP frames.

4.76.2 L2CP Buttons

The port select box determines which port is affected by clicking the buttons.

Refresh: Click to refresh the page.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.77 Ethernet Services – Bandwidth Profiles

This page displays current EVC ingress bandwidth profile configurations. These policers may be used to limit the traffic received on UNI ports. The settings can also be configured here.

TECHAYA
Control System

▼ Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs
 - ECs
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD
- Monitor
- Diagnostics
- Maintenance

Bandwidth Profiles Configuration

Start from Policer ID with entries per page.

Policer ID	State	Type	Policer Mode	Rate Type	CIR (kbps)	CBS (bytes)	EIR (kbps)	EBS (bytes)
*	<>	<>	<>	<>	0	0	0	0
1	Disabled	MEF	Aware	Data	0	0	0	0
2	Disabled	MEF	Aware	Data	0	0	0	0
3	Disabled	MEF	Aware	Data	0	0	0	0
4	Disabled	MEF	Aware	Data	0	0	0	0
5	Disabled	MEF	Aware	Data	0	0	0	0
6	Disabled	MEF	Aware	Data	0	0	0	0
7	Disabled	MEF	Aware	Data	0	0	0	0
8	Disabled	MEF	Aware	Data	0	0	0	0
9	Disabled	MEF	Aware	Data	0	0	0	0
10	Disabled	MEF	Aware	Data	0	0	0	0
11	Disabled	MEF	Aware	Data	0	0	0	0
12	Disabled	MEF	Aware	Data	0	0	0	0
13	Disabled	MEF	Aware	Data	0	0	0	0
14	Disabled	MEF	Aware	Data	0	0	0	0
15	Disabled	MEF	Aware	Data	0	0	0	0
16	Disabled	MEF	Aware	Data	0	0	0	0
17	Disabled	MEF	Aware	Data	0	0	0	0
18	Disabled	MEF	Aware	Data	0	0	0	0
19	Disabled	MEF	Aware	Data	0	0	0	0
20	Disabled	MEF	Aware	Data	0	0	0	0

Save Reset

4.77.1 Bandwidth Profiles Configuration

Start Policer ID

The start Policer ID for displaying the table entries. The allowed range is from 1 through 256.

Number of Entries

The number of entries per page. The allowed range is from 2 through 256.

Policer ID

The Policer ID is used to identify one of the 256 policers.

State

The administrative state of the bandwidth profile. The allowed values are:

Enabled: The bandwidth profile enabled.

Disabled: The bandwidth profile is disabled.

Type

The policer type of the bandwidth profile. The allowed values are:

MEF: MEF ingress bandwidth profile.

Single: Single bucket policer.

Policer Mode

The colour mode of the bandwidth profile. The allowed values are:

Coupled: Colour-aware mode with coupling enabled.

Aware: Colour-aware mode with coupling disabled.

Rate Type

The rate type of the bandwidth profile. The allowed values are:

Data: Specify that this bandwidth profile operates on data rate.

Line: Specify that this bandwidth profile operates on line rate.

CIR

The Committed Information Rate of the bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

CBS

The Committed Burst Size of the bandwidth profile. The allowed range is from 0 through 100000 bytes.

EIR

The Excess Information Rate for MEF type bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

EBS

The Excess Burst Size for MEF type bandwidth profile. The allowed range is from 0 through 100000 bytes.

4.77.2 Bandwidth Profile Buttons

The port select box determines which port is affected by clicking the buttons.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table, starting with the first entry in the table.

<<: Updates the table, ending at the entry before the first entry currently displayed.

>>: Updates the table, starting with the entry after the last entry currently displayed.

>>|: Updates the table, ending at the last entry in the table.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.78 Ethernet Services – EVC Control List

This page displays current EVC configurations. On this system, only Provider Bridge based EVCs are supported.

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLD
- Sync

EVC Control List Configuration

Auto-refresh ☐ Refresh Remove All

EVC ID	Name	VID	IVID	Learning	Inner Tag					Outer Tag		NNI Ports
					Type	VID Mode	VID	PCP/DEI Preservation	PCP	DEI	VID	

4.78.1 EVC Control List Configuration

EVC ID

The EVC ID identifies the EVC. The range is from 1 through 256.

Name

The name for the EVC.

VID

The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The range is from 1 through 4095.

IVID

The Internal/classified VLAN ID in the PB network. The range is from 1 through 4095.

Learning

The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. The possible values are:

Enabled: Learning is enabled (MAC addresses are learned).

Disabled: Learning is disabled (MAC addresses are not learned).

Inner Tag Type

The inner tag type is used to determine whether an inner tag is inserted in frames forwarded to NNI ports. The possible values are:

None: An inner tag is not inserted.

C-tag: An inner C-tag is inserted.

S-tag: An inner S-tag is inserted.

S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

Inner VID Mode

The inner VID Mode affects the VID in the inner and outer tag. The possible values are:

Normal: The VID of the two outer tags aren't swapped.

Tunnel: The VID of the two outer tags are swapped, so that the VID of the outer tag is taken from the Inner Tag configuration and the VID of the inner tag is the EVC VID. In this mode, the NNI ports are normally configured to do EVC classification based on the inner tag.

Inner Tag VID

The Inner tag VLAN ID. The allowed range is from 0 through 4095.

Inner Tag PCP/DEI Preservation

The inner tag PCP and DEI preservation. The possible values are:

Preserved: The inner tag PCP and DEI is preserved.

Fixed: The inner tag PCP and DEI is fixed.

Inner Tag PCP

The inner tag PCP value. The allowed range is from 0 through 7.

Inner Tag DEI

The inner tag DEI value. The allowed value is 0 or 1.

Outer Tag VID

The EVC outer tag VID for UNI ports. The allowed range is from 0 through 4095.

NNI Ports

The list of Network to Network Interfaces for the EVC.

4.78.2 Modification Buttons

You can modify each EVC in the table using the following buttons:

: Edits the EVC row.

: Deletes the EVC.

: Adds new EVC.

4.78.3 Buttons

Auto-Refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

Remove All: Click to remove all EVCs.

4.79 Ethernet Services – EVC Control Entries

This page displays the current EVC Control Entries (ECEs). The settings can also be configured here.

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE

EVC Control List Configuration

Auto-refresh ☐ Refresh Remove All

EVC ID	Name	VID	IVID	Learning	Inner Tag				Outer Tag		NNI Ports
					Type	VID Mode	VID	PCP/DEI Preservation	PCP	DEI	
+											

TECHAYA

Configuration

- System
- Green Ethernet
- Thermal Protection
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs
 - ECES
- QoS
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD
- Monitor
- Diagnostics
- Maintenance

ECE Configuration

UNI Ports

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☐	☐	☐	☐

Ingress Matching

Tag Type	Any
Frame Type	Any

Actions

Direction	Both
EVC ID Filter	Specific
EVC ID Value	1
Tag Pop Count	0
Policy ID	0
Class	Disabled

MAC Parameters

SMAC Filter	Any
DMAC Type	Any

Egress Outer Tag

Mode	Disabled
PCP/DEI Preservation	Fixed
PCP	0
DEI	0

Save Reset Cancel

ECE ID

The ECE ID identifies the ECE. Unique ECE IDs are automatically assigned to ECEs added. The possible range is from 1 through 256.

4.79.1 Ingress Matching

UNI Ports

The list of User Network Interfaces for the ECE.

Tag Type

The tag type for the ECE. The possible values are:

Any: The ECE will match both tagged and untagged frames.

Untagged: The ECE will match untagged frames only.

C-Tagged: The ECE will match custom tagged frames only.

S-Tagged: The ECE will match service tagged frames only.

Tagged: The ECE will match tagged frames only.

VID

The VLAN ID for the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:

Specific: The range is from 0 through 4095.

Any: The ECE will match any VLAN ID.

PCP

The PCP value for the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:

Specific: The ECE will match a specific PCP in the range 0 through 7.

Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

Any: The ECE will match any PCP value.

DEI

The DEI value for the ECE. It only significant if tag type 'Tagged' is selected. The possible values is: 0, 1 or Any.

Frame Type

The frame type for the ECE. The possible values are:

Any: The ECE will match any frame type.

IPv4: The ECE will match IPv4 frames only.

IPv6: The ECE will match IPv6 frames only.

4.79.2 Actions

Direction

The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. Possible values are:

Both: Bidirectional.

UNI-to-NNI: Unidirectional from UNI to NNI.

NNI-to-UNI: Unidirectional from NNI to UNI.

EVC ID

The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:

Specific: The range is from 1 through 256.

None: The ECE does not map to an EVC.

Tag Pop Count

The ingress tag pop count for the ECE. The possible range is from 0 through 2.

Policy ID

The ACL Policy ID for the ECE. The range is from 0 through 255.

Class

The traffic class for the ECE. The range is from 0 through 7.

4.79.3 Egress Outer Tag

Outer Tag Mode

The outer tag for nni-to-uni direction for the ECE. The possible values are:

Enable: Enable outer tag for nni-to-uni direction for the ECE.

Disable: Disable outer tag for nni-to-uni direction for the ECE.

Outer Tag PCP/DEI Preservation

The outer tag PCP and DEI preservation for the ECE. The possible values are:

Preserved: The outer tag PCP and DEI are preserved.

Disable: The outer tag PCP and DEI are fixed.

Outer Tag PCP

The outer tag PCP value for the ECE. The possible range is from 0 through 7.

Outer Tag DEI

The outer tag DEI value for the ECE. The possible value is 0 or 1.

Conflict

Indicates the hardware status of the specific ECE. The specific ECE is not applied to the hardware due to hardware limitations.

4.79.4 Modification Buttons

You can modify each ECE (EVC Control Entry) in the table using the following buttons:

: Inserts a new ECE before the current row.

- : Edits the ECE row.
- : Moves the ECE up the list.
- : Moves the ECE down the list.
- : Deletes the ECE.
- : The lowest plus sign adds a new entry at the bottom of the ECE listings.

4.79.5 Buttons

Auto-Refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

Remove All: Click to remove all ECEs.

4.80 QoS – Port Classification

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

TECHAYA
MULTI-DESIGN

- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs
 - ECEs
- QoS
 - Port Classification
 - Port Policing
 - Queue Policing
 - Port Scheduler
 - Port Shaping
 - Port Tag Remark
 - Port DSCP
 - DSCP-Based QoS
 - DSCP Translation
 - DSCP Classification
 - QoS Control List
 - Storm Policing
- Mirroring
- UPnP

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<> ▼	<> ▼	<> ▼	<> ▼		☐	<> ▼
1	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
2	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
3	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
4	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
5	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
6	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
7	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼
8	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐	Source ▼

Save Reset

4.80.1 QoS Ingress Port Classification

This page allows the user to configure the basic QoS Ingress Classification settings for all switch ports.

The displayed settings are:

Port

This field displays the port number for this row. All configurations on this row apply to this port.

CoS

Set or show the class of service.

All frames are classified to a CoS. There is a one to one mapping between CoS, queue, and priority. A CoS of 0 (zero) has the lowest priority.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.

The classified CoS can be overruled by a QCL (QoS Control List) entry.

Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

DPL

Controls the default drop precedence level.

All frames are classified to a drop precedence level.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

PCP

Set or show the default PCP value.

All frames are classified to a PCP value.

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority. A PCP of 0 (zero) has the lowest priority.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

DEI

Set or show the default DEI value.

All frames are classified to a DEI value.

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag:

1: drop eligible

0: not drop eligible (default)

If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

Tag Class.

Shows the classification mode for tagged frames on this port.

Disabled: Use default CoS and DPL for tagged frames.

Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the mode in order to configure the mode and/or mapping.

Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

DSCP Based

Click to Enable DSCP Based QoS Ingress Port Classification.

Address Mode

The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are:

Source: Enable SMAC/SIP matching.

Destination: Enable DMAC/DIP matching.

4.80.2 QoS Ingress Port Classification Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.81 QoS – Port Policing

A Policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

This page allows the user to configure the Policer settings for all switch ports.

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	☐

Save Reset

4.81.1 QoS Ingress Port Policers

The displayed settings are:

Port

This field displays the port number for this row. All configurations on this row apply to this port.

Enabled

Enable or disable the policer on this switch port.

- ☒ Enabled – the policer is enabled on this switch port
- ☐ Disabled – the policer is disabled on this switch port (This is the default.)

Rate

Set or show the rate for the policer. The default value is 500.

This value is restricted to:	when the "Unit" is:
100- 3276700	"kbps" or "fps"
1-3276	"Mbps" or "kfps"

Unit

Set or show the unit of measure for the policer rate as kbps, Mbps, fps, or kfps. The default value is "kbps".

Flow Control

Enable or disable the flow control.

- ☒ Enabled – flow control is enabled on this switch port
- ☐ Disabled – flow control is disabled on this switch port (This is the default.)

If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

4.81.2 QoS Ingress Port Policers Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.82 QoS – Queue Policing

TECHAYA
SUGGESTED DESIGN

- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs
 - ECEs
- QoS
 - Port Classification
 - Port Policing
 - Queue Policing
 - Port Scheduler
 - Port Shaping
 - Port Tag Remark
 - Port DSCP
 - DSCP-Based QoS
 - DSCP Translation
 - DSCP Classification
 - QoS Control List
 - Storm 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	☐	☐	☐	☐	☐	☐	☐	☐

Save Reset

4.82.1 Queue Port Policers

This page allows you to configure the Queue Policer settings for all switch ports.

The displayed settings are:

Port

This field displays the port number for this row. All configurations on this row apply to this port.

Enabled

Enable or disable the queue policer on this switch port.

- ☒ Enabled – the queue policer is enabled on this switch port
- ☐ Disabled – the queue policer is disabled on this switch port (This is the default.)

Rate

Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer.

This field is only shown if at least one of the queue policers are enabled.

Unit

Controls the unit of measure for the queue policer rate as kbps or Mbps.

This field is only shown if at least one of the queue policers are enabled.

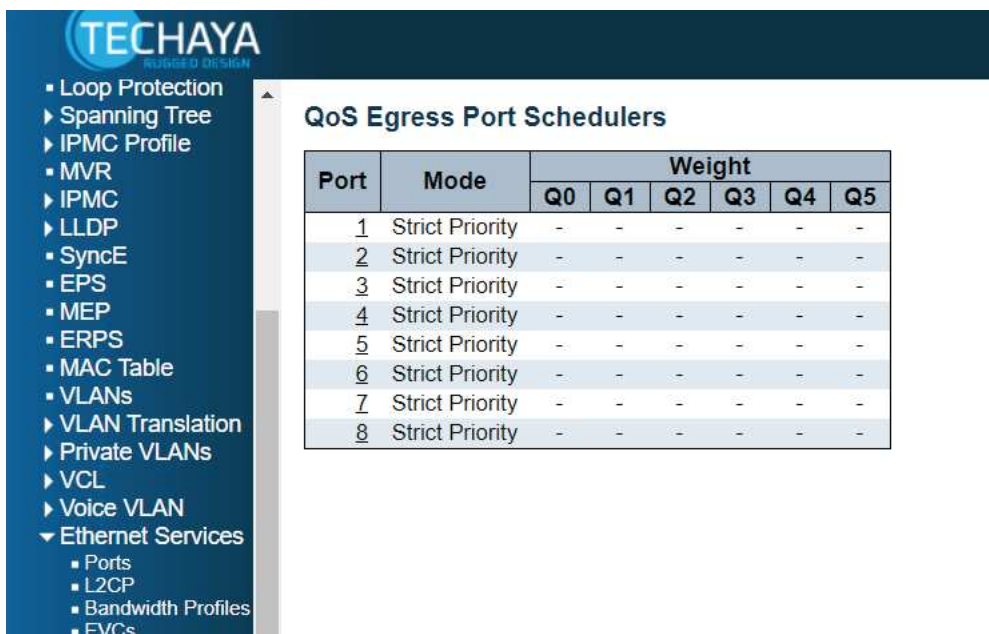
4.82.2 QoS Queue Policers Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.83 QoS – Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports.



QoS Egress Port Schedulers							
Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

The displayed settings are:

Port

The logical port for the settings contained in the same row.

Click on the port number in order to configure the schedulers.

Mode

This column shows the scheduling mode for this port.

Qn

This column shows the weight for this queue and port.

4.83.1 QoS Egress Port Schedulers and Shapers Page

This page allows the user to configure the Scheduler and Shapers for a specific port. It is opened from the **מקור ההפניה לא נמצא** page and also from QoS – Port Shaping page. The port number is displayed at top of the page.

TECHAYA
RUGGED DESIGN

- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs
 - ECEs
- QoS
 - Port Classification
 - Port Policing
 - Queue Policing
 - Port Scheduler
 - Port Shaping
 - Port Tag Remark
 - Port DSCP
 - DSCP-Based QoS
 - DSCP Translation
 - DSCP Classification
 - QoS Control List
 - Storm Policing
- Mirroring
- UPnP
- PTP
- GVRP
- sFlow
- UDLD
- Monitor
- Diagnostics
- Maintenance

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

Queue Shaper			
Enable	Rate	Unit	Excess
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐

Port Shaper

Enable	Rate	Unit
☐	500	kbps

STRICT

Save Reset Back

Port

The box at the top right of the page shows the logical port for the settings contained in this page. Click the down arrow to select a different port to configure.

Scheduler Mode

Set or show whether the scheduler mode is “Strict Priority” or “Weighted” on this switch port.

Queue Shaper Enable

Set or show whether the queue shaper is enabled for this queue on this switch port.

- ☒ Enabled – the queue shaper is enabled for this queue on this switch port
- ☐ Disabled – the queue shaper is disabled for this queue on this switch port
(This queue shaper is disabled by default.)

Queue Shaper Rate

Set or show the rate for the queue shaper. The default value is 500.

This value is restricted to:	when the "Unit" is:
100- 3281943	"kbps"
1-3281	"Mbps"

Queue Shaper Unit

Set or show the unit of measure for the queue shaper rate as "kbps" or "Mbps".
The default value is "kbps".

Queue Shaper Excess

Set or show whether the queue is allowed to use excess bandwidth.

- ☒ Enabled – the queue is allowed to use excess bandwidth
- ☐ Disabled – the queue is **not** allowed to use excess bandwidth (The queue is not allowed to use excess bandwidth by default.)

Queue Scheduler Weight

Set or show the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent

Show the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable

Set or show whether the port shaper is enabled for this switch port.

- ☒ Enabled – the port shaper is enabled for this switch port
- ☐ Disabled – the port shaper is disabled for this switch port (The port shaper is disabled for this switch port by default.)

Port Shaper Rate

Set or show the rate for the port shaper. The default value is 500.

This value is restricted to:	when the "Unit" is:
100- 3281943	"kbps"
1-3281	"Mbps"

Port Shaper Unit

Set or show the unit of measure for the port shaper rate as “kbps” or “Mbps”. The default value is “kbps”.

4.83.2 QoS Egress Port Schedulers Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

Back: Click to undo any changes made locally and return to the previous page

4.84 QoS – Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

TECHAYA
Rugged Design

- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- ▶ VLAN Translation
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▼ Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs
 - ECEs
- ▼ QoS
 - Port Classification
 - Port Policing

QoS Egress Port Shapers

Port	Shapers								Port
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-

4.84.1 QoS Egress Port Shapers

The displayed settings are:

Port

Displays the logical port for the settings contained in the same row.

Click on the port number in order to configure the shapers. The QoS Egress Port Schedulers and Shapers page opens.

