



HIRSCHMANN

A **BELDEN** BRAND

Reference Manual

Command Line Interface (CLI)

Embedded Ethernet Switch (HiOS-2E EES)

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2014 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD/DVD applies.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (<http://www.hirschmann.com>).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

Contents

	Safety instructions	27
	About this Manual	29
	Key	31
A	Introduction	32
A.1	Command Line Interface	33
B	Access to CLI	35
B.1	Preparing the data connection	36
B.2	CLI via SSH (Secure Shell)	37
B.3	CLI via the V.24 port	41
B.4	CLI access via telnet	45
	B.4.1 Telnet connection via Windows	45
	B.4.2 Telnet connection via PuTTY	47
C	Using the CLI	51
C.1	Mode-based command hierarchy	52
C.2	Executing the commands	57
	C.2.1 Syntax analysis	57
	C.2.2 Command tree	57
	C.2.3 Structure of a command	58
C.3	Properties of the CLI	62
	C.3.1 Input prompt	62
	C.3.2 Key combinations	64
	C.3.3 Data entry elements	66
D	Examples	69
D.1	Saving the Configuration	70
D.2	Syntax of the „radius server auth add“ command	71
E	Maintenance	73
E.1	Service Shell	74

	Command reference	77
1	Address Conflict Detection (ACD)	79
1.1	address-conflict	80
1.1.1	address-conflict operation	80
1.1.2	address-conflict detection-mode	80
1.1.3	address-conflict detection-ongoing	81
1.1.4	address-conflict delay	82
1.1.5	address-conflict release-delay	82
1.1.6	address-conflict max-protection	82
1.1.7	address-conflict protect-interval	83
1.1.8	address-conflict trap-status	83
1.2	show	84
1.2.1	show address-conflict global	84
1.2.2	show address-conflict detected	84
1.2.3	show address-conflict fault-state	85
2	Application Lists	87
2.1	applists	88
2.1.1	applists set-authlist	88
2.1.2	applists enable	88
2.1.3	applists disable	89
2.2	show	90
2.2.1	show appllists	90
3	Authentication Lists	91
3.1	authlists	92
3.1.1	authlists add	92
3.1.2	authlists delete	92
3.1.3	authlists set-policy	93
3.1.4	authlists enable	93
3.1.5	authlists disable	94
3.2	show	95
3.2.1	show authlists	95
4	Auto Disable	97
4.1	auto-disable	98
4.1.1	auto-disable reason	98
4.2	auto-disable	99
4.2.1	auto-disable timer	99

4.2.2	auto-disable reset	99
4.3	show	101
4.3.1	show auto-disable brief	101
4.3.2	show auto-disable reasons	101
5	Class Of Service	103
5.1	classofservice	104
5.1.1	classofservice ip-dscp-mapping	104
5.1.2	classofservice dot1p-mapping	107
5.2	classofservice	108
5.2.1	classofservice trust	108
5.3	cos-queue	109
5.3.1	cos-queue strict	109
5.3.2	cos-queue weighted	109
5.3.3	cos-queue min-bandwidth	110
5.4	show	111
5.4.1	show classofservice ip-dscp-mapping	111
5.4.2	show classofservice dot1p-mapping	111
5.4.3	show classofservice trust	112
5.4.4	show cos-queue	112
6	Command Line Interface (CLI)	113
6.1	cli	114
6.1.1	cli serial-timeout	114
6.1.2	cli prompt	114
6.1.3	cli numlines	115
6.1.4	cli banner operation	115
6.1.5	cli banner text	116
6.2	show	117
6.2.1	show cli global	117
6.2.2	show cli command-tree	117
6.3	logging	118
6.3.1	logging cli-command	118
6.4	show	119
6.4.1	show logging cli-command	119
7	Clock	121
7.1	clock	122
7.1.1	clock set	122
7.1.2	clock timezone offset	122
7.1.3	clock timezone zone	123

7.1.4	clock summer-time mode	123
7.1.5	clock summer-time recurring start	123
7.1.6	clock summer-time recurring end	124
7.1.7	clock summer-time zone	125
7.2	show	127
7.2.1	show clock	127
8	Configuration	129
8.1	save	130
8.1.1	save profile	130
8.2	config	131
8.2.1	config watchdog admin-state	131
8.2.2	config watchdog timeout	131
8.2.3	config encryption password set	132
8.2.4	config encryption password clear	132
8.2.5	config profile select	132
8.2.6	config profile delete	133
8.2.7	config fingerprint verify	133
8.3	copy	134
8.3.1	copy firmware remote	134
8.3.2	copy firmware system remote	134
8.3.3	copy config running-config nvm	135
8.3.4	copy config running-config remote	135
8.3.5	copy config nvm	135
8.3.6	copy config remote	136
8.4	clear	137
8.4.1	clear config	137
8.4.2	clear factory	137
8.5	show	138
8.5.1	show running-config xml	138
8.5.2	show running-config script	138
8.6	show	139
8.6.1	show config watchdog	139
8.6.2	show config encryption	139
8.6.3	show config profiles	140
8.6.4	show config status	140
9	Debugging	141
9.1	debug	142
9.1.1	debug tcpdump help	142
9.1.2	debug tcpdump start cpu	142
9.1.3	debug tcpdump stop	143

9.1.4	debug tcpdump filter show	143
9.1.5	debug tcpdump filter list	143
9.1.6	debug tcpdump filter delete	144
9.2	copy	145
9.2.1	copy tcpdumpcap nvm remote	145
9.2.2	copy tcpdumpfilter remote	145
9.2.3	copy tcpdumpfilter nvm	146
10	Device Monitoring	147
10.1	device-status	148
10.1.1	device-status monitor link-failure	148
10.1.2	device-status monitor ring-redundancy	148
10.1.3	device-status trap	149
10.2	device-status	150
10.2.1	device-status link-alarm	150
10.3	show	151
10.3.1	show device-status monitor	151
10.3.2	show device-status state	151
10.3.3	show device-status trap	152
10.3.4	show device-status events	152
10.3.5	show device-status link-alarm	152
10.3.6	show device-status all	153
11	Device Security	155
11.1	security-status	156
11.1.1	security-status monitor pwd-change	156
11.1.2	security-status monitor pwd-min-length	156
11.1.3	security-status monitor pwd-policy-config	157
11.1.4	security-status monitor pwd-policy-inactive	158
11.1.5	security-status monitor telnet-enabled	158
11.1.6	security-status monitor http-enabled	159
11.1.7	security-status monitor snmp-unsecure	159
11.1.8	security-status monitor sysmon-enabled	160
11.1.9	security-status monitor no-link-enabled	160
11.1.10	security-status monitor hidisc-write-enabled	161
11.1.11	security-status monitor iec61850-mms-enabled	161
11.1.12	security-status monitor https-certificate	162
11.1.13	security-status trap	162
11.2	security-status	163
11.2.1	security-status no-link	163
11.3	show	164
11.3.1	show security-status monitor	164
11.3.2	show security-status state	164

11.3.3	show security-status no-link	165
11.3.4	show security-status trap	165
11.3.5	show security-status events	165
11.3.6	show security-status all	166
12	Differentiated Services (DiffServ)	167
12.1	diffserv	168
12.2	class-map	169
12.2.1	class-map name	169
12.2.2	class-map rename	172
12.2.3	class-map match-all	172
12.2.4	class-map remove	173
12.3	policy-map	174
12.3.1	policy-map create	174
12.3.2	policy-map name class add	174
12.3.3	policy-map name class name assign-queue	175
12.3.4	policy-map name class name conform-color	176
12.3.5	policy-map name class name drop	176
12.3.6	policy-map name class name mark	177
12.3.7	policy-map name class name mirror	178
12.3.8	policy-map name class name police-simple conform action drop violate-action	180
12.3.9	policy-map name class name police-simple conform action set-cos-as-sec-cos violate-action	182
12.3.10	policy-map name class name police-simple conform action set-cos-transmit violate-action	184
12.3.11	policy-map name class name police-simple conform action set-dscp-transmit violate-action	186
12.3.12	policy-map name class name police-simple conform action set-prec-transmit violate-action	189
12.3.13	policy-map name class name police-simple conform action set-sec-cos-transmit violate-action	191
12.3.14	policy-map name class name police-simple conform action transmit violate-action	193
12.3.15	policy-map name class name police-two-rate conform-action ... exceed-action ... violate-action ...	195
12.3.16	policy-map name class name redirect	197
12.3.17	policy-map name class remove	198
12.3.18	policy-map rename	199
12.3.19	policy-map remove	199
12.4	service-policy	200
12.5	service-policy	201

12.6	show	202
12.6.1	show diffserv global	202
12.6.2	show diffserv service brief	202
12.6.3	show diffserv service interface	203
12.6.4	show class-map	203
12.6.5	show policy-map all	203
12.6.6	show policy-map interface	204
12.6.7	show policy-map name	204
12.6.8	show service-policy	204
13	DoS Mitigation	205
13.1	dos	206
13.1.1	dos tcp-null	206
13.1.2	dos tcp-xmas	206
13.1.3	dos tcp-syn-fin	207
13.1.4	dos tcp-min-header	207
13.1.5	dos icmp-fragmented	208
13.1.6	dos icmp payload-check	208
13.1.7	dos icmp payload-size	209
13.1.8	dos ip-land	209
13.1.9	dos tcp-offset	210
13.1.10	dos tcp-syn	210
13.1.11	dos l4-port	211
13.2	show	212
13.2.1	show dos	212
14	IEEE 802.1x (Dot1x)	213
14.1	dot1x	214
14.1.1	dot1x dynamic-vlan	214
14.1.2	dot1x system-auth-control	214
14.1.3	dot1x monitor	215
14.2	dot1x	216
14.2.1	dot1x guest-vlan	216
14.2.2	dot1x max-req	216
14.2.3	dot1x port-control	217
14.2.4	dot1x re-authentication	217
14.2.5	dot1x unauthenticated-vlan	218
14.2.6	dot1x timeout guest-vlan-period	218
14.2.7	dot1x timeout reauth-period	218
14.2.8	dot1x timeout quiet-period	219
14.2.9	dot1x timeout tx-period	219
14.2.10	dot1x timeout supp-timeout	219
14.2.11	dot1x timeout server-timeout	220
14.2.12	dot1x initialize	220