Qn

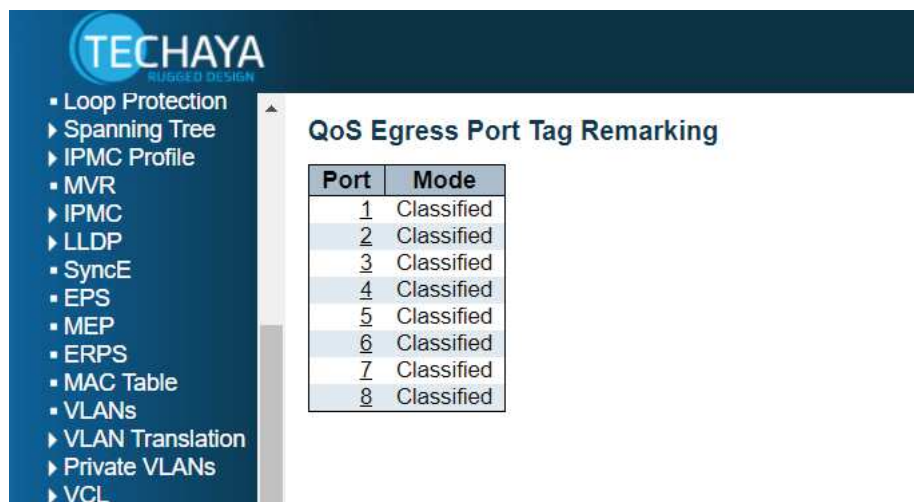
Shows “disabled” or actual queue shaper rate - e.g. “800 Mbps”.

Port

Shows “disabled” or actual port shaper rate - e.g. “800 Mbps”.

4.85 QoS – Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.



Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified

4.85.1 QoS Tag Remarking

The displayed settings are:

Port

Displays the logical port for the settings contained in the same row.

Click on the port number in order to configure the shapers.

Mode

Shows the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

4.86 QoS – Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

TECHAYA
RUGGED DESIGN

- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- ▶ VLAN Translation
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▼ Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs
 - ECEs
- ▼ QoS
 - Port Classification
 - Port Policing
 - Queue Policing

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 ▼

Save Reset

4.86.1 QoS Tag Remarking

The displayed settings are:

Port

The Port column shows the list of ports for which you can configure dscp ingress and egress settings.

Ingress

In Ingress settings you can change ingress translation and classification settings for individual ports.

There are two configuration parameters available in Ingress:

1. Translate
2. Classify

1.Translate

To Enable the Ingress Translation click the checkbox.

2. Classify

Classification for a port have 4 different values.

Disable: No Ingress DSCP Classification.

DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.

Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.

All: Classify all DSCP.

Egress

Port Egress Rewriting can be one of -

Disable: No Egress rewrite.

Enable: Rewrite enabled without remapping.

Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table.

Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

4.86.2 Port DSEP Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.87 QoS – DSCP Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

TECHAYA
RUGGED DESIGN

- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- ▶ VLAN Translation
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▼ Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs
 - ECEs
- ▼ QoS
 - Port Classification
 - Port Policing
 - Queue Policing
 - Port Scheduler
 - Port Shaping
 - Port Tag Remark
 - Port DSCP
 - DSCP-Based QoS
 - DSCP Translation
 - DSCP Classification
 - QoS Control List
 - Storm Policing
- Mirroring
- UPnP
- PTP
- ▶ GVRP
- sFlow
- UDLD
- ▶ Monitor
- ▶ Diagnostics
- ▶ Maintenance

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 ▼

4.87.1 QoS DSCP based QoS Ingress Classification

The displayed settings are:

DSCP

Maximum number of supported DSCP values are 64.

Trust

Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level.

Frames with untrusted DSCP values are treated as a non-IP frame.

QoS class

QoS class value can be any of (0-7).

DPL

Drop Precedence Level (0-1)

4.87.2 DSCP Based QoS Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.88 QoS – DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.



- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- ▶ VLAN Translation
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▼ Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs
 - ECEs
- ▼ QoS
 - Port Classification
 - Port Policing
 - Queue Policing
 - Port Scheduler
 - Port Shaping
 - Port Tag Remark
 - Port DSCP
 - DSCP-Based QoS
 - DSCP Translation
 - DSCP Classification
 - QoS Control List
 - Storm Policing
- Mirroring
- UPnP
- PTP
- ▶ GVRP
- sFlow
- UDLD
- ▶ Monitor
- ▶ Diagnostics
- ▶ Maintenance

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<> ▼	☐	<> ▼	<> ▼
0 (BE)	0 (BE) ▼	☐	0 (BE) ▼	0 (BE) ▼
1	1 ▼	☐	1 ▼	1 ▼
2	2 ▼	☐	2 ▼	2 ▼
3	3 ▼	☐	3 ▼	3 ▼
4	4 ▼	☐	4 ▼	4 ▼
5	5 ▼	☐	5 ▼	5 ▼
6	6 ▼	☐	6 ▼	6 ▼
7	7 ▼	☐	7 ▼	7 ▼
8 (CS1)	8 (CS1) ▼	☐	8 (CS1) ▼	8 (CS1) ▼
9	9 ▼	☐	9 ▼	9 ▼
10 (AF11)	10 (AF11) ▼	☐	10 (AF11) ▼	10 (AF11) ▼
11	11 ▼	☐	11 ▼	11 ▼
12 (AF12)	12 (AF12) ▼	☐	12 (AF12) ▼	12 (AF12) ▼
13	13 ▼	☐	13 ▼	13 ▼
14 (AF13)	14 (AF13) ▼	☐	14 (AF13) ▼	14 (AF13) ▼
15	15 ▼	☐	15 ▼	15 ▼
16 (CS2)	16 (CS2) ▼	☐	16 (CS2) ▼	16 (CS2) ▼
17	17 ▼	☐	17 ▼	17 ▼
18 (AF21)	18 (AF21) ▼	☐	18 (AF21) ▼	18 (AF21) ▼
19	19 ▼	☐	19 ▼	19 ▼
20 (AF22)	20 (AF22) ▼	☐	20 (AF22) ▼	20 (AF22) ▼
21	21 ▼	☐	21 ▼	21 ▼
22 (AF23)	22 (AF23) ▼	☐	22 (AF23) ▼	22 (AF23) ▼
23	23 ▼	☐	23 ▼	23 ▼
24 (CS3)	24 (CS3) ▼	☐	24 (CS3) ▼	24 (CS3) ▼
25	25 ▼	☐	25 ▼	25 ▼
26 (AF31)	26 (AF31) ▼	☐	26 (AF31) ▼	26 (AF31) ▼
27	27 ▼	☐	27 ▼	27 ▼
28 (AF32)	28 (AF32) ▼	☐	28 (AF32) ▼	28 (AF32) ▼

4.88.1 QoS DSCP Translation

The displayed settings are:

DSCP

Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress

Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

There are two configuration parameters for DSCP Translation

1. Translate
2. Classify

1.Translate

DSCP at Ingress side can be translated to any of (0-63) DSCP values.

2.Classify

Click to enable Classification at Ingress side.

Egress

There are the following configurable parameters for Egress side -

1. Remap DP0 Controls the remapping for frames with DP level 0.
2. Remap DP1 Controls the remapping for frames with DP level 1.

1. Remap DP0

Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

2. Remap DP1

Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

4.88.2 DSCP Translation Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.89 QoS – DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.

TECHAYA
RUGGED DESIGN

- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- VLAN Translation
- Private VLANs
- VCL
- Voice VLAN
- Ethernet Services
 - Ports
 - L2CP
 - Bandwidth Profiles
 - EVCs

DSCP Classification

QoS Class	DSCP DP0	DSCP DP1
*	<>	<>
0	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)

Save Reset

4.89.1 QoS DSCP Classification

The displayed settings are:

QoS Class

Actual QoS class.

DSCP DP0

Select the classified DSCP value (0-63) for Drop Precedence Level 0..

DSCP DP1

Select the classified DSCP value (0-63) for Drop Precedence Level 1.

4.89.2 DSCP Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.90 QoS Control List

This page shows the QoS Control List (QCL), which is made up of the QoS Control Entries (QCEs). Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.

Click on the lowest plus sign to add a new QCE to the list.



- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- ▶ VLAN Translation
- ▶ Private VLANs

QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action					
									CoS	DPL	DSCP	PCP	DEI	Policy
														+

4.90.1 QoS Control List Configuration

QCE

Display the QCE ID.

Port

Display the list of ports configured with the QCE or 'Any'..

DMAC

Display the destination MAC address. Possible values are:

- Any: Match any DMAC
- Unicast: Match unicast DMAC
- Multicast: Match multicast DMAC
- Broadcast: Match broadcast DMAC

The default value is "Any".

SMAC

Match specific source MAC address or 'Any'.

If a port is configured to match on destination addresses, this field indicates the DMAC.

Tag Type

Display the tag type. Possible values are:

- Any: Match tagged and untagged frames
- Untagged: Match untagged frames

Tagged: Match tagged frames

The default value is "Any".

VID

Display the VLAN ID, either a specific VID or range of VIDs. VID can be in the range 1-4095 or "Any".

PCP

Display the Priority Code Point. Valid values of PCP are:

Specific: (0, 1, 2, 3, 4, 5, 6, 7)

Range: (0-1, 2-3, 4-5, 6-7, 0-3, 4-7)

"Any"

DEI

Display the Drop Eligible Indicator. Valid values of DEI are 0, 1 or "Any".

Frame Type

Display the type of frame. Possible values are:

Any: Match any frame type

Ethernet: Match EtherType frames

LLC: Match (LLC) frames

SNAP: Match (SNAP) frames

IPv4: Match IPv4 frames

IPv6: Match IPv6 frames

Action

Display the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

CoS: Classify Class of Service

DPL: Classify Drop Precedence Level

DSCP: Classify DSCP value

PCP: Classify PCP value

DEI: Classify DEI value

Policy: Classify ACL Policy number

Modification Buttons

You can modify each QCE (QoS Control Entry) in the table using the following buttons:



: Inserts a new QCE before the current row



: Edits the QCE



: Moves the QCE up the list



: Moves the QCE down the list



: Deletes the QCE



: The lowest plus sign adds a new entry at the bottom of the QCE listings

4.90.2 QCE Configuration

This page allows the user to edit and insert a single QoS Control Entry (QCE) at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.

Open this page by clicking add (+) or edit (e) from the QoS Control List Configuration table.

Port Members

Check the checkbox button to include the port in the QCL entry. By default all ports are included.

- ☒ Include the port in the QCL entry
- ☐ Do not include the port in the QCL entry

4.90.2.1 Key Parameters

Key configuration is described as below.

DMAC

Set or show the Destination MAC address. Possible values are:

- Unicast
- Multicast
- Broadcast
- Any

SMAC

Set or show the Source MAC address:

- Specific – a field opens for the user to enter the MAC address: xx-xx-xx-xx-xx-xx
- Any

If a port is configured to match on DMAC/DIP, this field is the Destination MAC address.

Tag

Set or show the value of the Tag. Possible values are:

- Untagged
- Tagged
- Any

VID

Set or show a valid VLAN ID.

- Specific – a field opens for the user to enter the VLAN ID
- Range – two field open for the user to enter the range of VLAN IDs
- Any

Possible values are in the range 1-4095 or “Any”

The user can enter either a specific value or a range of VIDs.

PCP

Set or show the value of the PCP, either a specific value (0, 1, 2, 3, 4, 5, 6, 7) or a range of values (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or “Any”.

DEI

Set or show the value of the DEI. Values can be “0”, “1”, or “Any”.

Frame Type

Frame Type can have any of the following values:

- Any
- EtherType
- LLC
- SNAP
- IPv4
- IPv6

After the user selects a Frame Type, a table will pop up with specific parameters for that Frame Type (except for “Any”). The parameters per Frame Type are given below:

EtherType Parameters

Set or show the EtherType Parameters. When the “Specific” option is selected for the EtherType parameter, the user must enter a valid value for that parameter.

EtherType Parameters	
Ether Type	Specific ▼ Value: 0xFFFF

Valid Ether Type can be:

Specific: Requires a specific **Value**. Valid EtherType values are:

0x600-0xFFFF

Excluding: 0x800 (IPv4) and 0x86DD (IPv6)

Any

LLC Parameters

Set or show the LLC Parameters. When the “Specific” option is selected for an LLC parameter, the user must enter a valid value for that parameter.

LLC Parameters		
SSAP Address	Specific ▼	Value: 0xFF
DSAP Address	Specific ▼	Value: 0xFF
Control	Specific ▼	Value: 0xFF

SSAP Address:

Specific: **Value:** valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF

Any

DSAP Address:

Specific: **Value:** valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF

Any

Control:

Specific: **Value:** Control field can vary from 0x00 to 0xFF

Any

SNAP Parameters

Set or show the SNAP Parameters. When the “Specific” option is selected for a SNAP parameter, the user must enter a valid value for that parameter.

SNAP Parameters	
PID	Specific ▼ Value: 0xFFFF

PID:

Specific: **Value:** valid PID (a.k.a Ether Type) can be 0x0000-0xFFFF

Any

IPv4 Parameters

Set or show the IPv4 Parameters. When one of the following options is selected for an IPv4 parameter: "Specific", "Other", or "Range" the user must enter a valid value in each of the value fields that open for that parameter.

IPv4 Parameters			
Protocol	Other ▾	Value: 0	
SIP	Specific ▾	Value: 0.0.0.0	Mask: 0.0.0.0
IP Fragment	Any ▾		
DSCP	Range ▾	0 (BE) ▾	63 ▾

Protocol:

Any

UDP

TCP

Other: **Value:** IP protocol number: 0-255

Source IP:

Specific: **Value/Mask:** Source IP address in value/mask format

Any

IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When 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. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.

IP Fragment: IPv4 frame fragmented option values:

Yes

No

Any

DSCP: Diffserv Code Point (DSCP) values:

Specific value

Range of values

Any

Values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

IPv4 - TCP/UDP Parameters

UDP Parameters				
Sport	Specific ▼	Value:		
Dport	Range ▼	From:		To:

Sport: Source TCP/UDP port values:

Specific: Value: (0-65535)

Any

Set a specific or port range applicable for IP protocol TCP/UDP.

Dport: Destination TCP/UDP port values:

Specific: Value: (0-65535)

Any

Set a specific or port range applicable for IP protocol TCP/UDP.

IPv6 Parameters

Set or show the IPv6 Parameters. When one of the following options is selected for an IPv6 parameter: "Specific", "Other", or "Range" the user must enter a valid value in each of the value fields that open for that parameter.

IPv6 Parameters				
Protocol	Other ▼	Value:	0	
SIP (32 LSB)	Specific ▼	Value:	0.0.0.0	Mask: 0.0.0.0
DSCP	Range ▼	0 (BE)	▼	63 ▼

Protocol:

Any

UDP

TCP

Other: Value: IP protocol number: 0-255

SIP:

Specific: Value/Mask: 32 LS bits of IPv6 source address in value/mask format

Any

If a port is configured to match on DMAC/DIP, this field is the Destination IP address.

DSCP: Diffserv Code Point (DSCP) values:

Specific value

Range of values

Any

Values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

IPv6 - TCP/UDP Parameters

UDP Parameters			
Sport	Specific ▼	Value:	
Dport	Range ▼	From:	To:

Sport: Source TCP/UDP port values:

Specific: Value: (0-65535)

Any

Set a specific or port range applicable for IP protocol TCP/UDP.

Dport: Destination TCP/UDP port values:

Specific: Value: (0-65535)

Any

Set a specific or port range applicable for IP protocol TCP/UDP.

Action Parameters

CoS: Class of Service values: (0-7) or "Default"

DP: Drop Precedence Level values: (0-1) or "Default"

DSCP: DSCP values: (0-63, BE, CS1-CS7, EF, or AF11-AF43) or "Default"

"Default" means that the default classified value is not modified by this QCE.

4.90.3 QCE Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

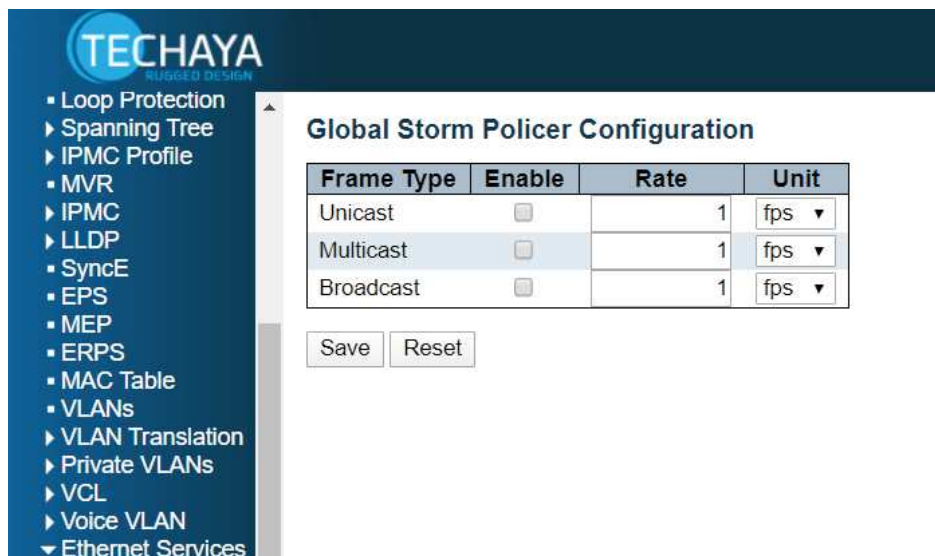
Cancel: Click to undo any changes made locally and return to the previous page

4.91 QoS – Storm Control

This page allows the user to configure the Storm control parameters for the switch.

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.



TECHAYA
RUGGED DESIGN

- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLANs
- ▶ VLAN Translation
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▼ Ethernet Services

Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	☐	1	fps ▼
Multicast	☐	1	fps ▼
Broadcast	☐	1	fps ▼

Save Reset

4.91.1 Storm Control Configuration

The displayed settings are:

Frame Type

This column displays the Frame Type to be configured in this row. The Frame Types are:

- Unicast
- Multicast
- Broadcast.

Enable

Enable or disable the storm control status for the given frame type.

- ☒ Enabled – the storm control status is enabled
- ☐ Disabled – the storm control status is disabled (This is the default.)

Rate

Controls the rate for the global storm policer. This value is restricted to 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer.

Unit

Controls the unit of measure for the global storm policer rate as fps or kfps.

4.91.2 Storm Control Configuration Buttons

Save: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.92 Mirroring & Remote Mirroring

This page allows the user to configure the Mirroring parameters for the switch.

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. The traffic to be copied on the mirror port is selected as follows:



- ▼ Configuration
 - ▶ System
 - ▶ Green Ethernet
 - ▶ Thermal Protection
 - ▶ Ports
 - ▶ DHCP
 - ▶ Security
 - ▶ Aggregation
 - ▶ Link OAM
 - ▶ Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - ▶ MVR
 - ▶ IPMC
 - ▶ LLDP
 - ▶ SyncE
 - ▶ EPS
 - ▶ MEP
 - ▶ ERPS
 - ▶ MAC Table
 - ▶ VLANs
 - ▶ VLAN Translation
 - ▶ Private VLANs
 - ▶ VCL
 - ▶ Voice VLAN
 - ▶ Ethernet Services
 - ▶ QoS
 - ▶ Mirroring
 - ▶ UPnP
 - ▶ PTP
 - ▶ GVRP

Mirroring & Remote Mirroring Configuration

Mode	Disabled ▼
Type	Mirror ▼
VLAN ID	200
Reflector Port	Port 1 ▼

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 ▼	☐	☐
CPU	Disabled ▼	☐	☐

4.92.1 Mirror and Remote Mirroring Configuration

The displayed settings are:

Mode

To Enabled/Disabled 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.

Source: The switch is a source node for monitor flow. The source port(s), reflector port and intermediate port(s) are located on this switch.

Intermediate: The switch is a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source switch to destination switch. The intermediate ports are located on this switch.

Destination: The switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are 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.

In the stacking mode, you need to select switch ID to select the correct device.

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.

4.92.2 Source VLAN(s) Configuration

The switch supports VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.

Note1: The Mirroring session shall have either ports or VLANs as sources, but not both.

4.92.3 Remote Mirroring Port Configuration

The following table is used for port role selecting.

Port

This column displays the logical port to be configured in this row.

Source

Set or show the mirror mode.

Disabled: Neither frames transmitted nor frames received are mirrored.

Both: Frames received and frames transmitted are mirrored on the Intermediate/Destination port.

Rx only: Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored.

Tx only: Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored.

Note: For a given port, a frame is only transmitted once. Therefore it is not possible to mirror the mirror port Tx frames. As a result, the mode for the selected mirror port is limited to Disabled or Rx only.