14.2.13	dot1x re-authenticate	221
14.3	show	222
14.3.1	show dot1x global	222
14.3.2	show dot1x auth-history	222
14.3.3	show dot1x detail	223
14.3.4	show dot1x summary	223
14.3.5	show dot1x clients	223
14.3.6	show dot1x statistics	224
14.4	clear	225
14.4.1	clear dot1x statistics port	225
14.4.2	clear dot1x statistics all	225
14.4.3	clear dot1x auth-history port	226
14.4.4	clear dot1x auth-history all	226
15	IEEE 802.3ad (Dot3ad)	227
15.1	link-aggregation	228
15.1.1	link-aggregation add	228
15.1.2	link-aggregation modify	228
15.1.3	link-aggregation delete	229
15.2	lacp	230
15.2.1	lacp admin-key	230
15.2.2	lacp collector-max-delay	230
15.2.3	lacp lacpmode	231
15.2.4	lacp actor admin key	231
15.2.5	lacp actor admin state lacp-activity	231
15.2.6	lacp actor admin state lacp-timeout	232
15.2.7	lacp actor admin state aggregation	232
15.2.8	lacp actor admin port priority	233
15.2.9	lacp partner admin key	233
15.2.10	lacp partner admin state lacp-activity	234
15.2.11	lacp partner admin state lacp-timeout	234
15.2.12	lacp partner admin state aggregation	235
15.2.13	lacp partner admin port priority	235
15.2.14	lacp partner admin port id	235
15.2.15	lacp partner admin system-priority	236
15.2.16	lacp partner admin system-id	236
15.3	show	237
15.3.1	show link-aggregation port	237
15.3.2	show link-aggregation statistics	237
15.3.3	show link-aggregation members	238
15.3.4	show lacp interface	238
15.3.5	show lacp mode	238
15.3.6	show lacp actor	239
15.3.7	show lacp partner operational	239

15.3.8	show lacp partner admin	239
16	Filtering Database (FDB)	241
16.1	mac-filter	242
16.1.1	mac-filter	242
16.2	bridge	243
16.2.1	bridge aging-time	243
16.3	show	244
16.3.1	show mac-filter-table static	244
16.4	show	245
16.4.1	show bridge aging-time	245
16.5	show	246
16.5.1	show mac-addr-table	246
16.6	clear	247
16.6.1	clear mac-addr-table	247
17	HiDiscovery	249
17.1	network	250
17.1.1	network hidiscovery operation	250
17.1.2	network hidiscovery mode	250
17.1.3	network hidiscovery blinking	251
17.2	show	252
17.2.1	show network hidiscovery	252
18	Hypertext Transfer Protocol (HTTP)	253
18.1	http	254
18.1.1	http port	254
18.1.2	http server	254
18.2	show	255
18.2.1	show http	255
19	HTTP Secure (HTTPS)	257
19.1	https	258
19.1.1	https server	258
19.1.2	https port	258
19.1.3	https certificate	259
19.2	copy	260
19.2.1	copy https-cert remote	260

19.3	show	261
	19.3.1 show https	261
20	Integrated Authentication Server (IAS)	263
20.1	ias-users	264
	20.1.1 ias-users add	264
	20.1.2 ias-users delete	264
	20.1.3 ias-users enable	265
	20.1.4 ias-users disable	265
	20.1.5 ias-users password	265
20.2	show	266
	20.2.1 show ias-users	266
21	IEC 61850 MMS Server	267
21.1	iec61850-mms	268
	21.1.1 iec61850-mms operation	268
	21.1.2 iec61850-mms write-access	269
	21.1.3 iec61850-mms port	269
	21.1.4 iec61850-mms max-sessions	270
	21.1.5 iec61850-mms technical-key	270
21.2	show	271
	21.2.1 show iec61850-mms	271
22	IGMP Snooping	273
22.1	igmp-snooping	274
	22.1.1 igmp-snooping mode	274
	22.1.2 igmp-snooping querier mode	274
	22.1.3 igmp-snooping querier query-interval	275
	22.1.4 igmp-snooping querier timer-expiry	275
	22.1.5 igmp-snooping querier version	276
	22.1.6 igmp-snooping forward-unknown	276
22.2	igmp-snooping	277
	22.2.1 igmp-snooping vlan-id	277
22.3	igmp-snooping	279
	22.3.1 igmp-snooping mode	279
	22.3.2 igmp-snooping fast-leave	279
	22.3.3 igmp-snooping groupmembership-interval	280
	22.3.4 igmp-snooping maxresponse	280
	22.3.5 igmp-snooping mcrtrexpiretime	281
	22.3.6 igmp-snooping static-query-port	281
22.4	show	282

22.4.1	show igmp-snooping global	282
22.4.2	show igmp-snooping interface	282
22.4.3	show igmp-snooping vlan	283
22.4.4	show igmp-snooping querier global	283
22.4.5	show igmp-snooping querier vlan	283
22.4.6	show igmp-snooping enhancements vlan	284
22.4.7	show igmp-snooping enhancements unknown-filtering	284
22.4.8	show igmp-snooping statistics global	284
22.4.9	show igmp-snooping statistics interface	285
22.5	show	286
22.5.1	show mac-filter-table igmp-snooping	286
22.6	clear	287
22.6.1	clear igmp-snooping	287
23	Interface	289
23.1	shutdown	290
23.1.1	shutdown	290
23.2	auto-negotiate	291
23.2.1	auto-negotiate	291
23.3	auto-power-down	292
23.3.1	auto-power-down	292
23.4	cable-crossing	293
23.4.1	cable-crossing	293
23.5	linktraps	294
23.5.1	linktraps	294
23.6	speed	295
23.6.1	speed	295
23.7	name	296
23.7.1	name	296
23.8	power-state	297
23.8.1	power-state	297
23.9	mac-filter	298
23.9.1	mac-filter	298
23.10	led-signaling	299
23.10.1	led-signaling operation	299
23.11	show	300
23.11.1	show port all	300
23.12	show	301

23.12.1	show led-signaling operation	301
24	Interface Statistics	303
24.1	utilization	304
24.1.1	utilization control-interval	304
24.1.2	utilization alarm-threshold lower	304
24.1.3	utilization alarm-threshold upper	305
24.2	clear	306
24.2.1	clear port-statistics	306
24.3	show	307
24.3.1	show interface counters	307
24.3.2	show interface utilization	307
24.3.3	show interface statistics	308
24.3.4	show interface ether-stats	308
25	Intern	309
25.1	help	310
25.2	logout	311
25.3	history	312
25.4	vlan-mode	313
25.4.1	vlan-mode	313
25.5	exit	314
25.6	end	315
25.7	serviceshell	316
25.7.1	serviceshell deactivate	316
25.8	traceroute	317
25.8.1	traceroute maxttl	317
25.9	reboot	318
25.9.1	reboot after	318
25.10	ping	319
25.10.1	ping	319
25.11	show	320
25.11.1	show reboot	320
25.11.2	show serviceshell	320
26	Internet Protocol Version 4 (IPv4)	321
26.1	network	322
26.1.1	network protocol	322

26.1.2	network parms	322
26.2	clear	323
26.2.1	clear arp-table-switch	323
26.3	show	324
26.3.1	show network parms	324
26.4	show	325
26.4.1	show arp	325
27	Link Backup	327
27.1	link-backup	328
27.1.1	link-backup operation	328
27.2	link-backup	329
27.2.1	link-backup add	329
27.2.2	link-backup delete	329
27.2.3	link-backup modify	330
27.3	show	331
27.3.1	show link-backup operation	331
27.3.2	show link-backup pairs	331
28	Link Layer Discovery Protocol (LLDP)	333
28.1	lldp	334
28.1.1	lldp operation	334
28.1.2	lldp config chassis admin-state	334
28.1.3	lldp config chassis notification-interval	335
28.1.4	lldp config chassis re-init-delay	335
28.1.5	lldp config chassis tx-delay	336
28.1.6	lldp config chassis tx-hold-multiplier	336
28.1.7	lldp config chassis tx-interval	336
28.2	show	337
28.2.1	show lldp global	337
28.2.2	show lldp port	337
28.2.3	show lldp remote-data	338
28.3	lldp	339
28.3.1	lldp admin-state	339
28.3.2	lldp fdb-mode	339
28.3.3	lldp max-neighbors	340
28.3.4	lldp notification	340
28.3.5	lldp tlv link-aggregation	341
28.3.6	lldp tlv mac-phy-config-state	341
28.3.7	lldp tlv max-frame-size	342
28.3.8	lldp tlv mgmt-addr	342
28.3.9	lldp tlv port-desc	343

28.3.10	lldp tlv port-vlan	343
28.3.11	lldp tlv protocol	344
28.3.12	lldp tlv sys-cap	344
28.3.13	lldp tlv sys-desc	345
28.3.14	lldp tlv sys-name	345
28.3.15	lldp tlv vlan-name	346
28.3.16	lldp tlv protocol-based-vlan	346
28.3.17	lldp tlv igmp	347
28.3.18	lldp tlv portsec	347
28.3.19	lldp tlv ptp	348
29	Logging	349
29.1	logging	350
29.1.1	logging audit-trail	350
29.1.2	logging buffered severity	350
29.1.3	logging host add	351
29.1.4	logging host delete	352
29.1.5	logging host enable	353
29.1.6	logging host disable	353
29.1.7	logging host modify	353
29.1.8	logging syslog operation	354
29.1.9	logging current-console operation	355
29.1.10	logging current-console severity	355
29.1.11	logging console operation	356
29.1.12	logging console severity	357
29.2	show	358
29.2.1	show logging buffered	358
29.2.2	show logging traplogs	358
29.2.3	show logging console	359
29.2.4	show logging syslog	359
29.2.5	show logging host	359
29.3	copy	360
29.3.1	copy eventlog buffered remote	360
29.3.2	copy traplog system remote	360
29.3.3	copy audittrail system remote	361
29.4	clear	362
29.4.1	clear logging buffered	362
29.4.2	clear eventlog	362
30	Management Access	363
30.1	network	364
30.1.1	network management access web timeout	364
30.1.2	network management access add	364
30.1.3	network management access delete	365

30.1.4	network management access modify	366
30.1.5	network management access operation	367
30.1.6	network management access status	367
30.2	show	368
30.2.1	show network management access global	368
30.2.2	show network management access rules	368
31	Management Address	369
31.1	network	370
31.1.1	network management mac	370
31.1.2	network management port	370
31.2	show	371
31.2.1	show network management mac	371
31.2.2	show network management port	371
32	Media Redundancy Protocol (MRP)	373
32.1	mrp	374
32.1.1	mrp domain modify advanced-mode	374
32.1.2	mrp domain modify manager-priority	374
32.1.3	mrp domain modify mode	375
32.1.4	mrp domain modify name	375
32.1.5	mrp domain modify operation	375
32.1.6	mrp domain modify port primary	376
32.1.7	mrp domain modify port secondary	376
32.1.8	mrp domain modify recovery-delay	376
32.1.9	mrp domain modify round-trip-delay	377
32.1.10	mrp domain modify vlan	377
32.1.11	mrp domain add default-domain	378
32.1.12	mrp domain add domain-id	378
32.1.13	mrp domain delete	378
32.1.14	mrp operation	379
32.2	show	380
32.2.1	show mrp	380
33	MRP IEEE	381
33.1	mrp-ieee	382
33.1.1	mrp-ieee global join-time	382
33.1.2	mrp-ieee global leave-time	382
33.1.3	mrp-ieee global leave-all-time	383
33.2	show	384
33.2.1	show mrp-ieee global interface	384

34	MRP IEEE MMRP	385
34.1	mrp-ieee	386
34.1.1	mrp-ieee mmrp vlan-id	386
34.2	show	387
34.2.1	show mrp-ieee mmrp global	387
34.2.2	show mrp-ieee mmrp interface	387
34.2.3	show mrp-ieee mmrp statistics global	388
34.2.4	show mrp-ieee mmrp statistics interface	388
34.2.5	show mrp-ieee mmrp service-requirement forward-all vlan	388
34.2.6	show mrp-ieee mmrp service-requirement forbidden vlan	389
34.3	mrp-ieee	390
34.3.1	mrp-ieee mmrp operation	390
34.3.2	mrp-ieee mmrp periodic-machine	391
34.4	clear	392
34.4.1	clear mrp-ieee mmrp	392
34.5	mrp-ieee	393
34.5.1	mrp-ieee mmrp operation	393
34.5.2	mrp-ieee mmrp restrict-register	394
34.6	show	395
34.6.1	show mac-filter-table mmrp	395
35	MRP IEEE MVRP	397
35.1	mrp-ieee	398
35.1.1	mrp-ieee mvrp operation	398
35.1.2	mrp-ieee mvrp periodic-machine	399
35.2	mrp-ieee	400
35.2.1	mrp-ieee mvrp operation	400
35.2.2	mrp-ieee mvrp restrict-register	401
35.3	show	402
35.3.1	show mrp-ieee mvrp global	402
35.3.2	show mrp-ieee mvrp interface	402
35.3.3	show mrp-ieee mvrp statistics global	403
35.3.4	show mrp-ieee mvrp statistics interface	403
35.4	clear	404
35.4.1	clear mrp-ieee mvrp	404
36	Port Monitor	405

36.1	port-monitor	406
	36.1.1 port-monitor operation	406
36.2	port-monitor	407
	36.2.1 port-monitor condition crc-fragments interval	407
	36.2.2 port-monitor condition crc-fragments count	407
	36.2.3 port-monitor condition crc-fragments mode	408
	36.2.4 port-monitor condition link-flap interval	408
	36.2.5 port-monitor condition link-flap count	409
	36.2.6 port-monitor condition link-flap mode	409
	36.2.7 port-monitor condition duplex-mismatch mode	410
	36.2.8 port-monitor action	410
	36.2.9 port-monitor reset	411
36.3	show	412
	36.3.1 show port-monitor operation	412
	36.3.2 show port-monitor brief	412
	36.3.3 show port-monitor port	413
	36.3.4 show port-monitor link-flap	413
	36.3.5 show port-monitor crc-fragments	413
37	Port Security	415
37.1	port-security	416
	37.1.1 port-security operation	416
37.2	port-security	417
	37.2.1 port-security operation	417
	37.2.2 port-security max-dynamic	417
	37.2.3 port-security max-static	418
	37.2.4 port-security mac-address add	418
	37.2.5 port-security mac-address move	418
	37.2.6 port-security mac-address delete	419
	37.2.7 port-security violation-traps	419
37.3	show	420
	37.3.1 show port-security global	420
	37.3.2 show port-security interface	420
	37.3.3 show port-security dynamic	421
	37.3.4 show port-security static	421
	37.3.5 show port-security violation	421
38	Precision Time Protocol (PTP)	423
38.1	ptp	424
	38.1.1 ptp operation	424
	38.1.2 ptp clock-mode	424
	38.1.3 ptp sync-lower-bound	425
	38.1.4 ptp sync-upper-bound	425

38.1.5	ptp management	426
38.1.6	ptp v2-transparent-clock syntonization	426
38.1.7	ptp v2-transparent-clock network-protocol	427
38.1.8	ptp v2-transparent-clock multi-domain	427
38.1.9	ptp v2-transparent-clock sync-local-clock	428
38.1.10	ptp v2-transparent-clock delay-mechanism	428
38.1.11	ptp v2-transparent-clock primary-domain	429
38.1.12	ptp v2-transparent-clock vlan	429
38.1.13	ptp v2-transparent-clock vlan-priority	429
38.1.14	ptp v2-boundary-clock domain	430
38.1.15	ptp v2-boundary-clock priority1	430
38.1.16	ptp v2-boundary-clock priority2	430
38.1.17	ptp v2-boundary-clock utc-offset	431
38.1.18	ptp v2-boundary-clock utc-offset-valid	431
38.2	ptp	432
38.2.1	ptp v2-transparent-clock operation	432
38.2.2	ptp v2-transparent-clock asymmetry	432
38.2.3	ptp v2-transparent-clock pdelay-interval	433
38.2.4	ptp v2-boundary-clock operation	433
38.2.5	ptp v2-boundary-clock pdelay-interval	434
38.2.6	ptp v2-boundary-clock announce-interval	434
38.2.7	ptp v2-boundary-clock sync-interval	435
38.2.8	ptp v2-boundary-clock announce-timeout	435
38.2.9	ptp v2-boundary-clock asymmetry	436
38.2.10	ptp v2-boundary-clock v1-compatibility-mode	436
38.2.11	ptp v2-boundary-clock delay-mechanism	436
38.2.12	ptp v2-boundary-clock network-protocol	437
38.2.13	ptp v2-boundary-clock vlan-priority	437
38.2.14	ptp v2-boundary-clock vlan	438
38.3	show	439
38.3.1	show ptp	439
39	Password Management	441
39.1	passwords	442
39.1.1	passwords min-length	442
39.1.2	passwords max-login-attempts	442
39.1.3	passwords min-uppercase-chars	443
39.1.4	passwords min-lowercase-chars	443
39.1.5	passwords min-numeric-chars	443
39.1.6	passwords min-special-chars	444
39.2	show	445
39.2.1	show passwords	445
40	Radius	447

40.1	authorization	448
40.1.1	authorization network radius	448
40.2	radius	449
40.2.1	radius accounting mode	449
40.2.2	radius server attribute 4	449
40.2.3	radius server acct add	450
40.2.4	radius server acct delete	450
40.2.5	radius server acct modify	451
40.2.6	radius server auth add	451
40.2.7	radius server auth delete	452
40.2.8	radius server auth modify	452
40.2.9	radius server retransmit	453
40.2.10	radius server timeout	454
40.3	show	455
40.3.1	show radius global	455
40.3.2	show radius auth servers	455
40.3.3	show radius auth statistics	456
40.3.4	show radius acct statistics	456
40.3.5	show radius acct servers	456
40.4	clear	457
40.4.1	clear radius	457
41	Remote Monitoring (RMON)	459
41.1	rmon-alarm	460
41.1.1	rmon-alarm add	460
41.1.2	rmon-alarm enable	461
41.1.3	rmon-alarm disable	461
41.1.4	rmon-alarm delete	461
41.1.5	rmon-alarm modify	462
41.2	show	464
41.2.1	show rmon statistics	464
41.2.2	show rmon alarm	464
42	Script File	465
42.1	script	466
42.1.1	script apply	466
42.1.2	script validate	466
42.1.3	script list system	467
42.1.4	script delete	467
42.2	copy	468
42.2.1	copy script remote	468
42.2.2	copy script nvm	468