Intermediate

Select intermediate port.

This checkbox is designed for Remote Mirroring.

The intermediate port is a switched port to connect to 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.

4.92.4 Configuration Guideline for All Features

When the switch is running on Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled.

For example, the administrator is not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port.

All recommended settings are described as follows.

	Impact	reflector port	intermediate port	destination port
arp_inspection	High	* disabled	* disabled	
acl	Critical	* disabled	* disabled	* disabled
dhcp_relay	High	* disabled	* disabled	
dhcp_snooping	High	* disabled	* disabled	
ip_source_guard	Critical	* disabled	* disabled	* disabled
ipmc/igmpsnp	Critical			
ipmc/mlidsnp	Critical			
lACP	Low			o disabled
lldp	Low			o disabled
mac_learning	Critical	* disabled	* disabled	* disabled
mstp	Critical	* disabled		o disabled
mvr	Critical			
nas	Critical	* authorized	* authorized	* authorized
psec	Critical	* disabled	* disabled	* disabled
qos	Critical	* unlimited	* unlimited	* unlimited
upnp	Low			o disabled
mac-based vlan	Critical	* disabled	* disabled	
protocol-based vlan	Critical	* disabled	* disabled	
vlan_translation	Critical	* disabled	* disabled	* disabled
voice_vlan	Critical	* disabled	* disabled	
mrp	Low			o disabled
mvrp	Low			o disabled

Note:

* -- must

o -- optional

Impact: Critical/High/Low

Critical 5 packets -> 0 packet

High 5 packets -> 4 packets

Low 5 packets -> 6 packets

4.92.1 Mirror Configuration Buttons

Apply: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.93 UPnP

This page allows the user to configure the UPnP parameters for the switch.

UPnP Configuration	
Mode	Disabled ▼
TTL	4
Advertising Duration	100

Save Reset

4.93.1 UPnP Configuration

The displayed settings are:

Mode

Indicates the UPnP operation mode. Possible modes are:

Enabled: Enable UPnP mode operation.

Disabled: Disable UPnP mode operation.

When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

TTL

The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.

Advertising Duration

The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

4.93.2 UPnP Configuration Buttons

Apply: Click to save all changes

Reset: Click to undo any changes made locally and revert to previously saved values

4.94 PTP

This page allows the user to configure and inspect the current PTP clock settings.

The screenshot shows the TECHAYA web interface with a sidebar menu on the left and a main configuration area on the right. The sidebar menu includes options like System, Green Ethernet, Thermal Protection, Ports, DHCP, Security, Aggregation, Link OAM, Loop Protection, Spanning Tree, IPMC Profile, MVR, IPMC, LLDP, SyncE, EPS, MEP, ERPS, MAC Table, VLANs, VLAN Translation, Private VLANs, VCL, Voice VLAN, Ethernet Services, QoS, Mirroring, UPnP, and PTP. The main configuration area is titled 'PTP External Clock Mode' and contains a table with the following settings:

One_PPS_Mode	Disable
External Enable	False
Adjust Method	LTC frequency
Clock Frequency	1

Below this table is a section titled 'PTP Clock Configuration' which contains a table with the following headers: Delete, Clock Instance, Device Type, and Profile. The table body shows 'No Clock' and 'Instances Present'. At the bottom of this section are three buttons: 'Add New PTP Clock', 'Save', and 'Reset'.

4.94.1 PTP External Clock Configuration

The displayed settings are:

One_PPS_Mode

This Selection box will allow you to select the One_pps_mode configuration.

The following values are possible:

1. Output : Enable the 1 pps clock output
2. Input : Enable the 1 pps clock input
3. Disable : Disable the 1 pps clock in/out-put.

External Enable

This Selection box will allow you to configure the External Clock output.

The following values are possible:

1. True : Enable the external clock output
2. False : Disable the external clock output.

Adjust Method

This Selection box will allow you to configure the Frequency adjustment configuration.

1. LTC frequency : Select Local Time Counter (LTC) frequency control
2. SyncE-DPLL : Select SyncE DPLL frequency control, if allowed by SyncE
3. Oscillator : Select an oscillator independent of SyncE for frequency control, if supported by the HW
4. LTC phase : Select Local Time Counter (LTC) phase control (assumes that the frequency is locked by means of SyncE).

Clock Frequency

This will allow to set the Clock Frequency.

The possible range of values are 1 - 25000000 (1 - 25MHz).

4.94.2 PTP Clock Configuration**Delete**

Check this box and click on 'Save' to delete the clock instance.

Inst

Indicates the Instance of a particular Clock Instance [0..3].

Click on the Clock Instance number to edit the Clock details.

ClkDom

Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3]. More instances may use the same clock domain, e.g. a Boundary clock and a Transparent clock. Only one Slave or Boundary clock is allowed within the same Clock domain.

Device Type

Indicates the Type of the Clock Instance. There are five Device Types.

1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.
2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.
3. E2e Transp - clock's Device Type is End to End Transparent Clock.
4. Master Only - clock's Device Type is Master Only.
5. Slave Only - clock's Device Type is Slave Only.

Profile

Indicates the profile used by the clock.

Port List

Set check mark for each port configured for this Clock Instance. One port can only be active within one Clock domain. I.e. enabling a port which is already active in another Clock domain is rejected.

2 Step Flag

Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used.

Clock Identity

It shows unique clock identifier.

One Way

If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

Protocol

Transport protocol used by the PTP protocol engine

Ethernet PTP over Ethernet multicast

EthernetMixed PTP using a combination of Ethernet multicast and unicast

IPv4Multi PTP over IPv4 multicast

IPv4Mixed PTP using a combination of IPv4 multicast and unicast

IPv4Uni PTP over IPv4 unicast

Note : IPv4 unicast protocol only works in Master only and Slave only clocks

See parameter Device Type.

In a unicast Slave only clock you also need configure which master clocks to request Announce and Sync messages from. See: Unicast Slave Configuration.

VID

VLAN Identifier used for tagging the PTP frames.

Note: Packets are tagged if the port is configured for vlan tagging for the configured VID.

PCP

Priority Code Point value used for PTP frames.

4.94.3 PTP Configuration Buttons

Add New PTP Clock: lick to create a new clock instance.

Save: Click to save all changes

Reset: Click to reset the page immediately.

4.95 GVRP – Global Configuration

This page allows you to configure the global GVRP configuration settings that are commonly applied to all GVRP enabled ports.

The screenshot shows the 'GVRP Configuration' page in the TECHAYA web interface. On the left is a sidebar with a tree view containing 'Configuration', 'System', 'Green Ethernet', 'Thermal Protection', 'Ports', 'DHCP', 'Security', 'Aggregation', 'Link OAM', 'Loop Protection', 'Spanning Tree', 'IPMC Profile', 'MVR', and 'IPMC'. The main area is titled 'GVRP Configuration' and contains a checkbox 'Enable GVRP' which is checked. Below it is a table with two columns: 'Parameter' and 'Value'.

Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

Below the table is a 'Save' button. In the top right corner of the main area is a 'Refresh' button. The top of the interface has a dark blue header with the TECHAYA logo and some icons.

4.95.1 GVRP Configuration

The displayed settings are:

Enable GVRP globally_PPS_Mode

The GVRP feature is globally enabled by setting the check mark in the checkbox named Enable GVRP and pressing the Save button.

GVRP protocol timers

Join-time is a value in the range of 1-20cs, i.e. in units of one hundredth of a second. The default value is 20cs.

Leave-time is a value in the range of 60-300cs, i.e. in units of one hundredth of a second. The default is 60cs.

LeaveAll-time is a value in the range of 1000-5000cs, i.e. in units of one hundredth of a second. The default is 1000cs.

Max number of VLANsMethod

When GVRP is enabled, a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.

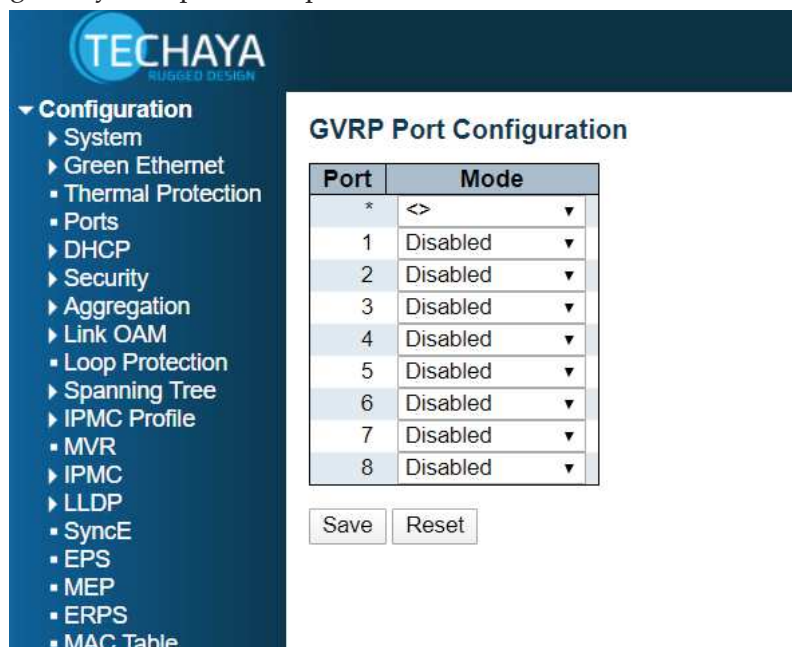
4.95.2 GVRP Configuration Buttons

Save: Click to save all changes.

4.96 GVRP – Port Configuration

This page allows you to enable or disable a port for GVRP operation.

This configuration can be performed either before or after GVRP is configured globally - the protocol operation will be the same.



Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

Save Reset

4.96.1 GVRP Port Configuration

The displayed settings are:

Port

The logical port that is to be configured.

Mode

Mode can be either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question.

4.96.2 GVRP Port Configuration Buttons

Save: Click to save all changes.

4.97 sFLOW

This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

- Configuration
 - System
 - Green Ethernet
 - Thermal Protection
 - Ports
 - DHCP
 - Security
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - LLDP
 - SyncE
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLANs
 - VLAN Translation
 - Private VLANs
 - VCL
 - Voice VLAN
 - Ethernet Services
 - QoS
 - Mirroring
 - UPnP
 - PTP
 - GVRP
 - sFlow
 - UDLD
- Monitor
- Diagnostics
- Maintenance

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	Max. Header	Enabled	Interval
*	☐	0	128	☐	0
1	☐	0	128	☐	0
2	☐	0	128	☐	0
3	☐	0	128	☐	0
4	☐	0	128	☐	0
5	☐	0	128	☐	0
6	☐	0	128	☐	0
7	☐	0	128	☐	0
8	☐	0	128	☐	0

4.97.1 Agent Configuration

IP Address

The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time.

Both IPv4 and IPv6 addresses are supported.

4.97.2 Receiver Configuration

Owner

Basically, sFlow can be configured in two ways: 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 "**Release**" 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

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.

4.97.3 Port Configuration

Port

The port number for which the configuration below applies.

Flow Sampler Enabled

Enables/disables flow sampling on this 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

Enables/disables counter polling 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.

4.97.4 sFLOW Buttons

Release: See description under Owner.

Refresh: Click to refresh the page. Note that unsaved changes will be lost.

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.98 UDLD

This page allows the user to inspect the current UDLD configurations, and possibly change them as well.

Port	UDLD mode	Message Interval
*	<>	7
1	Disable	7
2	Disable	7
3	Disable	7
4	Disable	7
5	Disable	7
6	Disable	7
7	Disable	7
8	Disable	7

Save Reset

4.98.1 UDLD Port Configuration

The displayed settings are:

Port

Port number of the switch.

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 exist 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).

4.98.2 UDLD Buttons

Save: Click to save all changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5 Web Interface - Monitor

The Web Interface – Monitor section of this manual describes the monitoring features and screens of the Switch User Interface.

From the Monitor section, the user can monitor the system by viewing:

- System information
- Statistics on the operation of the switch
- Status reports on different features on the switch and how they are operating

5.1 System – Information

The System Information page displays switch system information.

- System Contact
- System Name
- System Location
- Hardware Details
- Time
- Software Details

TECHAYA

Configuration

Monitor

System

- Information
- CPU Load
- IP Status
- Log
- Detailed Log

Green Ethernet

Thermal Protection

Ports

- State
- Traffic Overview
- QoS Statistics
- QCL Status
- Detailed Statistics

Link OAM

DHCP

Security

Aggregation

Loop Protection

Spanning Tree

MVR

IPMC

LLDP

Ethernet Services

PTP

MAC Table

VLANs

- sFlow
- UDLD

Diagnostics

Maintenance

System Information

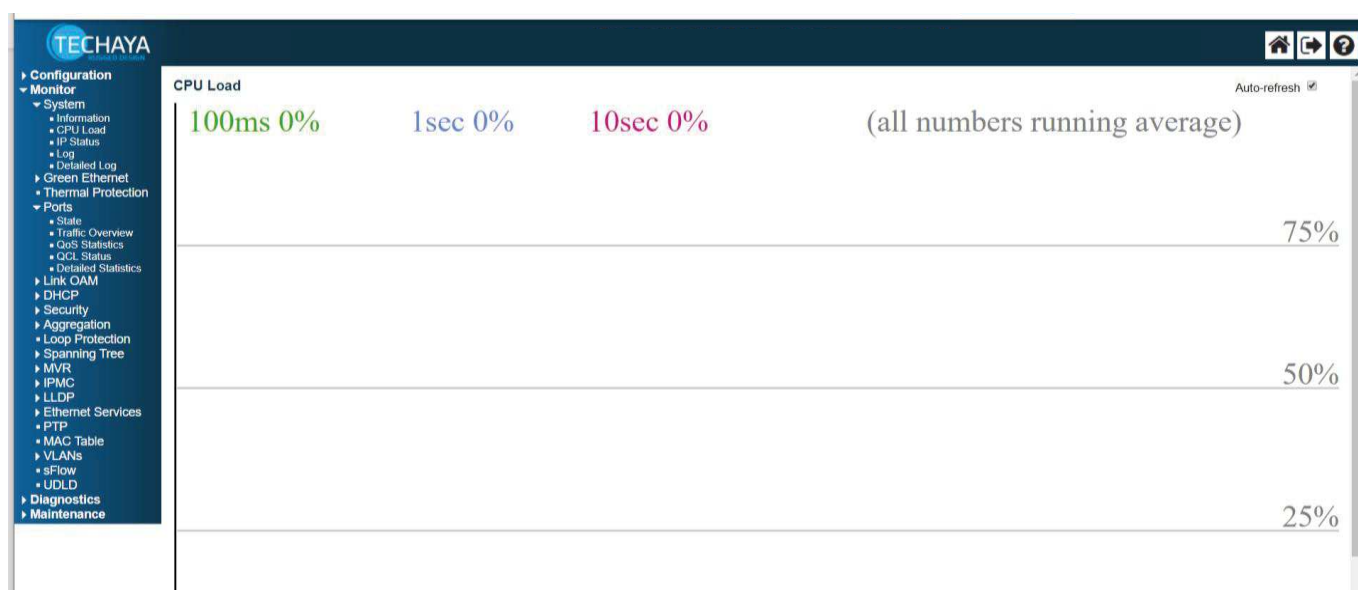
Auto-refresh ☐ Refresh

System	
Contact	
Name	M918
Location	
Hardware	
MAC Address	02-00-c1-93-4a-5f
Chip ID	VSC7428
Time	
System Date	1970-01-01T00:23:37+00:00
System Uptime	0d 00:23:37
Software	
Software Version	MILTECH-918 (standalone) 3.01.1074.1082-3.66-2019-12-13T16:29:43+02:00
Software Date	2019-12-13T16:29:43+02:00
Acknowledgments	Details

5.2 CPU Load

The CPU load 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. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.



5.2.1 CPU Load Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

5.3 System – IP Status

IP Interface

The IP Interface page shows the user the IP Interfaces, IP Routes and the Neighbour cache.

TECHAYA

Configuration

- Monitor
 - System
 - Information
 - CPU Load
 - IP Status
 - Log
 - Detailed Log
 - Green Ethernet
 - Thermal Protection
 - Ports
 - Link OAM
 - DHCP
 - Security
 - Aggregation
 - Loop Protection
 - Spanning Tree
 - MVR
 - IPMC
 - LLDP
 - Ethernet Services
 - PTP
 - MAC Table
 - VLANs
 - sFlow
 - UDLD
- Diagnostics
- Maintenance

IP Interfaces

Interface	Type	Address	Status
OS-10	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS-10	IPv4	127.0.0.1/8	
OS-10	IPv6	fe80::1/64	
OS-10	IPv6	::1/128	
VLAN1	LINK	02-00-c1-93-4a-5f	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.111/24	
VLAN1	IPv6	fe80::c1ff:fe93:4a5f/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.1.2	VLAN1:80-ce-62-4f-52-ff
fe80::c1ff:fe93:4a5f	VLAN1:02-00-c1-93-4a-5f

Auto-refresh ☐ Refresh

5.3.1 IP Interfaces

Each IP Interface has the following configurable parameters:

The name of the interface

The address type of the entry - This may be LINK or IPv4.

The current address of the interface (of the given type).

The status flags of the interface (and/or address).

5.3.2 IP Routes

Each IP Route has the following configurable parameters:

Network

The destination IP network or host address of this route.

Gateway

The gateway address of this route.

Status

The status flags of the route.

5.3.3 Neighbour cache

IP Address

The IP address of the entry.

Link Address

The Link (MAC) address for which a binding to the IP address given exist.

5.3.4 IP Interface Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every ? seconds.

5.4 System - Log

System Log Information

The System Log Information page shows the user the System Log page.

System Log Information

Level: Clear Level:

The total number of entries is 4 for the given level.

Start from ID with entries per page.

ID	Level	Time	Message
1	Informational	1970-01-01T00:00:03+00:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	1970-01-01T00:00:03+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	1970-01-01T00:02:57+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up.
4	Notice	1970-01-01T00:02:59+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.

5.4.1 System Log Information Table

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

The "Level" input field is used to filter the display system log entries.

The "Clear Level" input field is used to specify which system log entries will be cleared.

To clear specific system log entries, select the clear level first then click the button.

The "Start from ID" input field allow the user to change the starting point in this table. Clicking the button will update the displayed table starting from that or the closest next entry match.

In addition, these input fields will upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

The  will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table.

Use the  button to start over.

5.4.2 System Log Information Entry Columns

ID

The identification of the system log entry.

Level

The level of the system log entry.

Info: The system log entry is belonged information level.

Warning: The system log entry is belonged warning level.

Error: The system log entry is belonged error level

Time

The occurred time of the system log entry.

Message

The detail message of the system log entry.

5.4.3 System Log Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds.

☐ Disable Auto-refresh (This is the default.)

Refresh: Updates the table entries, starting from the current entry.

Clear: Flushes the selected entries.



Updates the table entries, starting from the first available entry.



Updates the table entries, ending at the last entry currently displayed.



Updates the table entries, starting from the last entry currently displayed.



Updates the table entries, ending at the last available entry.

5.5 System – Detailed Log

This page displays the system detailed log information. The user can arrive at this page via the main menu on the left side of the page or by clicking the ID number in the table. **שגיאה! מקור ההפניה לא נמצא.**

5.5.1 Detailed System Log Information

Level

The severity level of the system log entry.

ID

The ID (≥ 1) of the system log entry.

Message

This column displays the detailed message of the system log entry.

5.5.2 System Log Information Buttons

Refresh: Updates the system log entry to the current entry ID



Updates the system log entry to the first available entry ID



Updates the system log entry to the previous available entry ID



Updates the system log entry to the next available entry ID



Updates the system log entry to the last available entry ID

5.6 Green Ethernet – Port Power Savings

This page displays the current status for Energy Efficient Ethernet (EEE).

TECHAYA REDUCED DESIGN								
- Configuration - Monitor - System - Green Ethernet - Port Power Savings - Thermal Protection - Ports - Link OAM - DHCP - Security - Aggregation - Loop Protection - Spanning Tree - MVR - IPMC - LLDP - Ethernet Services - PTP - MAC Table - VLANs - sFlow - UDLD - Diagnostics - Maintenance								
Port Power Savings Status								
Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings	
1		✓	✗	✓	✗	✗	✗	
2		✓	✗	✗	✗	✗	✗	
3		✓	✗	✗	✗	✗	✗	
4		✓	✗	✗	✗	✗	✗	
5		✓	✗	✗	✗	✗	✗	
6		✓	✗	✗	✗	✗	✗	
7		✓	✗	✗	✗	✗	✗	
8		✓	✗	✗	✗	✗	✗	

5.6.1 Port Power Savings Status

The Port Power Savings are configured in the Port Power Savings Configuration Page. Navigate there as follows:

Configuration->Green Ethernet->Port Power Savings (for details, see section 4.7 Green Ethernet - Port Power Savings).

Port

This column displays the logical port number for this row.

Link

This column shows if the link is up for the port

Green = link up

Red = link down

LP EEE cap

This column shows if the link partner is EEE capable.

Green Check: Enabled

Red X: Disabled

EEE Ena

Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

Green Check: Enabled

Red X: Disabled

LP EEE cap

Shows if the link partner is EEE capable.

Green Check: Enabled

Red X: Disabled

EEE In power save

Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.

Green Check: Enabled

Red X: Disabled

ActiPhy Savings

Shows if the system is currently saving power due to ActiPhy.

Green Check: Enabled

Red X: Disabled

PerfectReach Savings

Shows if the system is currently saving power due to PerfectReach.

Green Check: Enabled

Red X: Disabled

5.6.2 Port Power Savings Status Buttons

Auto-refresh:

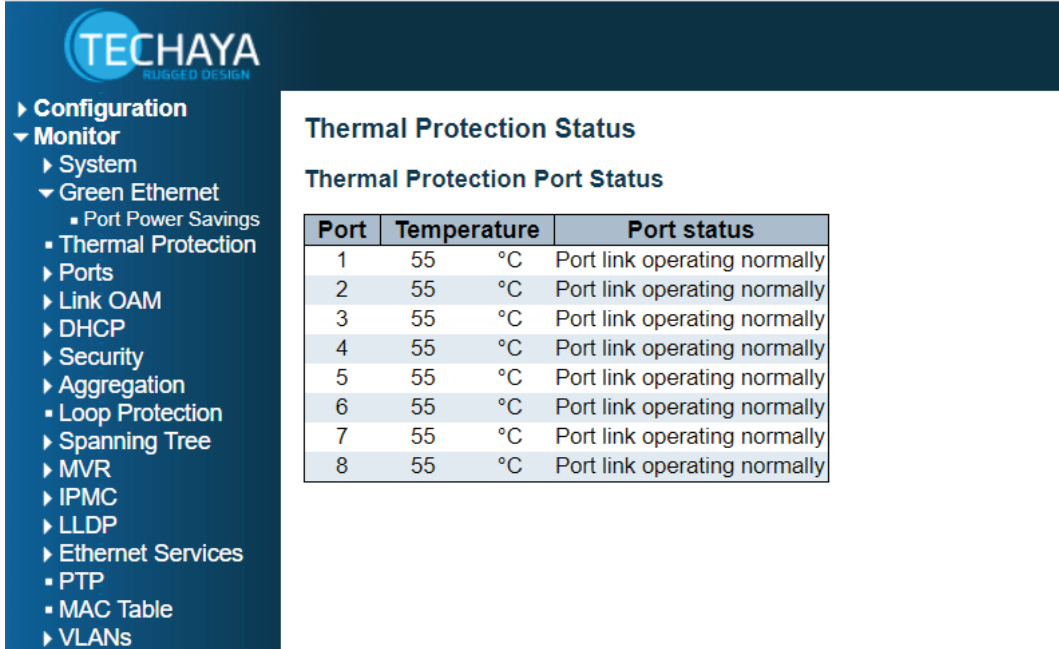
☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page

5.7 Thermal Protection

This page displays status information related to thermal protection.



TECHAYA
RUGGED DESIGN

- Configuration
- ▼ Monitor
 - System
 - ▼ Green Ethernet
 - Port Power Savings
 - Thermal Protection
 - Ports
 - Link OAM
 - DHCP
 - Security
 - Aggregation
 - Loop Protection
 - Spanning Tree
 - MVR
 - IPMC
 - LLDP
 - Ethernet Services
 - PTP
 - MAC Table
 - VLANs

Thermal Protection Status

Thermal Protection Port Status

Port	Temperature	Port status
1	55 °C	Port link operating normally
2	55 °C	Port link operating normally
3	55 °C	Port link operating normally
4	55 °C	Port link operating normally
5	55 °C	Port link operating normally
6	55 °C	Port link operating normally
7	55 °C	Port link operating normally
8	55 °C	Port link operating normally

5.7.1 Thermal Protection Port Status

Port

This column displays the switch port number for this row.

Temperature

This column shows the current chip temperature in degrees Celsius.

Port Status

This column shows if the port is thermally protected (link is down) or if the port is operating normally.

5.7.2 Port Power Savings Status Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page

5.8 Ports - State

This page displays the current switch port states



5.8.1 Port State Overview

The port states are illustrated as follows:



5.8.2 Port State Overview Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page

5.9 Ports – Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.






- Configuration
- Monitor
 - System
 - Green Ethernet
 - Port Power Savings
 - Thermal Protection
 - Ports
 - State
 - Traffic Overview
 - QoS Statistics
 - QCL Status
 - Detailed Statistics
 - Link OAM
 - DHCP
 - Security
 - Aggregation
 - Loop Protection
 - Spanning Tree

Port Statistics Overview

Auto-refresh ☐
 Refresh
 Clear

Port	Description	Packets		Bytes		Errors		Drops		Filtered
		Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1		3726	9540	465662	1164442	0	0	0	0	1084
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

5.9.1 Port Statistics Overview

The displayed counters are:

Port

This column displays the logical port number for this row. Click on the Port number to view Detailed Port Statistics.

Packets

This column displays the number of packets received and transmitted per port.

Bytes

This column displays the number of bytes received and transmitted per port.

Errors

This column displays the number of frames received in error and the number of incomplete transmissions per port.

Drops

This column displays the number of frames discarded due to ingress or egress congestion.

Filtered

This column displays the number of received frames filtered by the forwarding process.

5.9.2 Port Statistics Overview Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear the counters for all ports

5.10 Ports – QoS Statistics

This page provides an overview of general traffic statistics for all switch ports.

TECHAYA

TECHNICAL SUPPORT

Configuration

Monitor

System

- Green Ethernet
 - Port Power Savings
- Thermal Protection

Ports

- State
 - Traffic Overview
- QoS Statistics
 - QCL Status
 - Detailed Statistics

Link OAM

- DHCP

Security

Aggregation

- Loop Protection

Spanning Tree

- MVR

IPMC

- LLDP

Ethernet Services

- PTP
 - MAC Table

VLANs

- sFlow
- UDLD

Diagnostics

Maintenance

Queuing Counters

Auto-refresh

Refresh

Clear

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	3781	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9684
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

5.10.1 Queuing Counters

The displayed counters are:

Port

This column displays the logical port number for this row. Click on the Port number to view Detailed Port Statistics.

Qn

These column headers display the logical QoS queue for each column. There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx

These columns display the number of received and transmitted packets per queue.

5.10.2 Queuing Counters Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear the counters for all ports

5.11 Ports – QCL Status

This page shows the QoS Control List (QCL) status by different QCL users. Each row describes the QCE (QoS Control Entry) 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.

TECHAYA

Configuration
Monitor
System
Green Ethernet
Thermal Protection
Ports
State
Traffic Overview
QoS Statistics
QCL Status
Detailed Statistics
Link OAM
DHCP
Security

QoS Control List Status

Combined Auto-refresh Resolve Conflict Refresh

User	QCE	Port	Frame Type	Action	Conflict
				CoS DPL DSCP PCP DEI Policy	
No entries					

5.11.1 QoS Control List Status

The following QCE details are displayed:

User

This column shows the QCL user.

QCE

This column shows the QCE id.

Port

This column shows the list of ports configured with the QCE.

Frame Type

This column shows the type of frame. Possible values are:

- Any: Match any frame type.
- Ethernet: Match EtherType frames.
- LLC: Match (LLC) frames.
- SNAP: Match (SNAP) frames.
- IPv4: Match IPv4 frames.
- IPv6: Match IPv6 frames.

Action

This column shows the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

- CoS: Classify Class of Service
- DPL: Classify Drop Precedence Level
- DSCP: Classify DSCP value

Conflict

This column shows Conflict status of QCL entries. Since H/W resources are shared by multiple applications, the resources required to add a QCE may not be available when needed. In that case the conflict status is "Yes", otherwise the conflict status "No".

Note: To resolve conflict, click the **Resolve Conflict** button which releases the H/W resources required to add a QCL entry.

5.11.2 Queuing Counters Buttons

Combined ▼

Select the QCL status from the drop down list (Combined, Static, Conflict).

Resolve Conflict:

Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.12 Ports – Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

5.12.1 Detailed Port Statistics

The selected port belongs to the currently selected stack unit, as reflected by the page header.

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.

TECHAYA

TRUSSED BY DESIGN

Configuration

Monitor

System

Green Ethernet

- Port Power Savings
- Thermal Protection

Ports

- State
- Traffic Overview
- QoS Statistics
- QOL Status
- Detailed Statistics

Link OAM

DHCP

Security

Aggregation

Loop Protection

Spanning Tree

MVR

IPMC

LLDP

Ethernet Services

- PTP
- MAC Table
- VLANs
- sFlow
- UDLD

Diagnostics

Maintenance

Detailed Port Statistics

Port 1

Port 1

Auto-refresh

Refresh

Clear

Receive Total		Transmit Total	
Rx Packets	3886	Tx Packets	9894
Rx Octets	491742	Tx Octets	1217874
Rx Unicast	2092	Tx Unicast	1716
Rx Multicast	1290	Tx Multicast	8174
Rx Broadcast	504	Tx Broadcast	4
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	2105	Tx 64 Bytes	1335
Rx 65-127 Bytes	867	Tx 65-127 Bytes	7743
Rx 128-255 Bytes	637	Tx 128-255 Bytes	733
Rx 256-511 Bytes	122	Tx 256-511 Bytes	43
Rx 512-1023 Bytes	155	Tx 512-1023 Bytes	16
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	24
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	3886	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	9894
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	1103		

5.12.1.1 Receive Total and Transmit Total

Rx and Tx Packets

This row shows the number of received and transmitted (good and bad) packets.

Rx and Tx Octets

This row shows the number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast

This row shows the number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast

This row shows the number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast

This row shows the number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause

This row shows a count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

5.12.1.2 Receive and Transmit Size Counters

This section shows the number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

5.12.1.3 Receive and Transmit Queue Counters

This section shows the number of received and transmitted packets per input and output queue.

5.12.1.4 Receive Error Counters**Rx Drops**

This row shows the number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment

This row shows the number of frames received with CRC or alignment errors.

Rx Undersize

This row shows the number of short¹ frames received with valid CRC.

Rx Oversize

This row shows the number of long² frames received with valid CRC.

Rx Fragments

This row shows the number of short¹ frames received with invalid CRC.

Rx Jabber

The number of long² frames received with invalid CRC.

Rx Filtered

This row shows the number of received frames filtered by the forwarding process.

Footnotes

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.

5.12.1.5 Transmit Error Counters

Tx Drops

This row shows the number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.

This row shows the number of frames dropped due to excessive or late collisions.

5.12.2 Detailed Port Statistics Buttons

Port select box: 

The port select box determines which port is affected by clicking the buttons. Select a port from the drop-down list.

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear the counters for the selected port

5.13 Link OAM - Statistics

This page provides detailed OAM traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counter can occur at re-initialization of the management system.

Receive Total		Transmit Total	
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0
Rx Loopback Control	0	Tx Loopback Control	0
Rx Variable Request	0	Tx Variable Request	0
Rx Variable Response	0	Tx Variable Response	0
Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0
Rx Dying Gasp	0	Tx Dying Gasp	0
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0

5.13.1 Detailed Link OAM Port Statistics

Rx and Tx OAM Information PDU's

The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.

Rx and Tx Unique Error Event Notification

A count of the number of unique Event OAMPDU's received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Duplicate Error Event Notification

A count of the number of duplicate Event OAMPDU's received and transmitted on this interface. Event Notification OAMPDU's may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Loopback Control

A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Request

A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Response

A count of the number of Variable Response OAMPDUs received and transmitted on this interface.

Rx and Tx Org Specific PDU's

A count of the number of Organization Specific OAMPDUs transmitted on this interface.

Rx and Tx Unsupported Codes

A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

Rx and Tx Link fault PDU's

A count of the number of Link fault PDU's received and transmitted on this interface.

Rx and Tx Dying Gasp

A count of the number of Dying Gasp events received and transmitted on this interface.

Rx and Tx Critical Event PDU's

A count of the number of Critical event PDU's received and transmitted on this interface.

5.13.2 Detailed Link OAM Port Statistics Buttons

Port select box:

The port select box determines which port is affected by clicking the buttons. Select a port from the drop-down list.

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds.

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

Clear: Click to clear the counters for the selected port.

5.14 Link OAM – Port Status

This page provides Link OAM configuration operational status.

The displayed fields shows the active configuration status for the selected port.

TECHAYA

Detailed Link OAM Status for Port 1 Port 1 ▾ Auto-refresh ☐ Refresh

PDU Permission	Receive only
Discovery State	Fault state
Peer MAC Address	-----

Local		Peer	
Mode	Passive	Mode	-----
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	-----
Remote Loopback Support	Disabled	Remote Loopback Support	-----
Link Monitoring Support	Enabled	Link Monitoring Support	-----
MIB Retrieval Support	Disabled	MIB Retrieval Support	-----
MTU Size	1500	MTU Size	-----
Multiplexer State	Forwarding	Multiplexer State	-----
Parser State	Forwarding	Parser State	-----
Organizational Unique Identification	02-00-c1	Organizational Unique Identification	-----
PDU Revision	0	PDU Revision	-----

5.14.1 Local and Peer

Mode

The Mode in which the Link OAM is operating, Active or Passive.

Unidirectional Operation Support

This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.

Remote Loopback Support

If status is enabled, DTE is capable of OAM remote loopback mode.

Link Monitoring Support

If status is enabled, DTE supports interpreting Link Events.

MIB Retrieval Support

If status is enabled DTE supports sending Variable Response OAMPDUs.

MTU Size

It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remote's Maximum PDU Size and the smaller of the two is used.

Multiplexer State

When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sublayer. In case of discarding, the device discards all the non-OAMPDU's.

Parser State

When in forwarding state, Device is forwarding non-OAMPDUs to higher sublayer. When in loopback, Device is looping back non-OAMPDUs to the lower sublayer. When in discarding state, Device is discarding non-OAMPDUs.

Organizational Unique Identification

24-bit Organizationally Unique Identifier of the vendor.

PDU Revision

It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

PDU Permission

This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are:

- Link fault
- Receive only
- Information exchange only
- ANY

Discovery State

Displays the current state of the discovery process. Possible states are:

- Fault state
- Active state
- Passive state
- SEND_LOCAL_REMOTE_STATE
- SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE

5.14.2 Link OAM Port Status Buttons

Port select box:

The port select box determines which port is affected by clicking the buttons. Select a port from the drop-down list.

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds.
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

5.15 Link OAM – Event Status

This page allows the user to inspect the current Link OAM Link Event configurations and change them as well.

The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.

Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0

Local Frame Period Status		Remote Frame Period Status	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0

Local Symbol Period Status		Remote Symbol Period Status	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Symbol frame period errors	0	Symbol frame period errors	0
Symbol frame period error events	0	Symbol frame period error events	0

Local Event Seconds Summary Status		Remote Event Seconds Summary Status	
Event Seconds Summary Time Stamp	0	Event Seconds Summary Time Stamp	0
Event Seconds Summary Window	0	Event Seconds Summary Window	0
Event Seconds Summary Threshold	0	Event Seconds Summary Threshold	0
Event Seconds Summary Events	0	Event Seconds Summary Events	0
Event Seconds Summary Error Total	0	Event Seconds Summary Error Total	0
Event Seconds Summary Event Total	0	Event Seconds Summary Event Total	0

5.15.1 Link OAM Link Event Status

Port

The switch port number.

Sequence Number

This two-octet field indicates the total number of events occurred at the remote end.

Frame Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame error event window

This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one minute.

Frame error event threshold

This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.

MTU Size

It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

Frame errors

This four-octet field indicates the number of detected errored frames in the period.

Total frame errors

This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.

Total frame error events

This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.

Frame Period Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame Period Error Event Window

This four-octet field indicates the duration of period in terms of frames.

Frame Period Error Event Threshold

This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

Frame Period Errors

This four-octet field indicates the number of frame errors in the period.

Total frame period errors

This eight-octet field indicates the sum of frame errors that have been detected since the OAM sublayer was reset.

Total frame period error events

This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sublayer was reset.

Symbol Period Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Symbol Period Error Event Window

This eight-octet field indicates the number of symbols in the period.

Symbol Period Error Event Threshold

This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.

Symbol Period Errors

This eight-octet field indicates the number of symbol errors in the period.

Symbol frame period errors

This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.

Symbol frame period error events

This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset.

Event Seconds Summary Time Stamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Window

This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Threshold

This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.

Event Seconds Summary Events

This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

Event Seconds Summary Error Total

This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.

Event Seconds Summary Event Total

This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32bit unsigned integer.

5.15.2 Link OAM Event Status Buttons

Port select box:

The port select box determines which port is affected by clicking the buttons. Select a port from the drop-down list.

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3

seconds.

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

Clear: Click to clear the counters for the selected port.

5.16 DHCP – Server - Statistics

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.

TECHAYA

Configuration
Monitor
System
Green Ethernet
Thermal Protection
Ports
Link OAM
DHCP
Server
Statistics
Binding
Declined IP
Snooping Table
Relay Statistics
Detailed Statistics
Security
Aggregation
Loop Protection
Spanning Tree
MVR
IPMC
LLDP
Ethernet Services
PTP
MAC Table
VLANs
sFlow
UDLD

Auto-refresh ☐ Refresh Clear

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

5.16.1 Database Counters

Display counters of various databases.

Pool

Number of pools.

Excluded IP Address

Number of excluded IP address ranges.

Declined IP Address

Number of declined IP addresses.

5.16.2 Binding Counters

Display counters of various databases.

Automatic Binding

Number of bindings with network-type pools.

Manual Binding

Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

Expired Binding

Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

5.16.3 DHCP Message Received Counters

Display counters of DHCP messages received by DHCP server.

DISCOVER

Number of DHCP DISCOVER messages received.

REQUEST

Number of DHCP REQUEST messages received.

DECLINE

Number of DHCP DECLINE messages received.

RELEASE

Number of DHCP RELEASE messages received.

INFORM

Number of DHCP INFORM messages received.

5.16.4 **DHCP Message Sent Counters**

Display counters of DHCP messages sent by DHCP server.

OFFER

Number of DHCP OFFER messages sent.

ACK

Number of DHCP ACK messages sent.

NAK

Number of DHCP NAK messages sent.

5.16.5 **DHCP Server Buttons**

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds.

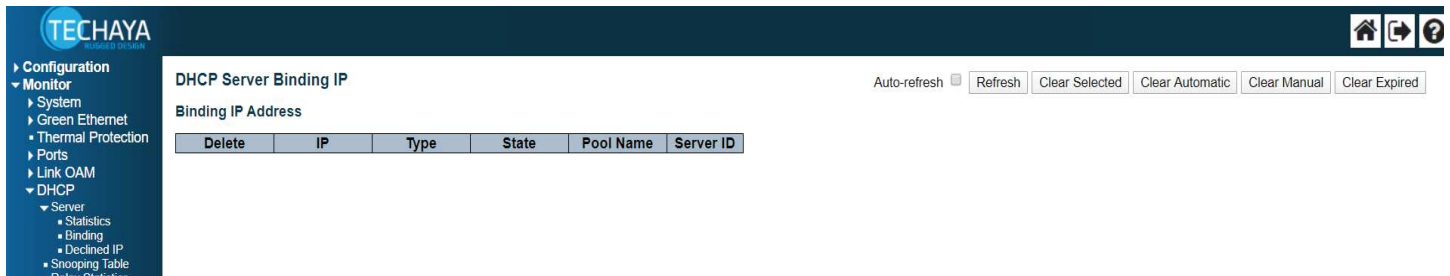
☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

Clear: Click to clear the counters for the selected port.