42.2.3	copy script running-config nvm	469
42.2.4	copy script running-config remote	469
42.3	show	470
42.3.1	show script system	470
43	Selftest	471
43.1	selftest	472
43.1.1	selftest action	472
43.1.2	selftest ramtest	472
43.1.3	selftest system-monitor	473
43.1.4	selftest boot-default-on-error	474
43.2	show	475
43.2.1	show selftest action	475
43.2.2	show selftest settings	475
44	sFlow	477
44.1	show	478
45	Switched Monitoring (SMON)	479
45.1	monitor	480
45.1.1	monitor session	480
45.2	show	482
45.2.1	show monitor session	482
45.3	clear	483
45.3.1	clear monitor session	483
46	Simple Network Management Protocol (SNMP)	485
46.1	snmp	486
46.1.1	snmp access version v1	486
46.1.2	snmp access version v2	486
46.1.3	snmp access version v3	487
46.1.4	snmp access port	487
46.1.5	snmp access snmp-over-802	488
46.2	show	489
46.2.1	show snmp access	489
47	SNMP Community	491
47.1	snmp	492
47.1.1	snmp community ro	492
47.1.2	snmp community rw	492

47.2	show	493
	47.2.1 show snmp community	493
48	SNMP Logging	495
48.1	logging	496
	48.1.1 logging snmp-request get operation	496
	48.1.2 logging snmp-request get severity	496
	48.1.3 logging snmp-request set operation	497
	48.1.4 logging snmp-request set severity	498
48.2	show	499
	48.2.1 show logging snmp	499
49	Simple Network Time Protocol (SNTP)	501
49.1	sntp	502
	49.1.1 sntp client operation	502
	49.1.2 sntp client operating-mode	502
	49.1.3 sntp client request-interval	503
	49.1.4 sntp client broadcast-rcv-timeout	503
	49.1.5 sntp client disable-after-sync	504
	49.1.6 sntp client server add	504
	49.1.7 sntp client server delete	505
	49.1.8 sntp client server mode	505
	49.1.9 sntp server operation	506
	49.1.10 sntp server port	506
	49.1.11 sntp server only-if-synchronized	507
	49.1.12 sntp server broadcast operation	507
	49.1.13 sntp server broadcast address	508
	49.1.14 sntp server broadcast port	508
	49.1.15 sntp server broadcast interval	508
	49.1.16 sntp server broadcast vlan	509
49.2	show	510
	49.2.1 show sntp global	510
	49.2.2 show sntp client status	510
	49.2.3 show sntp client server	511
	49.2.4 show sntp server status	511
	49.2.5 show sntp server broadcast	511
50	Spanning Tree	513
50.1	spanning-tree	514
	50.1.1 spanning-tree operation	514
	50.1.2 spanning-tree bpdu-filter	514
	50.1.3 spanning-tree bpdu-guard	515
	50.1.4 spanning-tree bpdu-migration-check	515

50.1.5	spanning-tree forceversion	516
50.1.6	spanning-tree forward-time	516
50.1.7	spanning-tree hello-time	516
50.1.8	spanning-tree hold-count	517
50.1.9	spanning-tree max-age	517
50.1.10	spanning-tree mst priority	517
50.2	spanning-tree	518
50.2.1	spanning-tree mode	518
50.2.2	spanning-tree bpdu-flood	518
50.2.3	spanning-tree edge-auto	519
50.2.4	spanning-tree edge-port	519
50.2.5	spanning-tree guard-loop	520
50.2.6	spanning-tree guard-root	520
50.2.7	spanning-tree guard-tcn	521
50.2.8	spanning-tree cost	521
50.2.9	spanning-tree priority	522
50.3	show	523
50.3.1	show spanning-tree global	523
50.3.2	show spanning-tree mst	523
50.3.3	show spanning-tree port	524
51	Secure Shell (SSH)	525
51.1	ssh	526
51.1.1	ssh server	526
51.1.2	ssh timeout	526
51.1.3	ssh port	527
51.1.4	ssh max-sessions	527
51.1.5	ssh key rsa	527
51.1.6	ssh key dsa	528
51.2	copy	529
51.2.1	copy sshkey remote	529
51.3	show	530
51.3.1	show ssh	530
52	Storm Control	531
52.1	storm-control	532
52.1.1	storm-control flow-control	532
52.2	traffic-shape	533
52.2.1	traffic-shape bw	533
52.3	storm-control	534
52.3.1	storm-control flow-control	534
52.3.2	storm-control ingress unit	534

52.3.3	storm-control ingress threshold	535
52.3.4	storm-control ingress unicast operation	535
52.3.5	storm-control ingress multicast operation	536
52.3.6	storm-control ingress broadcast operation	536
52.4	show	537
52.4.1	show storm-control flow-control	537
52.4.2	show storm-control ingress	537
52.4.3	show traffic-shape	538
53	System	539
53.1	system	540
53.1.1	system name	540
53.1.2	system location	540
53.1.3	system contact	541
53.1.4	system pre-login-banner operation	541
53.1.5	system pre-login-banner text	542
53.2	show	543
53.2.1	show eventlog	543
53.2.2	show system info	543
53.2.3	show system pre-login-banner	544
53.2.4	show system flash-status	544
54	Telnet	545
54.1	telnet	546
54.1.1	telnet server	546
54.1.2	telnet timeout	546
54.1.3	telnet port	547
54.1.4	telnet max-sessions	547
54.2	show	548
54.2.1	show telnet	548
55	Traps	549
55.1	snmp	550
55.1.1	snmp trap mode	550
55.1.2	snmp trap delete	550
55.1.3	snmp trap add	551
55.2	show	552
55.2.1	show snmp traps	552
56	Users	553
56.1	users	554

56.1.1	users add	554
56.1.2	users delete	554
56.1.3	users enable	555
56.1.4	users disable	555
56.1.5	users password	555
56.1.6	users snmpv3 authentication	556
56.1.7	users snmpv3 encryption	556
56.1.8	users access-role	556
56.1.9	users lock-status	557
56.1.10	users password-policy-check	557
56.2	show	558
56.2.1	show users	558
57	Virtual LAN (VLAN)	559
57.1	name	560
57.1.1	name	560
57.2	vlan-unaware-mode	561
57.2.1	vlan-unaware-mode	561
57.3	vlan	562
57.3.1	vlan add	562
57.3.2	vlan delete	562
57.4	vlan	563
57.4.1	vlan acceptframe	563
57.4.2	vlan ingressfilter	563
57.4.3	vlan priority	564
57.4.4	vlan pvid	564
57.4.5	vlan tagging	565
57.4.6	vlan participation include	565
57.4.7	vlan participation exclude	566
57.4.8	vlan participation auto	566
57.5	show	567
57.5.1	show vlan id	567
57.5.2	show vlan brief	567
57.5.3	show vlan port	568
57.5.4	show vlan member current	568
57.5.5	show vlan member static	568
57.6	network	569
57.6.1	network management vlan	569
57.6.2	network management priority dot1p	569
57.6.3	network management priority ip-dscp	570
F	Further Support	571

Safety instructions



WARNING

UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

About this Manual

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “GUI Graphical User Interface” reference manual contains detailed information on using the graphical user interface to operate the individual functions of the device.



The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The Industrial HiVision network management software provides you with additional options for smooth configuration and monitoring:

- ▶ ActiveX control for SCADA integration
- ▶ Auto-topology discovery
- ▶ Browser interface
- ▶ Client/server structure
- ▶ Event handling
- ▶ Event log
- ▶ Simultaneous configuration of multiple devices
- ▶ Graphical user interface with network layout
- ▶ SNMP/OPC gateway

Key

The designations used in this manual have the following meanings:

	List
<input data-bbox="210 661 232 692" type="checkbox"/>	Work step
	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
<code>Courier</code>	ASCII representation in the graphical user interface

A Introduction

A.1 Command Line Interface

The Command Line Interface enables you to use the functions of the device through a local or remote connection.

The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices. As an experienced user or administrator, you have knowledge about the basics and about using Embedded Ethernet Switch devices.

The “Command Line Interface” reference manual gives you step-by-step information on using the Command Line Interface (CLI) and its commands.

B Access to CLI

B.1 Preparing the data connection

Information for assembling and starting up your HiOS-2E EES device can be found in the “Installation” user manual.

You will find information for configuring your HiOS-2E EES device in the “Configuration” user manual.

You can access the user interface of the Command Line Interface with the freeware program PuTTY.

- Install PuTTY on your computer.

B.2 CLI via SSH (Secure Shell)

- Start the PuTTY program on your computer.

PuTTY appears with the login screen.