5.17 DHCP – Server – Building IP

This page displays bindings generated for DHCP clients.



TECHAYA

Configuration
Monitor
System
Green Ethernet
Thermal Protection
Ports
Link OAM
DHCP
Server
Statistics
Binding
Declined IP
Snooping Table
Delay Statistics

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

5.17.1 Binding IP Address

Display all bindings.

IP

IP address allocated to DHCP client.

Type

Type of binding. Possible types are Automatic, Manual, Expired.

State

State of binding. Possible states are Committed, Allocated, Expired.

Pool Name

The pool that generates the binding.

Server ID

Server IP address to service the binding.

5.17.2 DHCP Building IP Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds.

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

Clear: Click to clear the counters for the selected port.

Clear selected: Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

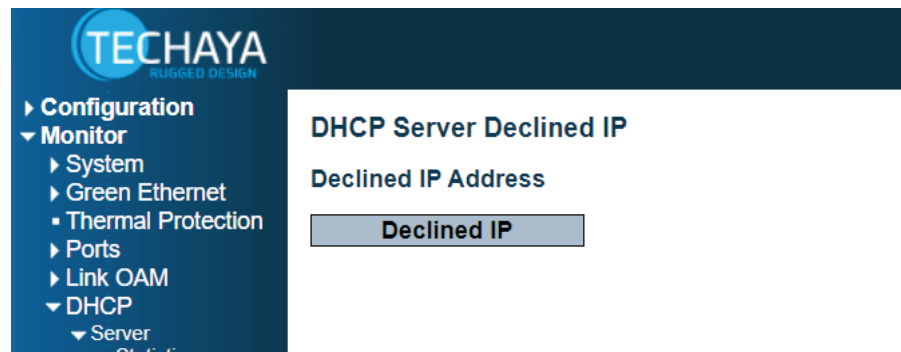
Clear automatic: Click to clear all Automatic bindings and Change them to Expired bindings.

Clear manual: Click to clear all Manual bindings and Change them to Expired bindings.

Clear expired: Click to clear all Expired bindings and free them.

5.18 DHCP – Server – Declined IP

This page displays declined IP addresses.



5.18.1 Declined IP Addresses

Display IP addresses declined by DHCP clients.

Declined IP

List of IP addresses declined.

5.18.2 Declined IP Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds.
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

5.19 DHCP – Snooping Table

This page displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

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					

Auto-refresh ☐ Refresh |<< >>

5.19.1 Navigating the DHCP snooping Table

Each page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic DHCP snooping Table.

The "MAC address" and "VLAN" input fields allow the user to select the starting point in the Dynamic DHCP snooping Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next Dynamic DHCP snooping Table match. In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

5.19.2 DHCP snooping Table Columns

MAC Address

User MAC address of the entry.

VLAN ID

VLAN-ID in which the DHCP traffic is permitted.

Source Port

Switch Port Number for which the entries are displayed.

IP Address

User IP address of the entry.

IP Subnet Mask

User IP subnet mask of the entry.

DHCP Server Address

DHCP Server address of the entry.

5.19.3 Snooping Table Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds.

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

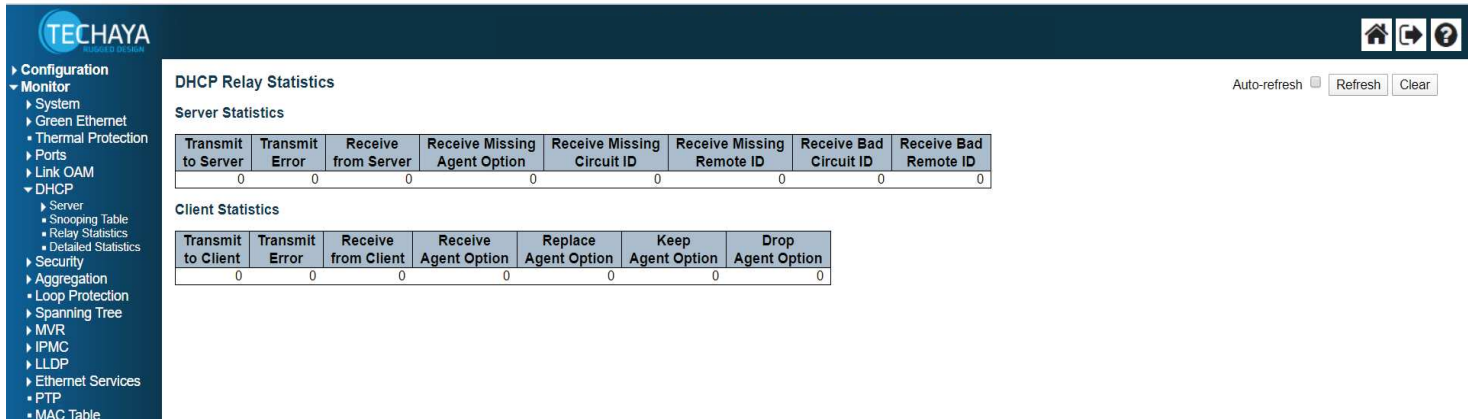
Clear: Flushes all dynamic entries.

|<<: Updates the table starting from the first entry in the Dynamic DHCP snooping Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

5.20 DHCP – Relay Statistics

This page provides statistics for DHCP relay.



5.20.1 Server 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 Server

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.

5.20.2 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.

5.20.3 Relay Statistics Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds.
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

Clear: Flushes all dynamic entries.

5.21 DHCP – Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

TECHAYA Web Interface - Monitor

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		

Combined Port 1 Auto-refresh Refresh Clear

5.21.1 Receive and Transmit Packets

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 Discarded checksum error

The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted

The number of discarded packet that are coming from untrusted port.

5.21.2 Detailed Statistics Buttons

The DHCP user select box determines which user is affected by clicking the buttons.

Select Box : Select a DHCP user from the drop down list:

Combined
Normal Forward
Server
Client
Snooping
Relay

Port select box:

The port select box determines which port is affected by clicking the buttons. Select a port from the drop-down list.

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds.
☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

Clear: Flushes all dynamic entries.

5.22 Security – Access Management

This page provides statistics for access management.

Access Management Statistics

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

Auto-refresh ☐ Refresh Clear

5.22.1 Access Management Statistics

The displayed counters are:

Interface

This column displays the interface type through which the remote host can access the switch.

Received Packets

This column displays the number of received packets from the interface when access management mode is enabled.

Allowed Packets

This column displays the number of allowed packets from the interface when access management mode is enabled.

Discarded Packets

This column displays the number of discarded packets from the interface when access management mode is enabled.

5.22.2 Access Management Statistics Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

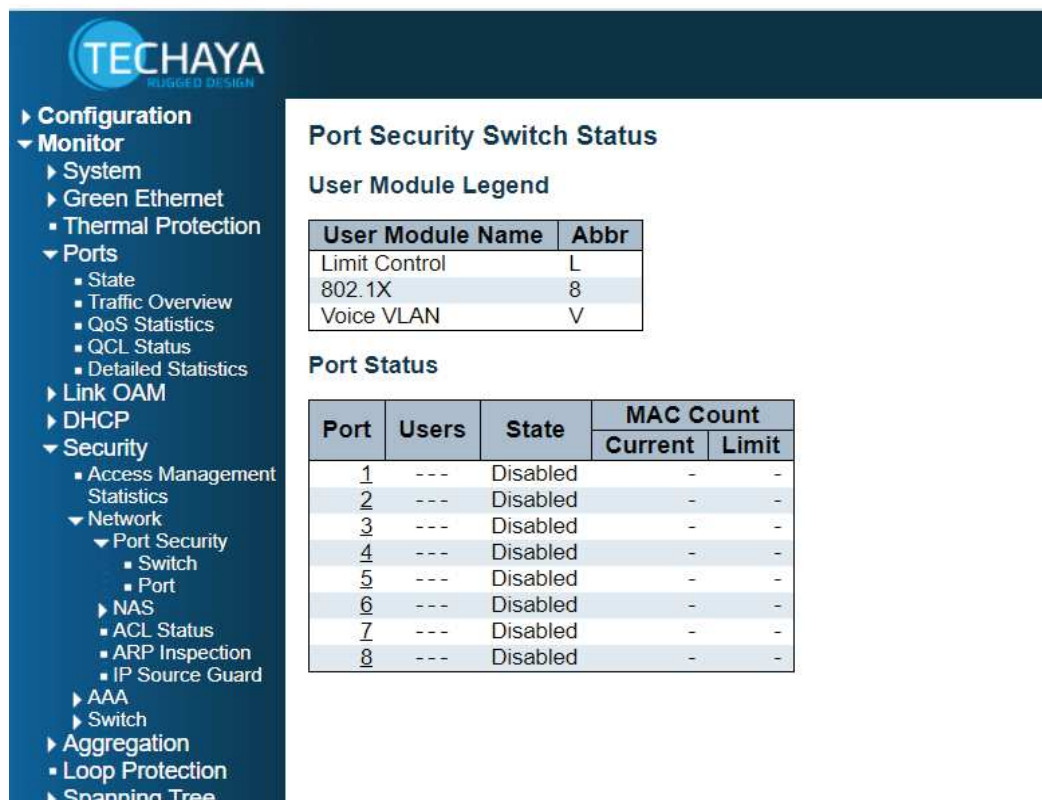
Clear: Click to clear the counters for all ports

5.23 Security – Network – Port Security – Switch

This page shows the Port Security status.

Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.



TECHAYA
RUGGED DESIGN

- Configuration
- ▼ Monitor
 - System
 - Green Ethernet
 - Thermal Protection
 - ▼ Ports
 - State
 - Traffic Overview
 - QoS Statistics
 - QCL Status
 - Detailed Statistics
 - Link OAM
 - DHCP
 - ▼ Security
 - Access Management Statistics
 - ▼ Network
 - ▼ Port Security
 - Switch
 - Port
 - NAS
 - ACL Status
 - ARP Inspection
 - IP Source Guard
 - AAA
 - Switch
 - Aggregation
 - Loop Protection
 - Spanning Tree

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	-	-

5.23.1 Port Security-Switch Status

5.23.1.1 User Module Legend

The legend shows all user modules that may request Port Security services.

User Module Name

This column displays the full name of a module that may request Port Security services.

Abbr

This column displays a one-letter abbreviation of the user module. This is used in the Users column in the port status table.

5.23.1.2 Port Status

The table has one row for each port on the switch and a number of columns:

Port

This column displays the port number for which the status applies. Click the Port number to see the status for this particular port.

Users

This column displays Port Security status (enabled/disabled).

Each of the user modules has a column that shows whether that module has enabled Port Security or not.

A dash ("-") means that the corresponding user module is not enabled.

A letter indicates that the user module abbreviated by that letter (see Abbr above) has enabled port security.

State

Shows the current state of the port. It can take one of four values:

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 Web-page.

MAC Count

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, a dash ("-") will be shown. If the Limit Control user module is not enabled on the port, the Limit column will show a dash ("-").

5.23.2 Access Management Statistics Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.24 Security – Network – Port Security – Port

This page shows the MAC addresses secured by the Port Security module.

Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

5.24.1 Port Security Port Status Port n

TECHAYA

Configuration

Monitor

System

Green Ethernet

Thermal Protection

Ports

State

Traffic Overview

QoS Statistics

QCL Status

Detailed Statistics

Link OAM

DHCP

Security

Access Management

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				

MAC Address and VLAN ID

These columns display the MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

State

This column displays the state of the corresponding MAC address: whether it is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition

This column displays the date and time when this MAC address was added to 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 still forwards 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.

5.24.2 Port Security Port Status Buttons

Port select box: 

The port select box determines which port's status to display. Select a port from the drop-down list.

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.25 Security – Network – NAS – Switch

This page provides an overview of the current NAS port states.

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	-	-	-	-

5.25.1 Network Access Server Switch Status

Port

This column displays the port number for which the status applies. Click the Port number to navigate to detailed NAS statistics for this port (described in section 5.24 Security – Network – NAS – Port).

Admin State

This column displays the port's current administrative state. Refer to NAS **שגיאה! מקור ההפניה לא נמצא.** in section **שגיאה! מקור ההפניה לא נמצא.** for a description of possible values.

Port State

This column displays the current state of the port. Refer to NAS **שגיאה! מקור ההפניה לא נמצא.** for a description of the individual states.

Last Source

This column displays the source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID

This column displays the user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class

QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID

The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs [here](#).

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs [here](#).

5.25.2 Network Access Server Switch Status Buttons**Auto-refresh:**

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.26 Security – Network – NAS – Port

This page shows the MAC addresses secured by the Port Security module.

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only.

Use the port select box to select which port details to be displayed.

5.26.1 NAS Statistics Port n

5.26.1.1 Port State

Admin State

This column displays the port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State

This column displays the current state of the port. Refer to NAS Port State for a description of the individual states.

QoS Class

The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID

The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

5.26.2 Port Counters

EAPOL Counters

These supplicant frame counters are available for the following administrative states:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

EAPOL Counters			
Direction	Name	IEEE Name	Description
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

Backend Server Counters

These backend (RADIUS) frame counters are available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Backend Server Counters			
Direction	Name	IEEE Name	Description
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	802.1X-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	802.1X-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. MAC-based: Not applicable.
Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	802.1X- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Rx	Auth. Failures	dot1xAuthBackendAuthFails	802.1X- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Tx	Responses	dot1xAuthBackendResponses	802.1X-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

Last Supplicant/Client Info

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Last Supplicant/Client Info		
Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	802.1X-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.
Identity	-	802.1X-based: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable.

5.26.1 Selected Counters

The Selected Counters table is visible when the port is in one of the following administrative states:

- Multi 802.1X
- MAC-based Auth.

The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

5.26.2 Attached MAC Addresses

Identity

Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.

This column is not available for MAC-based Auth.

MAC Address

For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

VLAN ID

This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

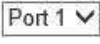
State

The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

Last Authentication

Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

5.26.3 NAS Port Buttons

Port select box: 

The port select box determines which port's details to display. Select a port from the drop-down list.

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

Clear: This button is available in the following modes:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Click to clear the counters for the selected port.

Clear All: This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.

Clear This: This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

5.27 Security – Network – ACL Status

This page shows the Access Control List (ACL) status by different ACL users. Each row describes the Access Control Entry (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.

5.27.1 ACL Status

The following ACL Status details are displayed:

User

This column shows the ACL user.

ACE

Indicates the ACE ID on local switch.

Frame Type

This column shows 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.
- 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

This column shows the forwarding action of the ACE. Possible values are:

- Permit:** Frames matching the ACE may be forwarded and learned
- Deny:** Frames matching the ACE are dropped

Filter: Frames matching the ACE are filtered

Rate Limiter

This column shows the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Mirror

This column shows 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.

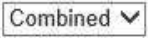
Counter

This column shows the number of times the ACE was hit by a frame.

Conflict

This column shows the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

5.27.2 ACL Status Buttons

Select Box : The select box determines which ACL user is affected by clicking the buttons. Select a user from the drop down list:

Combined

Static

IPMC

Loop Protect

Conflict

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

5.28 Security – ARP Inspection

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.

The screenshot shows the TECHAYA web interface. On the left is a sidebar with a tree view containing 'Configuration' and 'Monitor'. Under 'Monitor', there are sub-items: 'System', 'Green Ethernet', 'Thermal Protection', 'Ports' (with sub-items 'State', 'Traffic Overview', 'QoS Statistics', 'QCL Status', 'Detailed Statistics'), 'Link OAM', 'DHCP', 'Security' (with sub-items 'Access Management', 'Statistics', 'Network'), and 'Network'. The main content area is titled 'Dynamic ARP Inspection Table'. It features search filters: 'Start from' (Port 1), 'VLAN' (1), 'MAC address' (00-00-00-00-00-00), and 'IP address' (0.0.0.0), followed by a 'with 20 entries per page.' field. Below these filters is a table with headers 'Port', 'VLAN ID', 'MAC Address', and 'IP Address'. The table body contains the text 'No more entries'. To the right of the table are buttons for 'Auto-refresh', 'Refresh', '<<', and '>>'.

5.28.1 Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

5.28.2 ARP Inspection Table Columns

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the ARP traffic is permitted.

MAC Address

User MAC address of the entry.

IP Address

User IP address of the entry.

5.28.3 ARP Inspection Table Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

Clear: Flushes all dynamic entries.

|<<: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

5.29 Security – IP Source Guard

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

The screenshot shows the TECHAYA web interface. On the left is a sidebar menu with categories: Configuration, Monitor, System, Green Ethernet, Thermal Protection, Ports, Link OAM, DHCP, Security, Access Management, and Network. The 'Security' section is expanded, showing 'Access Management' and 'Network'. Under 'Network', 'Port Security' is selected, showing 'NAS', 'ACL Status', 'ARP Inspection', and 'IP Source Guard'. The main content area is titled 'Dynamic IP Source Guard Table'. It has search filters: 'Start from' (Port 1), 'VLAN' (1), and 'IP address' (0.0.0.0), with a 'with 20 entries per page' option. There are buttons for 'Auto-refresh', 'Refresh', '<<', and '>>'. Below the filters is a table with columns: Port, VLAN ID, IP Address, and MAC Address. The table currently displays 'No more entries'.

5.29.1 Navigating the IP Source Guard Table

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

5.29.2 IP Source Guard Table Columns

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the IP traffic is permitted.

MAC Address

Source MAC address.

IP Address

User IP address of the entry.

5.29.3 IP Source Guard Table Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

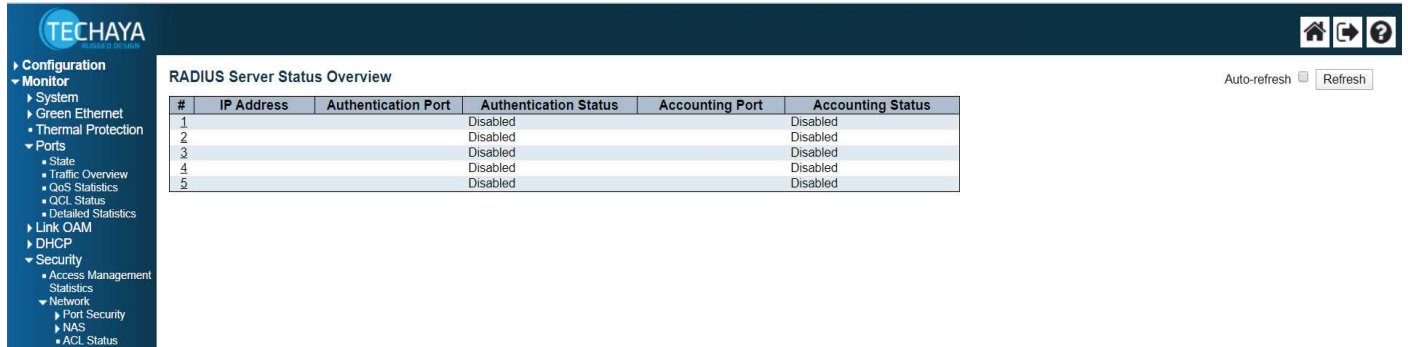
Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

5.30 Security – AAA – RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.



TECHAYA

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

Auto-refresh ☐ Refresh

5.30.1 RADIUS Authentication Server Status Overview

#

This column displays the RADIUS server number. Click the RADIUS server number to navigate to detailed statistics for this server.

IP Address

This column displays the IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Authentication Port

UDP port number for authentication.

Authentication Status

This column displays the current status of the server. This field takes one of the following values:

Disabled: The 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.

5.30.2 RADIUS Authentication Server Status Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.31 Security – AAA – RADIUS Details

This page provides detailed statistics for a particular RADIUS server.

5.31.1 RADIUS Authentication Statistics for Server n

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

The screenshot displays the Techaya web interface. On the left is a navigation menu with categories like Configuration, Monitor, System, Green Ethernet, Thermal Protection, Ports, State, Traffic Overview, QoS Statistics, QCL Status, Detailed Statistics, Link OAM, DHCP, Security, Access Management, Network, Port Security, NAS, ACL Status, ARP Inspection, IP Source Guard, AAA, RADIUS Overview, RADIUS Details, Switch, Aggregation, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, Ethernet Services, PTP, MAC Table, VLANs, sFlow, and UDLD. The main content area is titled 'RADIUS Authentication Statistics for Server #1'. It includes a dropdown for 'Server #1', an 'Auto-refresh' checkbox, and 'Refresh' and 'Clear' buttons. The statistics are presented in two tables: 'Receive Packets' and 'Transmit Packets'. The 'Receive Packets' table shows Access Accepts, Access Rejects, Access Challenges, Malformed Access Responses, Bad Authenticators, Unknown Types, and Packets Dropped, all with a value of 0. The 'Transmit Packets' table shows Access Requests, Access Retransmissions, Pending Requests, and Timeouts, all with a value of 0. Below these is an 'Other Info' section showing IP Address, State (Disabled), and Round-Trip Time (0 ms). A second section, 'RADIUS Accounting Statistics for Server #1', follows a similar format with Receive and Transmit packets for Responses, Malformed Responses, Bad Authenticators, Unknown Types, and Packets Dropped, all at 0, and an 'Other Info' section with IP Address, State (Disabled), and Round-Trip Time (0 ms).

5.31.1.1 Receive Packets (Rx)

Name	Description
Access Accepts	Displays the number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Access Rejects	Displays the number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Access Challenges	Displays the number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Malformed Access Responses	Displays the number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. The following are not included as malformed access responses: Bad authenticators or Message Authenticator attributes or unknown types.

Name	Description
Bad Authenticators	Displays the number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Unknown Types	Displays 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

5.31.1.2 Transmit Packets (Tx)

Name	Description
Access Requests	Displays the number of RADIUS Access-Request packets sent to the RADIUS authentication server. This does not include retransmissions.
Access Retransmissions	Displays the number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Pending Requests	Displays 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	Displays 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.

5.31.1.3 Other Info

IP Address

This field displays the IP address and UDP port for the authentication server in question.

State

This field displays 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

This field displays 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 has not been a round-trip communication with the server yet.

5.31.2 RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

5.31.2.1 Receive Packets (Rx)

Name	Description
Responses	Displays the number of RADIUS packets (valid or invalid) received from the server.
Malformed Responses	Displays the number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length.
Bad Authenticators	Displays the number of RADIUS Access-Response packets containing invalid authenticators received from the server.
Unknown Types	Displays the number of RADIUS packets that were received with unknown types from the server on the authentication port.
Packets Dropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

5.31.2.2 Transmit Packets (Tx)

Name	Description
Requests	Displays the number of RADIUS packets sent to the server. This does not include retransmissions.
Retransmissions	Displays the number of RADIUS packets retransmitted to the RADIUS authentication server.

Name	Description
Pending Requests	Displays 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	Displays 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.

5.31.2.3 Other Info

IP Address

This field displays the IP address and UDP port for the accounting server in question.

State

This field displays 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

This field displays 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 has not been a round-trip communication with the server yet.

5.31.3 RADIUS Details Buttons

Server select box:

The server select box determines which server is affected by clicking the buttons.

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear the counters for the selected server. The “Pending Requests” counter will not be cleared by this operation.

5.32 Security – Switch – RMON - Statistics

5.32.1 RMON Statistics Configuration

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the "**Refresh**" button will update the displayed table starting from that or the next closest Statistics table match.

The ">>" will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

ID	Data Source (IfIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~	128 ~	256 ~	512 ~	1024 ~
														127	255	511	1023	1588

No more entries

The displayed counters are:

ID

Indicates the index of the entry. The range is from 1 to 65535.

Data Source

The port ID which wants to be monitored.

Drop

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broad-cast

The total number of good packets received that were directed to the broadcast address.

Multi-cast

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, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Over-size

The total number of packets received that were less 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

The total number of packets (including bad packets) received that were 64 octets in length.

65~127

The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

128~255

The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

256~511

The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512~1023

The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

1024~1588

The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

5.32.2 RMON Statistics Configuration Buttons**Auto-refresh:**

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

5.33 Security – Switch – RMON – History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the "**Refresh**" button will update the displayed table starting from that or the next closest History table match.

The ">>" will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

5.33.1 RMON History Overview

TECHAYA

Configuration
Monitor
System
Green Ethernet
Thermal Protection
Ports
Link OAM
DHCP
Security
Access Management
Statistics
Network
Port Security
NAS
ACL Status
ARP Inspection
IP Source Guard

RMON History Overview

Auto-refresh ☐ Refresh << >>

Start from Control Index 0 and Sample Index 0 with 20 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														

The displayed fields are:

History Index

Indicates the index of History control entry.

Sample Index

Indicates the index of the data entry associated with the control entry.

Sample Start

The value of sysUpTime at the start of the interval over which this sample was measured.

Drop

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast 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.

CRCErrors

The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Undersize

The total number of packets received that were less than 64 octets.

Oversize

The total number of packets received that were longer than 1518 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.

5.33.2 RMON History Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

- |<<: Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index.
- >>: Updates the table, starting with the entry after the last entry currently displayed.

5.34 Security – Switch – RMON – Alarm

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the "**Refresh**" button will update the displayed table starting from that or the next closest Alarm table match.

The ">>" will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

5.34.1 Alarm Overview

The displayed fields are:

ID

Indicates the index of Alarm control entry.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable

Indicates the particular variable 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 sent when this entry is first set to valid.

Rising Threshold

Rising threshold value.

Rising Index

Rising event index.

Falling Threshold

Falling threshold value.

Falling Index

Falling event index.

5.34.2 RMON Alarm Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

5.35 Security – Switch – RMON – Event

This page provides an overview of RMON Event entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest ID found in the Event table.

The "Start from Control Index" allows the user to select the starting point in the Event table. Clicking the "**Refresh**" button will update the displayed table starting from that or the next closest Event table match.

The ">>" will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

5.35.1 Event Overview

The displayed fields are:

Event Index

Indicates the index of the event entry.

Log Index

Indicates the index of the log entry.

LogTime

Indicates Event log time.

LogDescription

Indicates the Event description.

5.35.2 RMON Event Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.

>>: Updates the table, starting with the entry after the last entry currently displayed.

5.36 Aggregation – Static

This page is used to see the status of ports in Aggregation group.

The screenshot shows the TECHAYA Web Interface. On the left is a dark blue sidebar with a navigation menu. The main content area has a title 'Aggregation Status' and a table with the following columns: Aggr ID, Name, Type, Speed, Configured Ports, and Aggregated Ports. The table is currently empty, displaying the text 'No aggregation groups'. Above the table, there are two buttons: 'Auto-refresh' (with a checkbox) and 'Refresh'.

5.36.1 Aggregation Group Status

Aggr ID

The Aggregation ID associated with this aggregation instance.

Name.

Name

Name of the Aggregation group ID.

Type

Type of the Aggregation group (Static or LACP).

Speed

Speed of the Aggregation group.

Configured ports

Configured member ports of the Aggregation group.

Aggregated ports

Aggregated member ports of the Aggregation group.

5.36.2 Aggregation Status Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

5.37 Aggregation – LACP – System Status

This page provides a status overview for all LACP instances.

TECHAYA

Configuration

Monitor

System

Green Ethernet

Thermal Protection

Ports

State

Traffic Overview

QoS Statistics

QCL Status

Detailed Statistics

Link OAM

DHCP

Security

Aggregation

Static

LACP

System Status

Port Status

Port Statistics

Loop Protection

Spanning Tree

MVR

LACP System Status

Auto-refresh ☐ Refresh

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

5.37.1 LACP System Status

Aggr ID

This column displays the Aggregation ID associated with this aggregation instance. For LLAG the id is shown as “isid:aggr-id” and for GLAGs as “aggr-id”.

Partner System ID

This column displays the system ID (MAC address) of the aggregation partner.

Partner Key

This column displays the Key that the partner has assigned to this aggregation ID.

Partner Prio

This column displays the priority of the partner port.

Last changed

This column displays the time since this aggregation changed.

Local Ports

This column displays the ports that are a part of this aggregation for this switch.

5.37.2 LACP System Status Buttons

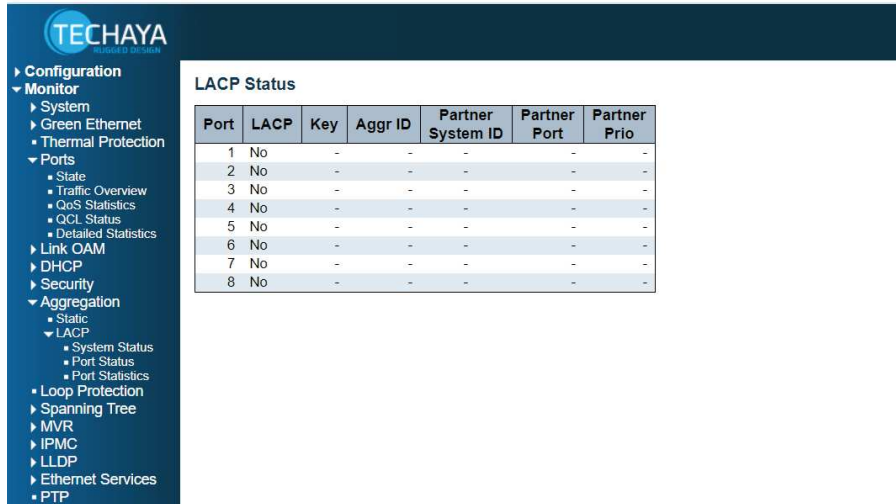
Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.38 LACP – Port Status

This page provides a status overview for LACP for all ports.



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	-	-	-	-	-

5.38.1 LACP Status

Port

This column displays the switch port number for the row of status information.

LACP

This column displays the LACP operational status of the port. It takes one of the following values:

Yes: LACP is enabled and the port link is up

No: LACP is **not** enabled or the port link is down

Backup: The port could not join the aggregation group but will join if other port leaves. Meanwhile its LACP status is disabled.

Key

This column displays the key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID

This column displays the Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.

Partner System ID

This column displays the partner's System ID (MAC address).

Partner Port

This column displays the port number of the partner connected to this port.

Partner Prio

This column displays the partner's port priority.

5.38.2 LACP Status Buttons**Auto-refresh:**

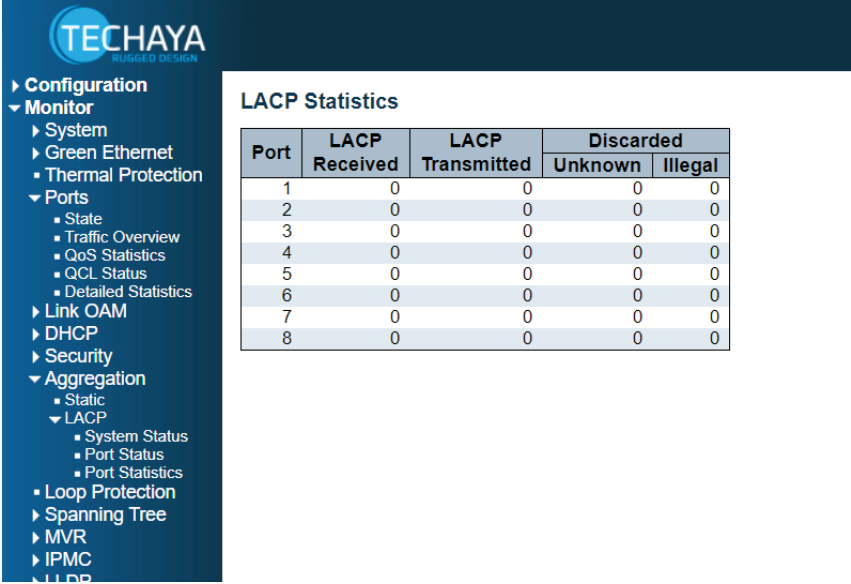
- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.39 LACP – Port Statistics

This page provides an overview for LACP statistics for all ports.

5.39.1 LACP Statistics



TECHAYA
RUGGED DESIGN

Configuration
Monitor
System
Green Ethernet
Thermal Protection
Ports
State
Traffic Overview
QoS Statistics
QCL Status
Detailed Statistics
Link OAM
DHCP
Security
Aggregation
Static
LACP
System Status
Port Status
Port Statistics
Loop Protection
Spanning Tree
MVR
IPMC
LLDP

LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

Port

This column displays the switch port number for the row of statistics.

LACP Received

This column shows how many LACP frames have been received at each port.

LACP Transmitted

This column shows how many LACP frames have been sent from each port.

Discarded

This column shows how many unknown or illegal LACP frames have been discarded at each port.

5.39.2 LACP Statistics Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.40 Loop Protection

This page displays the loop protection port status of the currently switch.

5.40.1 Loop Protection Status

Port

This column displays the switch port number of the logical port.

Action

This column displays the currently configured port action.

Transmit

This column displays the currently configured port transmit mode.

Loops

This column displays the number of loops detected on this port.

Status

This column displays the current loop protection status of the port.

Loop

This column displays whether or not a loop is currently detected on the port.

Time of Last Loop

This column displays the time of the last loop event detected.

5.40.2 LACP Status Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.41 Spanning Tree – Bridge Status

This page provides detailed information on a single STP bridge instance, along with port state for all active ports associated.

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.02-00-C1-93-4A-5F	32768.02-00-C1-93-4A-5F	-	0	Steady	-

Auto-refresh ☐ Refresh

5.41.1 STP Detailed Bridge Status

MSTI

The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID

This field displays the Bridge ID of this Bridge instance.

Root ID

This field displays the Bridge ID of the currently elected root bridge.

Root Port

The switch port currently assigned the root port role.

Root Cost

This field displays the Root Path Costs:

- 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

This field displays the current state of the Topology Change Flag of this Bridge instance.

Topology Change Last

The time since last Topology Change occurred.

5.41.2 STP Bridge Status Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.42 Spanning Tree – Port Status

This page displays the STP CIST port status for physical ports of the currently switch.

STP Port Status

Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	0d 04:58:18
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-

Auto-refresh ☐ Refresh

5.42.1 STP Port Status

Port

This column displays the switch port number of the logical STP port.

CIST Role

This column displays the current STP port role of the CIST port. The port role can be one of the following values:

- AlternatePort
- BackupPort
- RootPort
- DesignatedPort
- Disabled

CIST State

This column displays the current STP port state of the CIST port. The port state can be one of the following values:

- Discarding
- Learning
- Forwarding

Uptime

This column displays the time since the bridge port was last initialized.

5.42.2 STP Port Status Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3

seconds.

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

5.43 Spanning Tree – Port Statistics

This page displays the STP port statistics counters of bridge ports in the currently switch.

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	9307	0	0	0	0	0	0	0	0	0

5.43.1 STP Statistics

Port

This column displays the switch port number of the logical STP port.

5.43.1.1 Transmitted/Received

MSTP

This column displays the number of MSTP BPDUs received/transmitted on the port.

RSTP

This column displays the number of RSTP BPDUs received/transmitted on the port.

STP

This column displays the number of legacy STP Configuration BPDUs received/transmitted on the port.

TCN

This column displays the number of (legacy) Topology Change Notification BPDUs received/transmitted on the port.

5.43.1.2 Discarded

Unknown

This column displays the number of unknown Spanning Tree BPDUs received (and discarded) on the port.

Illegal

This column displays the number of illegal Spanning Tree BPDUs received (and discarded) on the port.

5.43.2 STP Port Status Buttons**Auto-refresh:**

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to reset the counters

5.44 MVR - Statistics

This page provides MVR Statistics information.

TECHAYA Web Interface - Monitor

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
No more entries						

Auto-refresh ☒ Refresh Clear

5.44.1 MVR Statistics Table

VLAN ID

The Multicast VLAN ID.

IGMP/MLD Queries Received

The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted

The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received

The number of Received IGMPv1 Join's.

IGMPv2/MLDv1 Report's Received

The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

IGMPv3/MLDv2 Report's Received

The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.

IGMPv2/MLDv1 Leave's Received

The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

5.44.2 MVR Statistics Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to reset the counters

5.45 MVR - Channels (Groups) Information

Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.

TECHAYA

MVR Channels (Groups) Information

Start from VLAN and Group Address with entries per page.

VLAN ID	Groups	Port Members
1	2	3 4 5 6 7 8

No more entries

Auto-refresh ☐ Refresh |<< >>

5.45.1 Navigating the MVR Channels (Groups) Information Table

Each page shows up to 99 entries from the MVR GroupTable, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the **"Refresh"** button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a **"Refresh"** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

5.45.2 MVR Channels (Groups) Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group ID of the group displayed.

Port Member

Ports under this group.

5.45.3 MVR Channels (Groups) Information Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds.

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

>>: Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.

|<<: Updates the table, starting with the entry after the last entry currently displayed.

5.46 MVR - SFM Information

Entries in the MVR SFM Information Table are shown on this page. The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

5.46.1 Navigating the MVR SFM Information Table

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **Forward Arrows** (">>") will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the **Back Arrows** ("<<") button to start over.

5.46.2 MVR SFM Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

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

IP Address of the source. Currently, the maximum number of IP source address for filtering (per group) is 8. When there is no any source filtering address, the text "None" is shown in the Source Address field.

Type

Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

5.46.3 MVR SFM Information Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds.

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

Back Arrows (>>): Updates the table starting from the first entry in the MVR SFM Information Table.

Forward Arrows (l<<): Updates the table, starting with the entry after the last entry currently displayed.

5.47 IPMC – IGMP Snooping – Status

This page provides Internet Group Management Protocol (IGMP) Snooping status.

TECHAYA Web Interface

Auto-refresh ☐ Refresh Clear

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
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

5.47.1 IGMP Snooping Status

5.47.1.1 Statistics

VLAN ID

This column displays the VLAN ID of the entry.

Querier Version

This column displays the Version of the current Working Querier.

Host Version

This column displays the Version of the current Working Host.

Querier Status

This column displays the Querier status as

- ACTIVE
- IDLE
- DISABLE (denotes the specific interface is administratively disabled)

Queries Transmitted

This column displays the number of Transmitted Queries.

Queries Received

This column displays the number of Received Queries.

V1 Reports Received

This column displays the number of Received V1 Reports.

V2 Reports Received

This column displays the number of Received V2 Reports.

V3 Reports Received

This column displays the number of Received V3 Reports.

V2 Leaves Received

This column displays the number of Received V2 Leaves.

5.47.1.2 Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

This column displays the switch port number.

Status

Indicate whether specific port is a router port or not.

5.47.2 STP Port Status Buttons**Auto-refresh:**

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear all statistics counters

5.48 IPMC – IGMP Snooping – Groups Information

This page provides Internet Group Management Protocol (IGMP) Snooping status. The IGMP Group Table is sorted first by VLAN ID, and then by group.

TECHAYA

Configuration
Monitor
System
Green Ethernet
Thermal Protection
Ports
Link OAM
DHCP
Security
Aggregation
Loop Protection
Spanning Tree
MVR
IPMC
IGMP Snooping
MLD Snooping

IGMP Snooping Group Information

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

VLAN ID	Groups
No more entries	

Auto-refresh Refresh << >>

5.48.1 Navigating the IGMP Group Table

Each page can show up to 99 entries from the IGMP Group table. Set the number of entries per page in the “entries per page” input field (the default is 20). When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The “Start from VLAN”, and “group address” input fields allow the user to set the starting point in the IGMP Group Table. Click the **Refresh** button to update the displayed table starting from the current settings or the closest next IGMP Group Table match. After clicking the **Refresh** button, the two input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **Forward Arrows** button () will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the

Back Arrows button () to start over.

5.48.2 IGMP Snooping Groups Information

VLAN ID

This column displays the VLAN ID of the group.