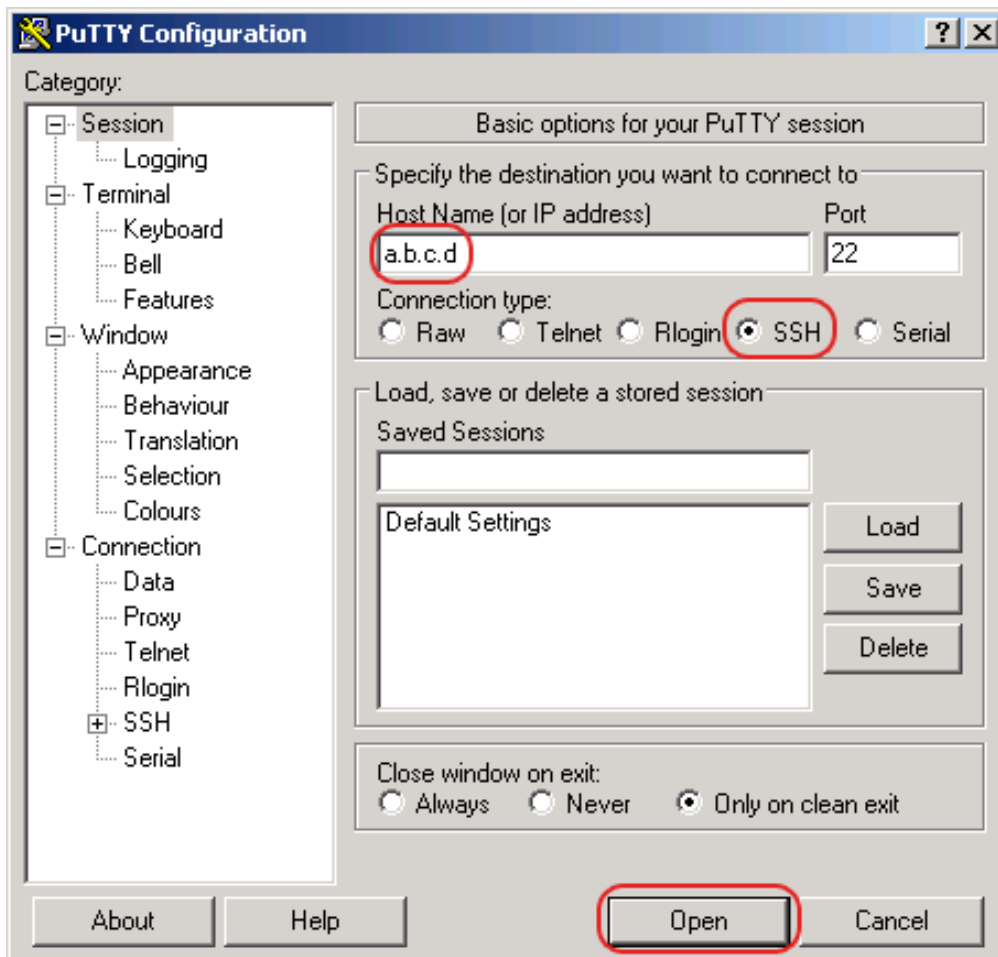


Figure 1: PuTTY input screen

- In the Host Name (or IP address) input field you enter the IP address of your device.
The IP address (a.b.c.d) consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by points.

- To select a connection type, click on `SSH` under `Connection type`.
- After selecting and setting the required parameters, the device enables you to set up the data connection via SSH.
Click “Open” to set up the data connection to your device. Depending on the device and the time at which SSH was configured, setting up the connection takes up to a minute.

When you first login to your device, towards the end of the connection setup, PuTTY displays a security alert message and gives you the option of checking the fingerprint of the key.



Figure 2: Security alert prompt for the fingerprint

- Check the fingerprint to help protect yourself from unwelcome guests.
- If the fingerprint matches that of the device key, click “Yes”.

The device offers the possibility to read the fingerprints of the device key with the CLI command `show ssh` or in the graphical user interface, in the `Device Security > Management Access > Server` dialog, "SSH" tab.

Note:

The OpenSSH Suite offers experienced network administrators a further option to access your device via SSH. To set up the data connection, enter the following command:

```
ssh admin@10.149.112.53
```

`admin` represents the user name.

`10.149.112.53` is the IP address of your device.

CLI appears on the screen with a window for entering the user name.

The device enables up to 5 users to have access to the Command Line Interface at the same time.

```
login as: admin
admin@a.b.c.d's password:
```

Figure 3: Login window in CLI

a.b.c.d is the IP address of your device.

Enter a user name. The default setting for the user name is **admin**.
Press the Enter key.

Enter the password. The default setting for the password is private.
Press the Enter key.

The device offers the possibility to change the user name and the password later in the Command Line Interface.

These entries are case-sensitive.

The device displays the CLI start screen.

Note: Change the password during the first startup procedure.

Copyright (c) 2011-2014 Hirschmann Automation and Control GmbH

All rights reserved

EES Release HiOS-2E-4.0

(Build date 2014-02-20 20:20)

System Name : EES-ECE555010B83
Management IP : 10.115.45.100
Subnet Mask : 255.255.224.0
Base MAC : EC:E5:55:01:0B:83
System Time : 2014-02-11 11:37:30

NOTE: Enter '?' for Command Help. Command help displays all options that are valid for the particular mode.
For the syntax of a particular command form, please consult the documentation.

EES >

Figure 4: Start screen of CLI.

Your HiOS-2E EES appears with the command prompt

(EES) >

B.3 CLI via the V.24 port

The V.24 interface is a serial interface for the local connection of an external management station (VT100 terminal or PC with terminal emulation). The interface allows you to set up a data connection to the Command Line Interface (CLI) and to the system monitor.

The socket housing is electrically connected to the housing of the device.

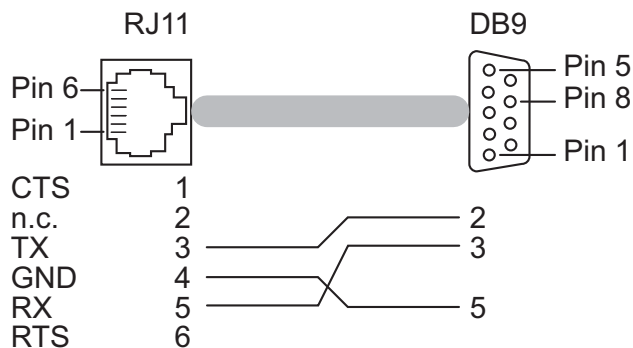


Figure 5: Pin assignment of the V.24 interface and the DB9 connector

VT 100 terminal settings	
Speed	9,600 Baud
Data	8 bit
Stopbit	1 bit
Handshake	off
Parity	none

Set up the serial configuration parameters of the terminal emulation program as follows:

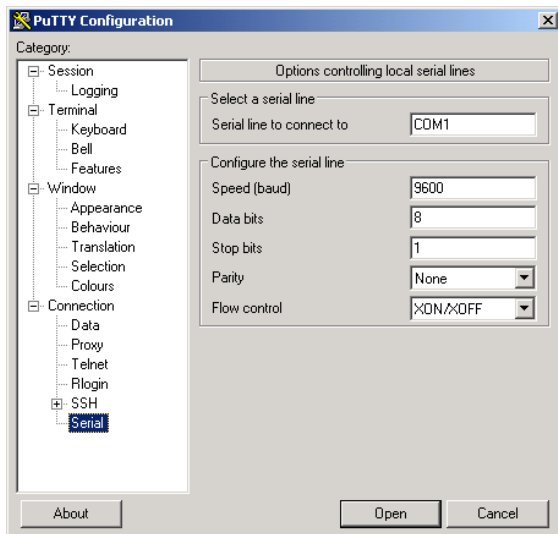


Figure 6: Configuring the serial data connection via PuTTY

- Connect the device to a terminal via V.24. Alternatively connect the device to a “COM” port of your PC using terminal emulation based on VT100 and press any key.
- Alternatively you set up the serial data connection to the device via V.24 with PuTTY (see figure 7). Press the Enter key.

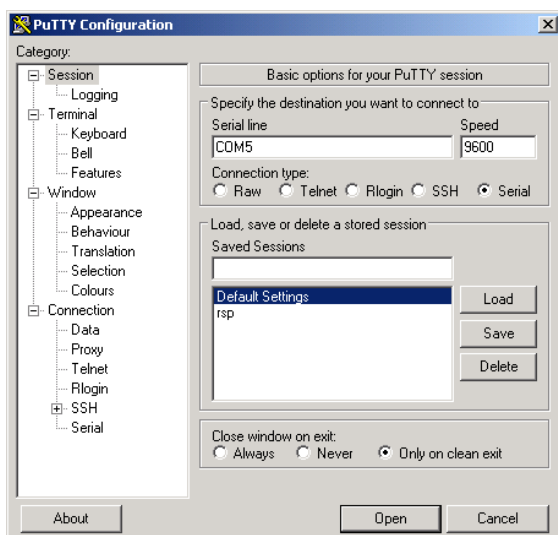


Figure 7: Serial data connection via V.24 with PuTTY

After the data connection has been set up successfully, the device displays a window for entering the user name.

```
Copyright (c) 2011-2014 Hirschmann Automation and Control GmbH
```

```
All rights reserved
```

```
EES Release HiOS-2E-4.0
```

```
(Build date 2014-02-20 20:20)
```

```
System Name      : EES-ECE555010B83
Management IP    : 10.115.45.100
Subnet Mask      : 255.255.224.0
Base MAC         : EC:E5:55:01:0B:83
System Time      : 2014-02-11 11:37:30
```

```
EES >
```

```
User: admin
```

```
Password: *****
```

Figure 8: Logging in to the Command Line Interface program

- Enter a user name. The default setting for the user name is **admin**. Press the Enter key.
- Enter the password. The default setting for the password is private. Press the Enter key.
The device offers the possibility to change the user name and the password later in the Command Line Interface.
These entries are case-sensitive.