Groups

This column displays the Group address of the group displayed.

Port Members

This column displays Ports that are members of this group.

5.48.3 STP Port Status Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Back Arrows (): Updates the table, starting with the first entry in the IGMP Group Table.

Forward Arrows (): Updates the table, starting with the entry after the last entry currently displayed.

5.49 IPMC – IGMP Snooping – IPV4 SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

5.49.1 Navigating the SFM Information Table

Each page can show up to 99 entries from the IGMP SFM Information table. Set the number of entries per page in the “entries per page” input field (the default is 20). When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The “Start from VLAN”, and “group address” input fields allow the user to set the starting point in the IGMP SFM Information Table. Click the **Refresh** button to update the displayed table starting from the current settings or the closest next IGMP SFM Information Table match. After clicking the **Refresh** button, the two input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **Forward Arrows** button () will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the

Back Arrows button () to start over.

5.49.2 IGMP SFM Information

VLAN ID

This column displays the VLAN ID of the group.

Groups

This column displays the Group address of the group displayed.

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

IP Address of the source.

Currently, the maximum number of IPv4 source address for filtering (per group) is 8. When there is no source filtering address, the text "None" is shown in the Source Address field.

Type

Indicates the Type. It can be either Allow or Deny.

Type Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

5.49.3 IGMP SFM Information Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Back Arrows (): Updates the table, starting with the first entry in the IGMP SFM Information Table.

Forward Arrows (): Updates the table, starting with the entry after the last entry currently displayed.

5.50 IPMC – MLD Snooping – Status

This page provides Multicast Listener Discovery (MLD) for IPv6 Snooping status.

TECHAYA

MLD Snooping Status

Auto-refresh ☐ Refresh Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
1	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

5.50.1 MLD Snooping Status

5.50.1.1 Statistics

VLAN ID

This column displays the VLAN ID of the entry.

Querier Version

This column displays the Version of the current Working Querier.

Host Version

This column displays the Version of the current Working Host.

Querier Status

This column displays the Querier status as

- ACTIVE
- IDLE
- DISABLE (denotes the specific interface is administratively disabled)

Queries Transmitted

This column displays the number of Transmitted Queries.

Queries Received

This column displays the number of Received Queries.

V1 Reports Received

This column displays the number of Received V1 Reports.

V2 Reports Received

This column displays the number of Received V2 Reports.

V1 Leaves Received

This column displays the number of Received V1 Leaves.

5.50.1.2 Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

This column displays the switch port number.

Status

Indicate whether specific port is a router port or not.

5.50.2 MLD Status Buttons**Auto-refresh:**

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Click to clear all statistics counters

5.51 IPMC – MLD Snooping – Groups Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

TECHAYA

Configuration

Monitor

System

Green Ethernet

Thermal Protection

Ports

State

Traffic Overview

QoS Statistics

QCL Status

Detailed Statistics

Link OAM

DHCP

Security

Aggregation

Loop Protection

Spanning Tree

MVR

IPMC

IGMP Snooping

MLD Snooping

Status

Groups

Information

IPv6 SFM

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

No more entries

5.51.1 Navigating the MLD Group Table

Each page can show up to 99 entries from the MLD Group table. Set the number of entries per page in the “entries per page” input field (the default is 20). When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The “Start from VLAN”, and “group address” input fields allow the user to set the starting point in the MLD Group Table. Click the **Refresh** button to update the displayed table starting from the current settings or the closest next MLD Group Table match. After clicking the **Refresh** button, the two input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **Forward Arrows** button () will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the

Back Arrows button () to start over.

5.51.2 MLD Group Table Columns

VLAN ID

This column displays the VLAN ID of the group.

Groups

This column displays the Group address of the group displayed.

Port Members

This column displays Ports that are members of this group.

5.51.3 MLD Group Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Back Arrows (): Updates the table, starting with the first entry in the MLD Group Table.

Forward Arrows (): Updates the table, starting with the entry after the last entry currently displayed.

5.52 IPMC – MLD Snooping – IPV6 SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

5.52.1 Navigating the MLD SFM Information Table

Each page can show up to 99 entries from the MLD SFM Information table. Set the number of entries per page in the “entries per page” input field (the default is 20). When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The “Start from VLAN”, and “group address” input fields allow the user to set the starting point in the MLD SFM Information Table. Click the **Refresh** button to update the displayed table starting from the current settings or the closest next MLD SFM Information Table match. After clicking the **Refresh** button, the two input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **Forward Arrows** button () will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the

Back Arrows button () to start over.

5.52.2 MLD SFM Information

VLAN ID

This column displays the VLAN ID of the group.

Group

This column displays the Group address of the group displayed.

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

IP Address of the source.

Currently, the maximum number of IPv4 source address for filtering (per group) is 8. When there is no source filtering address, the text "None" is shown in the Source Address field.

Type

Indicates the Type. It can be either Allow or Deny.

Type Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

5.52.3 MLD SFM Information Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

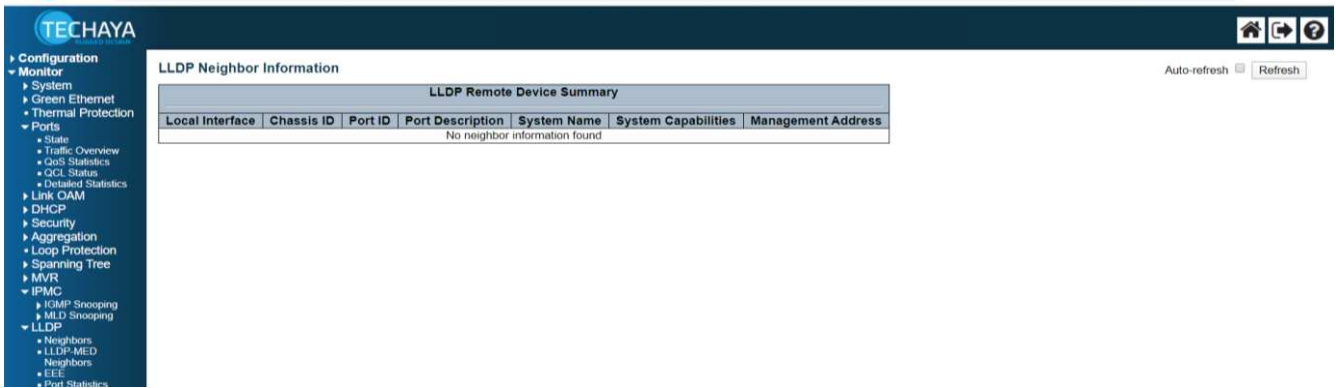
Refresh: Click to refresh the page immediately

Back Arrows (): Updates the table, starting with the first entry in the MLD SFM Information Table.

Forward Arrows (): Updates the table, starting with the entry after the last entry currently displayed.

5.53 LLDP – Neighbors

This page provides a status overview for all Link Layer Discovery Protocol (LLDP) neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected.



LLDP Remote Device Summary						
Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbor information found						

5.53.1 LLDP Neighbor Information

5.53.1.1 LLDP Remote Device Summary

Local Interface

This column displays the port on which the LLDP frame was received.

Chassis ID

This column displays the Chassis ID (Identification) of the neighbor's LLDP frames.

Port ID

This column displays the Port ID of the neighbor port.

Port Description

This column displays the Port Description advertised by the neighbor unit.

System Name

This column displays the System Name advertised by the neighbor unit.

System Capabilities

This column displays the System Capabilities of the neighbor unit. The possible capabilities are:

- Other
- Repeater
- Bridge
- WLAN Access Point

- Router
- Telephone
- DOCSIS cable device
- Station only
- Reserved

When a capability is enabled, it is followed by (+). If the capability is disabled, it is followed by (-).

Management Address

This column displays the Management Address of the neighbor unit used for higher layer entities to assist discovery by the network management. For example, this might hold the neighbor's IP address.

5.53.2 LLDP Neighbor Information Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.54 LLDP – MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each interface on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.



5.54.1 LLDP Media Neighbor Information

Interface

This column displays the interface on which the LLDP frame was received.

Device Type

This column displays the Chassis ID (Identification) of the neighbor's LLDP frames.

LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication

appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

LLDP-MED Capabilities

LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved

Application Type

Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

1. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. **Voice Signalling** - for use in network topologies that require a different policy for the voice signalling than for the voice media.
3. **Guest Voice** - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. **Guest Voice Signalling** - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.
5. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops.
6. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

8. **Video Signaling** - for use in network topologies that require a separate policy for the video signaling than for the video media.

Policy

Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined (known).

TAG

TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: The device is using the IEEE 802.1Q tagged frame format.

VLAN ID

VLAN ID is the VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress interface is used instead.

Priority

Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

Auto-negotiation

Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

Auto-negotiation status

Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

Auto-negotiation Capabilities

Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

5.54.2 LLDP MED Neighbor Information Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.55 LLDP – EEE

By using Energy Efficient Ethernet (EEE) power savings can be achieved at the expense of traffic latency. This latency results from the time required to boot up circuits that were turned off by EEE to save power. This time is called “wake up time”.

To achieve minimal latency, devices can use Link Layer Discovery Protocol (LLDP) to exchange information about their respective Tx and Rx “wake up time”, as a way to agree upon the minimum wake up time they need.

This page provides an overview of EEE information exchanged by LLDP.

5.55.1 LLDP Neighbors EEE Information

The displayed table contains a row for each port. If the interface does not support EEE, then it displays as "EEE not supported for this interface".

If EEE is not enabled on particular interface, then it displays as "EEE not enabled for this interface".

If the link partner doesn't supports EEE, then it displays as "Link partner is not EEE capable. The columns display the following information:

Local Port

This column displays the port on which LLDP frames are received or transmitted.

Tx Tw

This column displays the maximum time that link partner's transmit path can hold-off sending data after de-assertion of LPI.

Rx Tw

This column displays the time that link partner's receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.

Fallback Receive Tw

This column displays the link partner's fallback receive Tw.

A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default to the same value as that of the Receive Tw_sys_tx.

Echo Tx Tw

This column displays the link partner's Echo Tx Tw value.

The respective echo values shall be defined as the local link partner's reflection (echo) of the remote link partner's respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered, and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

Echo Rx Tw

This column displays the link partner's Echo Rx Tw value.

Resolved Tx Tw

This column displays the Resolved Tx Tw for this link.

Note: NOT the link partner

The Resolved Tx Tw value is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw

This column displays the Resolved Rx Tw for this link.

Note: NOT the link partner

The Resolved Rx Tw value is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

EEE in Sync

This column displays whether the switch and the link partner have agreed on wake times:

Red: Switch and link partner have **not** agreed on wakeup times

Green: Switch and link partner have agreed on wakeup times

5.55.2 EEE Neighbor Information Buttons

Auto-refresh:



Enable Auto-refresh – to refresh the page automatically every 3

seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.56 LLDP – Port Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to per port counters for the currently selected switch.

- Configuration
- Monitor
 - System
 - Green Ethernet
 - Thermal Protection
 - Ports
 - State
 - Traffic Overview
 - QoS Statistics
 - QCL Status
 - Detailed Statistics
 - Link OAM
 - DHCP
 - Security
 - Aggregation
 - Loop Protection
 - Spanning Tree
 - MVR
 - IPMC
 - IGMP Snooping
 - MLD Snooping
 - LLDP
 - Neighbors
 - LLDP-MED
 - Neighbors
 - EEE
 - Port Statistics
 - Ethernet Services
 - PTP
 - MAC Table
 - VLANs
 - sFlow
 - UDLD
- Diagnostics
- Maintenance

LLDP Global Counters

☐ Auto-refresh

Global Counters	
Clear global counters	☒
Neighbor entries were last changed	1970-01-01T00:00:00+00:00 (10906 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

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	365	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	☒

5.56.1 LLDP Global Counters

Clear global counters

If checked the global counters are cleared when "Clear" is pressed.

Neighbor entries were last changed

This column displays the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added

This column displays the number of new entries added since switch reboot.

Total Neighbors Entries Deleted

This column displays the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped

This column displays the number of LLDP frames dropped due to the entry table being full.

Total Neighbors Entries Aged Out

This column displays the the number of entries deleted due to Time-To-Live expiring.

5.56.2 LLDP Statistics Local Counters**Local Interface**

This column displays the interface on which LLDP frames are received or transmitted.

Tx Frames

This column displays the number of LLDP frames transmitted on the port.

Rx Frames

This column displays the number of LLDP frames received on the port.

Rx Errors

This column displays the number of received LLDP frames containing some kind of error.

Frames Discarded

This column displays the number of LLDP frames discarded.

If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded

This column displays the number of TLVs discarded.

Each LLDP frame can contain multiple pieces of information, known as TLVs (Type Length Value). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized

This column displays the number of TLVs unrecognized.

This is the number of well-formed TLVs that have an unknown type value.

Org. Discarded

This column displays the number of Organizational TLVs unrecognized.

If an LLDP frame is received with an Organizational TLV, but the TLV is not supported the TLV is discarded and counted.

Age-Outs

This column displays the number of 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.

5.56.3 LLDP Statistics Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Clears the counters which have the corresponding checkbox checked.

5.57 Ethernet Services – EVC Statistics

This page provides NNI port traffic statistics for the selected EVC. It also shows counters for UNI ports of ECEs mapping to the EVC. And the MPLS Pseudo-Wires counters are included when the PW ID is attached to the selected EVC.

Class	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
	Rx	Tx	Rx	Tx	Rx	Green	Yellow
0	2831	0	0	0	0	0	0
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	7305	0	0	0	0	0

5.57.1 EVC Statistics

Class

The traffic class for the EVC.

Rx Green

The number of greens received.

Tx Green

The number of green transmitted.

Rx Yellow

The number of yellow received.

Tx Yellow

The number of yellow transmitted.

Rx Red

The number of reds received.

Green Discarded

The number of discarded in the green color.

Yellow Discarded

The number of discarded in the yellow color.

5.57.2 EVC Statistics Buttons

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Clear: Clears the counters for selected ports.

5.58 PTP

This page allows the user to inspect the current PTP (Precision Time Protocol) clock settings.

The screenshot shows the TECHAYA web interface. On the left is a navigation menu with categories like Configuration, Monitor, System, Green Ethernet, Thermal Protection, Ports, Link OAM, DHCP, Security, Aggregation, MVR, IPMC, LLDP, and Ethernet Services. The main content area is titled 'PTP External Clock Mode' and contains two tables. The first table, 'PTP External Clock Mode', has four rows: 'One_PPS_Mode' (Disable), 'External Enable' (False), 'Adjust Method' (LTC frequency), and 'Clock Frequency' (1). The second table, 'PTP Clock Configuration', has two columns: 'Inst' and 'Device Type'. Below this table is a message: 'No Clock Instances Present'. In the top right corner, there are icons for home, back, and help, along with an 'Auto-refresh' checkbox and a 'Refresh' button.

One_PPS_Mode	Disable
External Enable	False
Adjust Method	LTC frequency
Clock Frequency	1

Inst	Device Type	Port List
1	2	3 4 5 6 7 8

No Clock Instances Present

5.58.1 PTP External Clock Description

One_PPS_Mode

Shows the current One_pps_mode configured.

1. Output : Enable the 1 pps clock output
2. Input : Enable the 1 pps clock input
3. Disable : Disable the 1 pps clock in/out-put.

External Enable

Shows the current External clock output configuration.

1. True : Enable the external clock output
2. False : Disable the external clock output.

Adjust Method

Shows the current Frequency adjustment configuration.

1. LTC frequency : Local Time Counter (LTC) frequency control
2. SyncE-DPLL : SyncE DPLL frequency control, if allowed by SyncE
3. Oscillator : Oscillator independent of SyncE for frequency control, if supported by the HW
4. LTC phase : Local Time Counter (LTC) phase control (assumes that the frequency is locked by means of SyncE).

Clock Frequency

Shows the current clock frequency used by the External Clock.

The possible range of values are 1 - 25000000 (1 - 25MHz).

5.58.2 PTP Clock Description

Inst

Indicates the Instance of a particular Clock Instance [0..3].

Click on the Clock Instance number to monitor the Clock details.

ClkDom

Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].

Device Type

Indicates the Type of the Clock Instance. There are five Device Types.

1. Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.
2. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.
3. E2e Transp - Clock's Device Type is End to End Transparent Clock.
4. Master Only - Clock's Device Type is Master Only.
5. Slave Only - Clock's Device Type is Slave Only.

Port List

Shows the ports configured for that Clock Instance.

5.58.3 PTP Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.59 MAC Table

This page displays the entries in the MAC Table. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID , then by MAC address.

TECHAYA

MAC Address Table

Start from VLAN and MAC address with entries per page.

Auto-refresh ☐ Refresh Clear << >>

Type	VLAN	MAC Address	Port Members								
			CPU	1	2	3	4	5	6	7	8
Static	1	02-00-C1-93-4A-5F	✓								
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-93-4A-5F	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	80-CE-62-4F-52-FF	✓								
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓

5.59.1 Navigating the MAC Table

Each page can show up to 999 entries from the MAC table. Set the number of entries per page in the “entries per page” input field (the default is 20). When first visited, the web page will show the first 20 entries from the beginning of the MAC Table.

The “Start from VLAN”, and “MAC address” input fields allow the user to set the starting point in the MAC Table. Click the **Refresh** button to update the displayed table starting from the current settings or the closest next MAC Table match. After clicking the **Refresh** button, the two input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **Forward Arrows** button () will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the **Back Arrows** button () to start over.

5.59.2 MAC Address Table

Type

This column displays the entry type:

- Static
- Dynamic

VLAN

This column displays the VLAN ID of the entry.

MAC address

This column displays the MAC address of the entry.

Port Members

This column displays the ports that are members of the entry.



Port is a member of the entry



Port is **not** a member of the entry

5.59.3 MAC Address Table Buttons

Auto-refresh:

Enable Auto-refresh – to refresh the page automatically every 3 seconds



Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the displayed table starting from the “Start from MAC address” and “VLAN” input fields.

Back Arrows (): Updates the table, starting from the first entry in the MAC Table (i.e. the entry with the lowest VLAN ID and MAC address).

Forward Arrows (): Updates the table, starting with the entry after the last entry currently displayed.

5.60 VLANs – Membership

This page provides an overview of membership status of VLAN users.

TECHAYA

VLAN Membership Status for Combined users

Start from VLAN 1 with 20 entries per page. |<< >>|

VLAN ID	Port Members							
	1	2	3	4	5	6	7	8
1	✓	✓	✓	✓	✓	✓	✓	✓

Combined Auto-refresh Refresh

5.60.1 Navigating the VLAN Membership Status Page

Each page can show up to 99 entries from the VLAN table. Set the number of entries per page in the “entries per page” input field (the default is 20). When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first entry displayed will be the one with the lowest VLAN ID found in the VLAN Table.

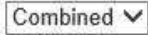
The “VLAN” input field allows the user to set the starting point in the VLAN Table. Click the **Refresh** button to update the displayed table starting from the current setting or the closest next VLAN Table match.

The **Forward Arrows** button () will use the last entry of the currently displayed VLAN Table as a basis for the next lookup. When the end is reached the text “No data exists for the selected user” is shown in the table. Use the

Back Arrows button () to start over.

VLAN User

Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

The drop-down list  on the top of the page allows the user to select the type of VLAN membership to display. The type of VLAN membership is determined by how it was configured; administrator or one of the internal software modules. The current options are:

- Combined
- Admin
- NAS

The “Combined” entry will show a combination of the administrator and internal software modules configuration. It reflects what is actually configured in the hardware.

5.60.2 VLAN Membership for ____ user(s)

The following VLAN Membership details are displayed:

VLAN ID

This column displays the VLAN ID for which the Port members are displayed.

Port Members

This column displays a row of check boxes for – one for each port is displayed for each VLAN ID:



Indicates that the port is included in the VLAN

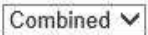


Indicates that the port is in the forbidden port list



Indicates that the port is in the forbidden port list, but attempted to be included in the VLAN. The port will not be a member of the VLAN in this case.