The device displays the CLI start screen.

NOTE: Enter '?' for Command Help. Command help displays all options that are valid for the particular mode. For the syntax of a particular command form, please consult the documentation.

```
!*(EES)>
```

Figure 9: CLI screen after login

Note: You can configure the V.24 interface as a terminal/CLI interface. Press any key on your terminal keyboard a number of times until the login screen indicates the CLI mode.

B.4 CLI access via telnet

B.4.1 Telnet connection via Windows

Note: Telnet is only installed as standard in Windows versions before Windows Vista.

► **Start screen**

- Open the Windows start screen on your computer with Start>Run. . . .
- Enter the command `telnet <IP address of the device>` into the "Open:" field.

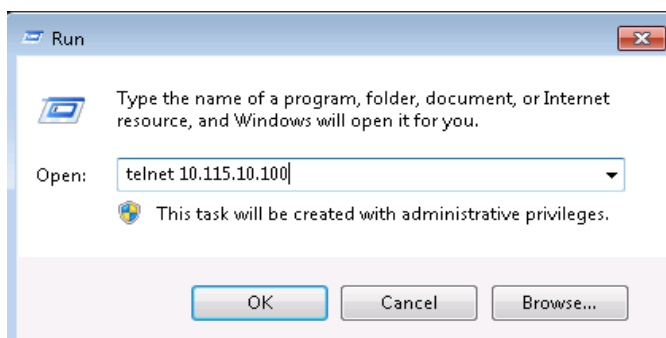
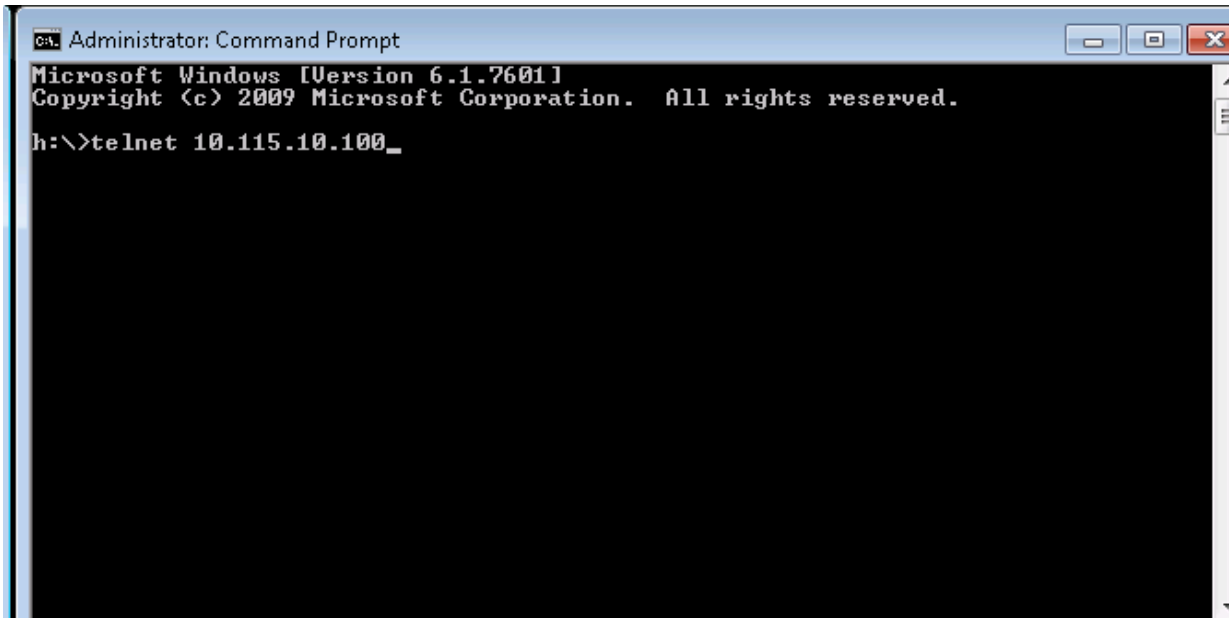


Figure 10: Setting up the telnet connection to the HiOS-2E EES via the Windows entry screen

► **Command prompt**

- With Start>Programs>Accessories>Command Prompt you start the DOS command line interpreter on your computer.
- Enter the command `telnet <IP address of the device>`.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
h:\>telnet 10.115.10.100_
```

Figure 11: Setting up the telnet connection to the HiOS-2E EES via the DOS command line

B.4.2 Telnet connection via PuTTY

- Start the PuTTY program on your computer.

PuTTY appears with the login screen.

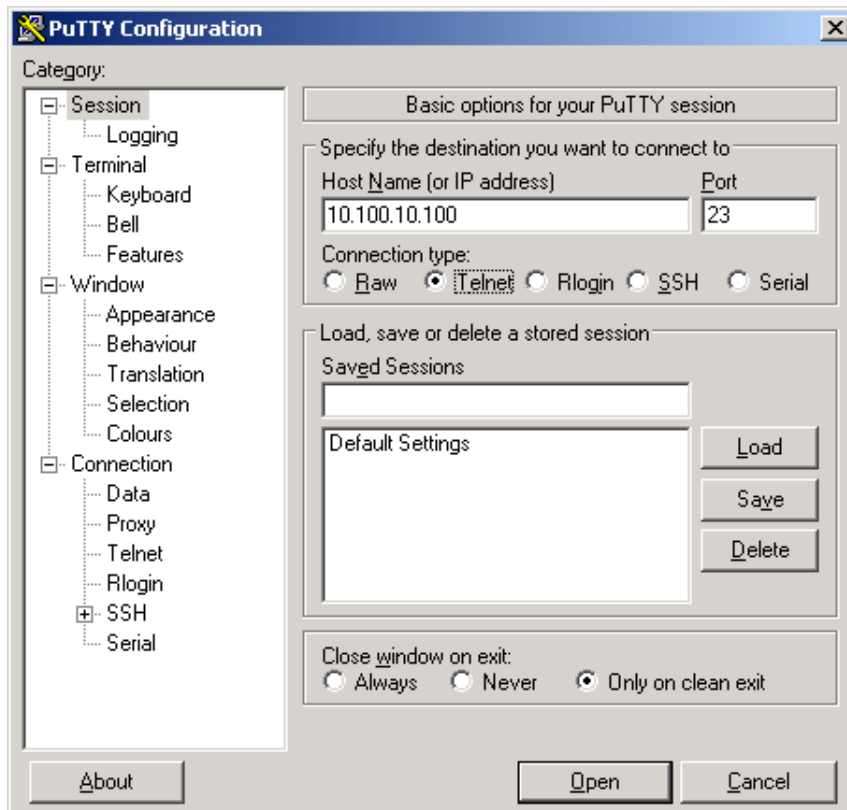


Figure 12: PuTTY input screen

- In the Host Name (or IP address) input field you enter the IP address of your device.
The IP address (a.b.c.d) consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by points.
- To select the connection type, click Telnet under Connection type.
- Click "Open" to set up the data connection to your device.

CLI appears on the screen with a window for entering the user name. The device enables up to 5 users to have access to the Command Line Interface at the same time.

Note: Change the password during the first startup procedure.

- Enter a user name. The default setting for the user name is **admin**. Press the Enter key.
- Enter the password. The default setting for the password is private. Press the Enter key. The device offers the possibility to change the user name and the password later in the Command Line Interface. These entries are case-sensitive.

The device displays the CLI start screen.

Copyright (c) 2011-2014 Hirschmann Automation and Control GmbH

All rights reserved

EES Release HiOS-2E-4.0

(Build date 2014-02-20 20:20)

```
System Name      : EES-ECE555010B83
Management IP    : 10.115.45.100
Subnet Mask      : 255.255.224.0
Base MAC         : EC:E5:55:01:0B:83
System Time      : 2014-02-11 11:37:30
```

```
User:admin
Password:*****
```

NOTE: Enter '?' for Command Help. Command help displays all options that are valid for the particular mode. For the syntax of a particular command form, please consult the documentation.