5.60.3 VLAN Membership Status Buttons

Select Box : Select a VLAN user from the drop down list:

Combined

Admin

NAS

Auto-refresh:



Enable Auto-refresh – to refresh the page automatically every 3 seconds



Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

Back Arrows (): Updates the table, starting from the first entry in the MAC Table (i.e. the entry with the lowest VLAN ID and MAC address).

Forward Arrows (): Updates the table, starting with the entry after the last entry currently displayed.

5.61 VLANs – Ports

This page provides VLAN Port Status.

VLAN Port Status for Combined users

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

5.61.1 VLAN Port Status for ____ user(s)

The following VLAN Port Status details are displayed:

VLAN User

Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

The drop-down list **Combined** on the top of the page allows the user to select the type of VLAN membership to display. The type of VLAN membership is determined by how it was configured; administrator or one of the internal software modules. The current options are:

- Combined
- Admin
- NAS
- MSTP

The “Combined” entry will show a combination of the administrator and internal software modules configuration. It reflects what is actually configured in the hardware.

If a given software modules has not overridden any of the port settings, the text “No data exists for the selected user” is shown in the table.

Port

This column displays the logical port for the settings contained in the same row.

Port Type

This column displays the Port Type that a given user wants to configure on the port. The values are:

- Unaware
- C-Port
- S-Port
- S-Custom-Port

The field is empty if not overridden by the selected user.

Ingress Filtering

This column displays the whether a given user wants ingress filtering enabled or not:



Ingress Filtering enabled



Ingress Filtering disabled

The field is empty if not overridden by the selected user.

Frame Type

This column displays the acceptable frame types that a given user wants to configure on the port:

- All
- Tagged
- Untagged

The field is empty if not overridden by the selected user.

Port VLAN ID

This column displays the Port VLAN ID (PVID) that a given user wants the port to have.

The field is empty if not overridden by the selected user.

Tx Tag

This column displays the Tx Tag requirements that a given user has on a port. The values are:

- Tag All
- Tag PVID
- Tag UVID
- Untag All
- Untag PVID
- Untag UVID)

The field is empty if not overridden by the selected user.

Untagged VLAN ID

This column displays a VLAN ID. It is the VLAN ID that the user wants to tag or untag on egress, when Tx Tag is overridden by the selected user and is set to Tag or Untag UVID.

The field is empty if not overridden by the selected user.

Conflicts

This column displays the Conflicts status:

Yes: There is a conflict

No: There is **no** conflict

Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.

Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the lowest priority. Other software modules are prioritized according to their position in the drop-down list (the higher in the list, the higher priority).

If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module.

5.61.2 VLAN Port Status Buttons

Select Box : Select a VLAN user from the drop down list:

Combined

Admin

NAS

MSTP

Auto-refresh:

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately

5.62 sFlow

This page shows receiver and per-port sFlow statistics.

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

5.62.1 Receiver Statistics

The following VLAN Port Status details are displayed:

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

The IP address or hostname of the sFlow receiver.

Timeout

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.

5.62.2 Port Statistics

Port

The port number for which the following statistics applies.

Flow Samples

The number of flow samples sent to the sFlow receiver originating from this port.

Counter Samples

The total number of counter samples sent to the sFlow receiver originating from this port.

5.62.3 sFlow Buttons

Auto-refresh:

- ☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds
- ☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

Clear receiver: Clears the sFlow receiver counters.

Clear ports: Clears the per-port counters.

5.63 UDLD

This page displays the UDLD (Uni Directional Link Detection) status of the ports. UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links. Its functionality is to provide mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. RFC 5171 specifies a way at data link layer to detect Uni directional link.

TECHAYA

Detailed UDLD Status for Port 1

UDLD status	
UDLD Admin state	Disable
Device ID(local)	02-00-C1-93-4A-5F
Device Name(local)	M918
Bidirectional State	Indeterminant

Neighbour Status

Port	Device Id	Link Status	Device Name
No Neighbour ports enabled or no existing partners			

Port 1 ▼ Auto-refresh ☐ Refresh

5.63.1 UDLD port 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

Bidirectional State.

5.63.2 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.

5.63.3 UDLD Buttons**Auto-refresh:**

☒ Enable Auto-refresh – to refresh the page automatically every 3 seconds

☐ Disable Auto-refresh (This is the default.)

Refresh: Click to refresh the page immediately.

6 Web Interface - Diagnostics

The Web Interface – Diagnostics section of this manual describes the diagnostic features and screens of the 8MG Ethernet Switch User Interface.

From the Diagnostics section of the Web interface the user can troubleshoot IP connectivity issues and cable diagnostics. See the following sections:

- Ping
- VeriPHY

6.1 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

After you press the **Start** button (), ICMP packets are transmitted, and the sequence number and round trip time are displayed upon receipt of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space (the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING server 10.10.132.20, 56 bytes of data.  
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms  
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms  
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms  
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms  
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms  
Sent 5 packets, received 5 OK, 0 bad
```

DHCP Link OAM MIB Retrieval

This page allows you to retrieve the local or remote OAM MIB variable data on a particular port. Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest. Click on the **Start** button () to retrieve the content. Click on the **New Retrieval** button () to retrieve another content of interest.

Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press the **Start** button (), ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```

PING6 server ff02::2, 56 bytes of data.
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=0ms
Sent 5 packets, received 10 OK, 0 bad

```

You can configure the following properties of the issued ICMP packets.

TECHAYA
RUGGED DESIGN

- Configuration
- ▼ Monitor
 - System
 - Green Ethernet
 - Thermal Protection
 - ▼ Ports
 - State
 - Traffic Overview
 - QoS Statistics
 - QCL Status
 - Detailed Statistics
 - Link OAM
 - DHCP
 - Security
 - Aggregation
 - Loop Protection
 - Spanning Tree

ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

6.1.1 ICMP Ping

The user can configure the following properties of the issued ICMP packets:

IP Address

Set or show the destination IP Address.

Ping Length

Set or show the payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count

Set or show the count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval

Set or show the interval of the ICMP packet. Values range from 0 second to 30 seconds.

Egress Interface (Only for IPv6)

Set or show the VLAN ID (VID) of the specific egress IPv6 interface where the ICMP packet goes.

The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.

When the egress interface is not given, PING6 finds the best match interface for destination.

Do not specify egress interface for loopback address.

Do specify egress interface for link-local or multicast address.

6.1.2

ICMP Ping Buttons

A rectangular button with a light gray background and a thin border, containing the text "Start" in a dark gray font.

Click to start transmitting ICMP packets

A rectangular button with a light gray background and a thin border, containing the text "New Ping" in a dark gray font.

Click to re-start diagnostics with PING

6.2 VeriPHY

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

Press the **Start** button (), to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.

Note:

- VeriPHY is only accurate for cables of length 7 - 140 meters.
- 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.

TECHAYA
Network Design

- ▶ Configuration
- ▼ Monitor
 - ▶ System
 - ▶ Green Ethernet
 - ▶ Thermal Protection
 - ▼ Ports
 - State
 - Traffic Overview
 - QoS Statistics
 - QCL Status
 - Detailed Statistics
 - ▶ Link OAM
 - ▶ DHCP
 - ▶ Security
 - ▶ Aggregation
 - ▶ Loop Protection
 - ▶ Spanning Tree
 - ▶ MVR
 - ▶ IPMC
 - ▶ LLDP
- ▼ Ethernet Services
 - EVC Statistics
 - PTP
 - MAC Table
- ▼ VLANs
 - Membership
 - Ports
 - sFlow
 - UDLD
- ▼ Diagnostics

VeriPHY Cable Diagnostics

Port: ▼

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--

6.2.1 VeriPHY Cable Diagnostics

Port

Set or show the port requesting VeriPHY Cable Diagnostics.

6.2.2 Cable Status Table

Port:

This column displays the port number for the status row

Pair n:

This column displays the status of the cable pair. The possible values are:

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:

This column displays the length (in meters) of the cable pair. The resolution is 3 meters.

6.2.3 VeriPHY Cable Diagnostics Buttons



Click to start VeriPHY Cable Diagnostics

7 Web Interface - Maintenance

The Web Interface – Maintenance section of this manual describes the maintenance features and screens of the CE Services Switch User Interface.

From the Maintenance section of the Web interface the user can restart the device, revert to factory default settings, and update the firmware software that controls the switch. See the following sections:

- Restart Device
- Factory Defaults
- Software – Upload
- Software – Image Select

From the Maintenance section of the Web interface the user may also save multiple configuration files for the device and easily reset the device with the desired configuration file for different performance purposes. These features can be found in the following sections:

- Configuration – Save Startup-Config
- Configuration – Download
- Configuration – Upload
- Configuration – Activate
- Configuration – Delete

7.1 Restart Device

The user can restart the switch from this page.



7.1.1 Restart Device Buttons



Click to restart the device



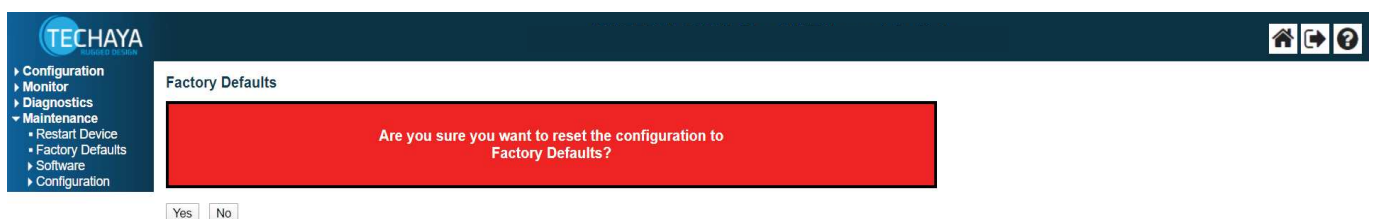
Click to return to the Port State page without restarting the device

7.2 Factory Defaults

The user can reset the configuration of the stack switch from this page. Only the IP configuration is retained.

The new configuration is available immediately, which means that no restart is necessary.

Note: Restoring factory defaults can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, “loopback” packets will be transmitted at port 1. If a “loopback” packet is received at port 2 the switch will do a restore to default.



7.2.1 Factory Defaults Buttons

Click to reset the configuration to Factory Defaults

Click to return to the Port State page without resetting the configuration

7.3 Software – Upload

This page facilitates an update of the firmware controlling the switch.

Browse () to the location of a software image and click the **Upload** button ()

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

Warning: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. **Do not restart or power off the device at this time or the switch may fail to function afterwards.**



7.4 Software – Image Select

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

Note:

- In case the active firmware image is the alternate image, only the “Active Image” table is shown. In this case, the **Activate Alternate Image** button is also disabled.
- If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this image.
- The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

TECHAYA
UNIVERSITY DESIGN

- Configuration
- Monitor
- Diagnostics
- ▼ Maintenance
 - Restart Device
 - Factory Defaults
 - ▼ Software
 - Upload
 - Image Select
- Configuration

Software Image Selection

Active Image	
Image	ce_switch_caracal1_MIL918.dat
Version	MILTECH-918 (standalone) 3.01.1074:1082-3.66-2019-12-13T16:29:43+02:00
Date	2019-12-13T16:29:43+02:00

Alternate Image	
Image	managed.bk
Version	
Date	

7.4.1 Software Image Selection

Image

This field displays the flash index name of the firmware image. The name of primary (preferred) image is “image”, the alternate image is named “image.bk”.

Version

This field displays the version of the firmware image.

Date

This field displays the date when the firmware was produced.

7.4.2 Software Image Selection Buttons

Click to use the alternate image. This button may be disabled depending on system state.



Click to cancel activating the backup image. Navigates away from this page

7.5 Configuration – Save Startup-Config

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

There are three system files:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

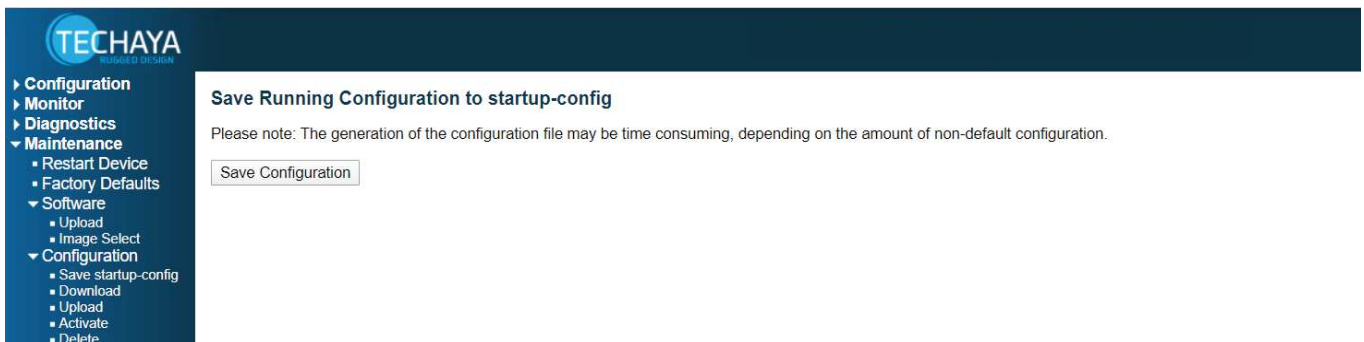
startup-config: The startup configuration for the switch, read at boot time.

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Up to 31 other files, typically used for configuration backups or alternative configurations.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

This page allows the user to copy the running-config to the startup-config and save it, thereby ensuring that the currently active configuration will be used at the next reboot.



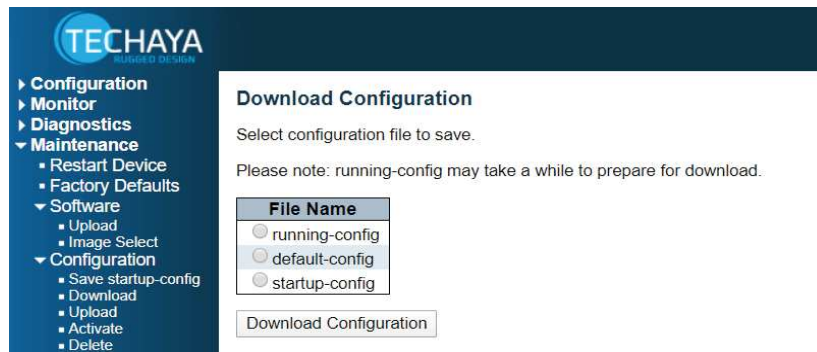
7.5.1 Save Running Configuration to Startup-Config

Click  to copy the running-config to the startup-config and save it.

7.6 Configuration – Download

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

It is possible to download any of the files on the switch to the web browser. This page allows the user to download a file from the switch.



7.6.1 Download Configuration

To download one of the configuration files:

1. Click one of the radio buttons to select the file.
2. Click the **Download Configuration** button ().
Download of running-config may take a little while to complete, as the file must be prepared for download.

7.7 Configuration – Upload

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

It is possible to upload a file from the web browser to all the files on the switch, except default-config, which is read-only. This page allows the user to upload a file from the web browser.

TECHAYA
RUGGED DESIGN

- Configuration
- Monitor
- Diagnostics
- ▼ Maintenance
 - Restart Device
 - Factory Defaults
- ▼ Software
 - Upload
 - Image Select
- ▼ Configuration
 - Save startup-config
 - Download
 - Upload
 - Activate
 - Delete

Upload Configuration

File To Upload

Choose File

Destination File

File Name	Parameters
☐ running-config	☒ Replace ☐ Merge
☐ startup-config	
☐ Create new file	

Upload Configuration

7.7.1 File to Upload

Choose file () to upload.

7.7.2 Destination File

To upload the selected configuration file:

1. Click one of the radio buttons to select the destination file to replace.
2. Click the **Upload Configuration** button ().
Download of running-config may take a little while to complete, as the file must be prepared for download.

If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.

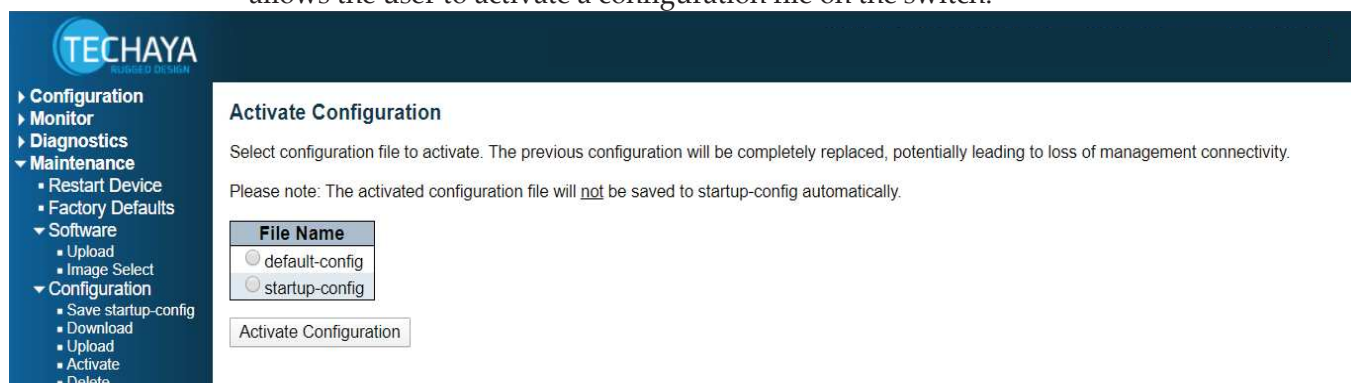
Merge mode: The uploaded file is merged into running-config.

Note: If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

7.8 Configuration – Activate

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration. This page allows the user to activate a configuration file on the switch.



TECHAYA
Rugged Ethernet

- Configuration
- Monitor
- Diagnostics
- ▼ Maintenance
 - Restart Device
 - Factory Defaults
- ▼ Software
 - Upload
 - Image Select
- ▼ Configuration
 - Save startup-config
 - Download
 - Upload
 - Activate
 - Delete

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

7.8.1 Activate Configuration

To activate a configuration file:

1. Click one of the radio buttons to select the file.
2. Click the **Activate Configuration** button ().

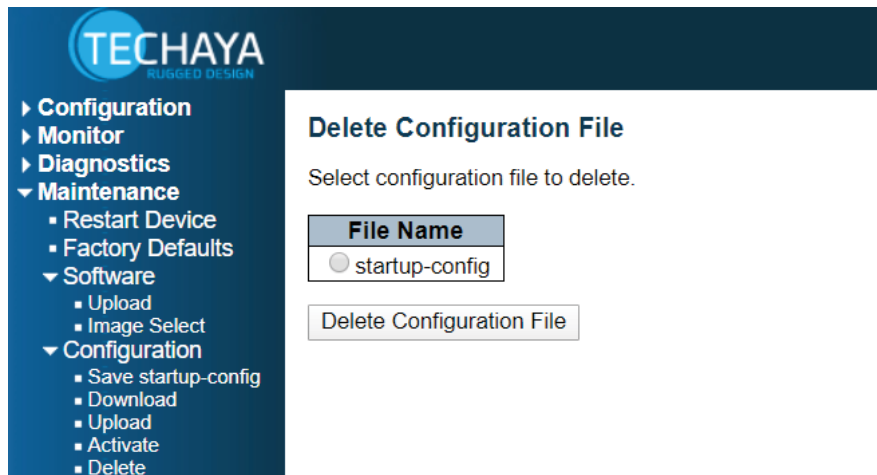
This will initiate the process of completely replacing the existing configuration with that of the selected file.

7.9 Configuration – Delete

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

This page allows the user to delete a configuration file on the switch.



TECHAYA
RUGGED DESIGN

- Configuration
- Monitor
- Diagnostics
- ▼ Maintenance
 - Restart Device
 - Factory Defaults
 - ▼ Software
 - Upload
 - Image Select
 - ▼ Configuration
 - Save startup-config
 - Download
 - Upload
 - Activate
 - Delete

Delete Configuration File

Select configuration file to delete.

File Name
☐ startup-config

Delete Configuration File

7.9.1 Delete Configuration

To delete a configuration file:

1. Click one of the radio buttons to select the file.
2. Click the **Delete Configuration File** button (Delete Configuration File).