```
EES >
```

Figure 13: Start screen of CLI.

Your HiOS-2E EES appears with the command prompt
(EES) >

C Using the CLI

C.1 Mode-based command hierarchy

In the CLI, the commands are grouped in the related modes, according to the type of the command. Every command mode supports specific Hirschmann software commands.

The commands available to you as a user depend on your privilege level (administrator, operator, guest, auditor). They also depend on the mode in which you are currently working. The commands of a specific mode are available to you when you switch to this mode.

The User Exec mode commands are an exception. The CLI enables you to execute these commands in the Privileged Exec mode, too.

The following figure shows the modes of the Command Line Interface.

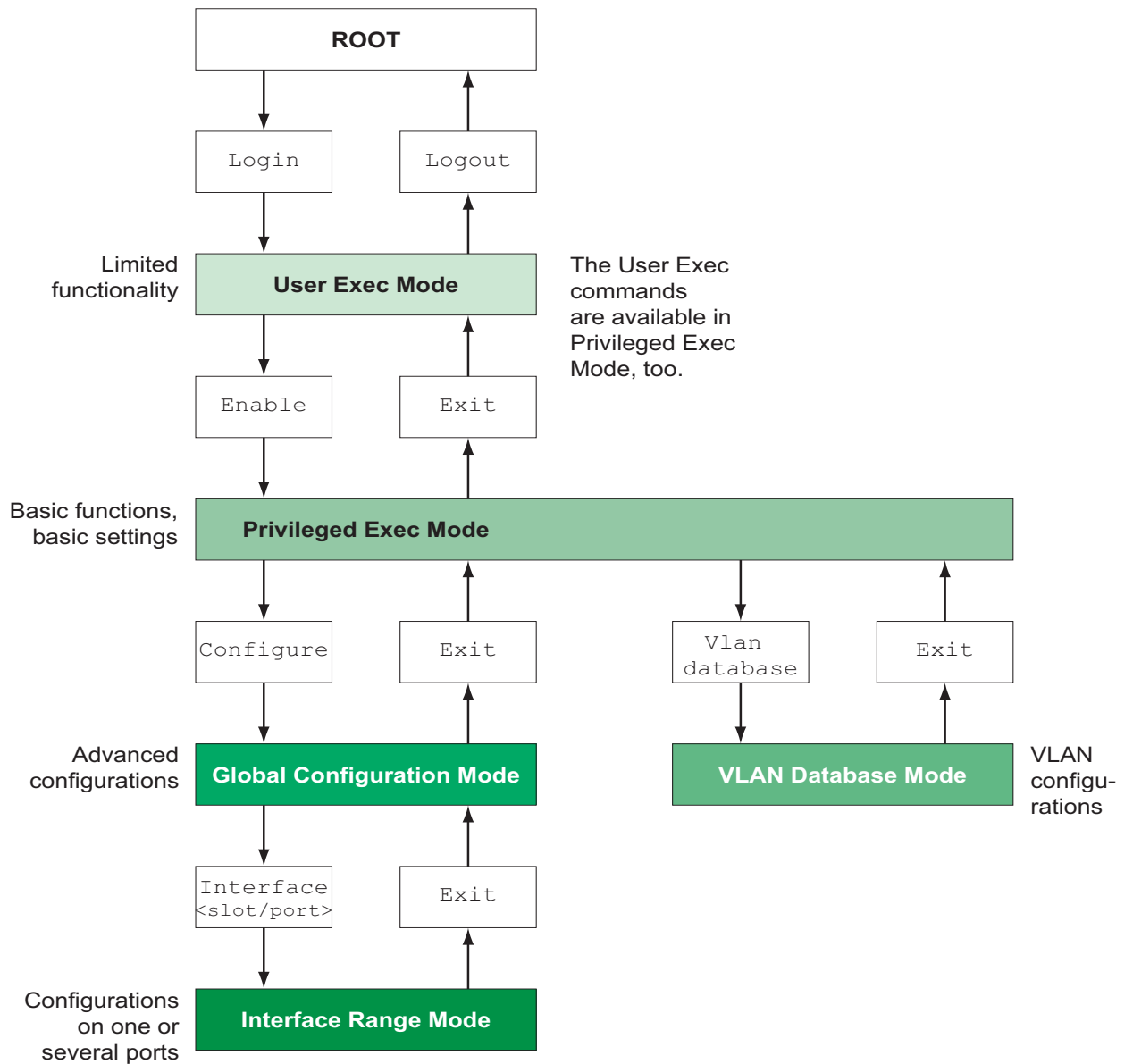


Figure 14: Structure of the CLI

The CLI supports, depending on the user level, the following modes:

▶ **User Exec mode**

When you login to the CLI, you enter the User Exec mode. The User Exec mode contains a limited range of commands.

Command prompt: (EES) >

▶ **Privileged Exec mode**

To access the entire range of commands, you enter the Privileged Exec mode. If you are authenticated as a privileged user by the login, you are able to enter the Privileged Exec mode. In the Privileged Exec mode, you are able to execute the User Exec mode commands, too.

Command prompt: (EES) #

▶ **VLAN mode**

The VLAN mode contains VLAN-related commands.

Command prompt: (EES) (VLAN)#

▶ **Global Config mode**

The Global Config mode allows you to perform modifications to the current configuration. This mode groups general setup commands.

Command prompt: (EES) (config)#

▶ **Interface Range mode**

The commands in the Interface Range mode affect a specific port, a selected group of multiple ports or all port of the device. The commands modify a value or switch a function on/off on one or more specific ports.

▶ All physical ports on the device

Command prompt: (EES) ((interface) all)#

Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:

```
(EES) (config)#interface all
```

```
(EES) ((Interface)all)#
```

▶ A single port on one interface

Command prompt: (EES) (interface <slot/port>)#

Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:

```
(EES) (config)#interface 2/1
```

```
(EES) (interface 2/1)#
```

▶ A range of ports on one interface

Command prompt: (EES) (interface <interface range>)#

Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:

```
(EES) (config)#interface 1/2-1/4
```

```
(EES) ((Interface)1/2-1/4)#
```

- ▶ A list of single ports
 Command prompt: (EES) (interface <interface list>)#
 Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:

```
(EES) (config)#interface 1/2,1/4,1/5
(EES) ((Interface)1/2,1/4,1/5)#
```
- ▶ A list of port ranges and single ports
 Command prompt: (EES) (interface <complex range>)#
 Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:

```
(EES) (config)#interface 1/2-1/4,1/6-1/9
(EES) ((Interface)1/2-1/4,1/6-1/9)
```

The following table shows the command modes, the command prompts (input request characters) visible in the corresponding mode, and the option with which you quit this mode.

Command mode	Access method	Quit or start next mode
User Exec mode	First access level. Perform basic tasks and list system information.	To quit you enter <code>logout</code> : (EES) >logout Are you sure (Y/N) ?y
Privileged Exec mode	From the User Exec mode, you enter the command <code>enable</code> : (EES) >enable (EES) #	To quit the Privileged Exec mode and return to the User Exec mode, you enter <code>exit</code> : (EES) #exit (EES) >
VLAN mode	From the Privileged Exec mode, you enter the command <code>vlan database</code> : (EES) #vlan database (EES) (Vlan)#	To end the VLAN mode and return to the Privileged Exec mode, you enter <code>exit</code> or press <code>Ctrl Z</code> . (EES) (Vlan)#exit (EES) #

Table 1: Command modes

Command mode	Access method	Quit or start next mode
Global Configuration mode	<p>From the Privileged Exec mode, you enter the command <code>configure</code>:</p> <pre>(EES) #configure (EES) (config)#</pre> <p>From the User Exec mode, you enter the command <code>enable</code>, and then in Privileged Exec mode, enter the command <code>Configure</code>:</p> <pre>(EES) >enable (EES) #configure (EES) (config)#</pre>	<p>To quit the Global Configuration mode and return to the Privileged Exec mode, you enter <code>exit</code>:</p> <pre>(EES) (config)#exit (EES) #</pre> <p>To then quit the Privileged Exec mode and return to the User Exec mode, you enter <code>exit</code> again:</p> <pre>(EES) #exit (EES) ></pre>
Interface Range mode	<p>From the Global Configuration mode you enter the command <code>interface {all <slot/port> <interface range> <interface list> <complex range>}</code>.</p> <pre>(EES) (config)#interface <slot/port> (EES) (interface slot/port)#</pre>	<p>To quit the Interface Range mode and return to the Global Configuration mode, you enter “<code>exit</code>”. To return to the Privileged Exec mode, you press <code>Ctrl Z</code>.</p> <pre>(EES) (interface slot/port)#exit (EES) #</pre>

Table 1: Command modes

If you enter a question mark (?) after the prompt, the CLI displays a list of the available commands and a short description of the commands.

```
(EES)>
cli          Set the CLI preferences.
enable      Turn on privileged commands.
help        Display help for various special keys.
history     Show a list of previously run commands.
logout      Exit this session.
ping        Send ICMP echo packets to a specified IP address.
show        Display device options and settings.
telnet      Establish a telnet connection to a remote host.

(EES)>
```

Figure 15: Commands in the User Exec mode

C.2 Executing the commands

C.2.1 Syntax analysis

After you login to the CLI session, you enter the User Exec mode. The CLI displays the prompt `(EES)>` on the screen.

When you enter a command and press the Enter key, the CLI starts the syntax analysis. The CLI searches the command tree for the desired command.

If the command is outside the CLI command range, a message informs you of the detected error.

Example:

The user wants to execute the `show system info` command, but enters „info“ without „f“ and presses the Enter key.

The CLI then displays a message:

```
(EES)>show system ino
Error: Invalid command 'ino'
```

C.2.2 Command tree

The commands in the CLI are organized in a tree structure. The commands, and, if applicable, the related parameters branch down until the command is completely defined and therefore executable. The CLI checks the input. If you have entered the command and the parameters correctly and completely, you execute the command with the Enter key.

After you have entered the command and the required parameters, the other parameters entered are treated as optional parameters. If one of the parameters is unknown, the CLI displays a syntax message.

The command tree branches for the required parameters until the required parameters have reached the last branch in the structure.
With optional parameters, the command tree branches until the required parameters and the optional parameters have reached the last branch in the structure.

C.2.3 Structure of a command

This section describes the syntax, conventions and terminology, and uses examples to represent them.

■ Format of commands

Most of the commands include parameters.

If the command parameter is missing, the CLI informs you about the detection of an incorrect command syntax.

This manual displays the commands and parameters in the `Courier` font. Use them as shown in the manual ([see table 2](#)).

■ Parameters

The sequence of the parameters is relevant for the correct syntax of a command.

Parameters are required values, optional values, selections, or a combination of these things. The representation ([see table 2](#)) indicates the type of the parameter.

<code><command></code>	Commands in pointed brackets (<>) are obligatory.
<code>[command]</code>	Commands in square brackets ([]) are optional.
<code><parameter></code>	Parameters in pointed brackets (<>) are obligatory.
<code>[parameter]</code>	Parameters in square brackets ([]) are optional.

Table 2: Parameter and command syntax

...	An ellipsis (3 points in sequence without spaces) after an element indicates that you can repeat the element.
[Choice1 Choice2]	A vertical line enclosed in brackets indicates a selection option. Select one value. Elements separated by a vertical line and enclosed in square brackets indicate an optional selection (Option1 or Option2 or no selection).
{list}	Curved brackets ({}) indicate that a parameter is to be selected from a list of options.
{Choice1 Choice2}	Elements separated by a vertical line and enclosed in curved brackets ({}) indicate an obligatory selection option (option1 or option2).
[param1 {Choice1 Choice2}]	Shows an optional parameter that contains an obligatory selection.
<a.b.c.d>	Small letters are wild cards. You enter parameters with the notation a.b.c.d with decimal points (e.g. IP addresses)
<cr>	You press the Enter key to create a line break (carriage return).

Table 2: Parameter and command syntax

The following list shows the possible parameter values within the Command Line Interface:

Value	Description
IP address	This parameter represents a valid IPv4 address. The address consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by a decimal point. The IP address 0.0.0.0 is a valid entry.
MAC address	This parameter represents a valid MAC address. The address consists of 6 hexadecimal numbers with values from 00 to FF. The numbers are separated by a colon, for example, 00:F6:29:B2:81:40.
string	User-defined text with a length in the specified range, e.g. a maximum of 32 characters.
character string	Use double quotation marks to indicate a character string, e.g. "System name with space character".
number	Whole integer in the specified range, e.g. 0...999999.
date	Date in format YYYY-MM-DD.
time	Time in format HH:MM:SS.

Table 3: Parameter values in the Command Line Interface

■ Network addresses

Network addresses are a requirement for establishing a data connection to a remote work station, a server, or another network. You distinguish between IP addresses and MAC addresses.

The IP address is an address allocated by the network administrator. Do not use duplicate addresses in one network area.

The MAC addresses are assigned by the hardware manufacturer. MAC addresses are unique worldwide.

The following table shows the representation and the range of the address types:

Address Type	Format	Range	Example
IP Address	nnn.nnn.nnn.nnn	nnn: 0 to 255 (decimal)	192.168.11.110
MAC Address	mm:mm:mm:mm:mm:mm	mm: 00 to ff (hexadecimal number pairs)	A7:C9:89:DD:A9:B3

Table 4: Format and range of network addresses

■ Strings

A string is indicated by quotation marks. For example, “System name with space character”. Space characters are not valid user-defined strings. You enter a space character in a parameter between quotation marks.

Example:

```
*(EES)#cli prompt Device name
Error: Invalid command 'name'
```

```
*(EES)#cli prompt 'Device name'
```

```
*(Device name)#
```

■ Examples of commands

Example 1: clear arp-table-switch

Command for clearing the ARP table of the management agent (cache).

`clear arp-table-switch` is the command name. The command is executable without any other parameters by pressing the Enter key.

Example 2: radius server timeout

Command to configure the RADIUS server timeout value.

```
(EES) (config)#radius server timeout
<1..30> Timeout in seconds (default: 5).
```

`radius server timeout` is the command name.

The parameter is required. The value range is 1..30.

Example 3: radius server auth modify <1..8>

Command to set the parameters for RADIUS authentication server 1.

```
(EES) (config)#radius server auth modify 1
[name] RADIUS authentication server name.
[port] RADIUS authentication server port
      (default: 1812).
[msgauth] Enable or disable the message authenticator
          attribute for this server.
[primary] Configure the primary RADIUS server.
[status] Enable or disable a RADIUS authentication
         server entry.
[secret] Configure the shared secret for the RADIUS
         authentication server.
[encrypted] Configure the encrypted shared secret.
<cr> Press Enter to execute the command.
```

“radius server auth modify” is the command name.

The parameter <1..8> (RADIUS server index) is required. The value range is 1 to 8 (integer).

The parameters [name], [port], [msgauth], [primary], [status], [secret] and [encrypted] are optional.

C.3 Properties of the CLI

C.3.1 Input prompt

■ Command mode

With the input prompt, the CLI shows you which of the three modes you are in:

- ▶ (EES) >
User Exec mode
- ▶ (EES) #
Privileged Exec mode
- ▶ (EES) (config)#
Global Configuration mode
- ▶ (EES) (Vlan)#
VLAN Database Mode
- ▶ (EES) ((Interface)all)#
Interface Range Mode / Alle Ports des Gerätes
- ▶ (EES) ((Interface)2/1)#
Interface Range Mode / A single port on one interface
- ▶ (EES) ((Interface)1/2-1/4)#
Interface Range Mode / A range of ports on one interface
- ▶ (EES) ((Interface)1/2,1/4,1/5)#
Interface Range Mode / A list of single ports
- ▶ (EES) ((Interface)1/1-1/2,1/4-1/6)#
Interface Range Mode / A list of port ranges and single ports

■ Asterisk, pound sign and exclamation point

Asterisk “*”

An asterisk “*” in the first or second position of the input prompt shows you that the settings in the volatile memory and the settings in the non-volatile memory are different. In your configuration, the device has detected modifications which have not been saved.

```
*(EES) >
```

Pound sign “#”

A pound sign “#” at the beginning of the input prompt shows you that the boot parameters and the parameters during the boot phase are different.

```
*#(EES) >
```

Exclamation point „!”

An exclamation point „!” at the beginning of the input prompt shows: the password for the user or admin user account corresponds with the default setting.

```
!(EES) >
```

■ Wildcards

The device offers you the possibility to change the input prompt. The CLI supports the following wildcards:

Wildcard	Description
%d	System date.
%t	System time.
%i	IP address of the device.
%m	MAC address of the device.
%p	Product name of the device.

Table 5: Using wildcards within the CLI input prompt

```
!(EES)>enable
!(EES)#cli prompt %i
!10.100.10.100#cli prompt (EES)%d
!*(EES)2014-01-27#cli prompt (EES)%d%t
!*(EES)2014-01-2715:45:41#cli prompt %m
!*AA:BB:CC:DD:EE:FF#
```

C.3.2 Key combinations

The following key combinations make it easier for you to work with the Command Line Interface:

Key combination	Description
CTRL + H, Backspace	Delete previous character
CTRL + A	Go to beginning of line
CTRL + E	Go to end of line
CTRL + F	Go forward one character
CTRL + B	Go backward one character
CTRL + D	Delete current character
CTRL + U, X	Delete to beginning of line
CTRL + K	Delete to end of line
CTRL + W	Delete previous word
CTRL + P	Go to previous line in history buffer
CTRL + R	Rewrite or paste the line
CTRL + N	Go to next line in history buffer
CTRL + Z	Return to root command prompt
CTRL + G	Aborts running tcpdump session

Table 6: Key combinations in the Command Line Interface

Key combination	Description
Tab, <SPACE>	Command line completion
Exit	Go to next lower command prompt
?	List choices

Table 6: Key combinations in the Command Line Interface

The Help command displays the possible key combinations in CLI on the screen:

```
(EES) #help
HELP:
Special keys:

Ctrl-H, BkSp delete previous character
Ctrl-A .... go to beginning of line
Ctrl-E .... go to end of line
Ctrl-F .... go forward one character
Ctrl-B .... go backward one character
Ctrl-D .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K .... delete to end of line
Ctrl-W .... delete previous word
Ctrl-P .... go to previous line in history buffer
Ctrl-R .... rewrites or pastes the line
Ctrl-N .... go to next line in history buffer
Ctrl-Z .... return to root command prompt
Ctrl-G .... aborts running tcpdump session
Tab, <SPACE> command-line completion
Exit .... go to next lower command prompt
? .... list choices

(EES) #
```

Figure 16: Listing the key combinations with the Help command

C.3.3 Data entry elements

■ Command completion

To facilitate making entries, the CLI gives you the option of command completion (Tab Completion). Thus you are able to abbreviate key words.

- ▶ Type in the beginning of a keyword. If the characters entered identify a keyword, the CLI will complete the keyword when you press the tab key or the space key. If there is more than one option for completion, enter the letter or the letters being necessary for uniquely identifying the keyword. Press the tab key or the space key again. After that, the system completes the command or parameter.
- ▶ If you make a non-unique entry and press “Tab” or “Space” twice, the CLI provides you with a list of options.
- ▶ On a non-unique entry and pressing "Tab" or "Space", the CLI completes the command up to the end of the uniqueness. If several commands exist: When you press “Tab” or “Space” again, the CLI provides you with a list of options.

Example:

If you enter „lo“ and "Tab" or "Space"

```
(EES) (Config)#lo
```

the CLI completes the command up to the end of the uniqueness to „log“.

```
(EES) (Config)#log
```

When “Tab” or “Space” is pressed again, the CLI provides you with a list of options (logging, logout).

```
(EES) (Config)#log
```

```
logging logout
```

■ Possible commands/parameters

You can obtain a list of the commands or the possible parameters by entering “help” or “?”, for example by entering

```
(EES) >show ?
```

When you enter the command displayed, you get a list of the parameters available for the command `show`.

When you enter the command without space character in front of the question mark, the device displays the help text for the command itself:

```
!*#(EES)(Config)#show?
```

```
show          Display device options and settings.
```


D Examples

D.1 Saving the Configuration

To ensure that your password settings and your other configuration changes are kept after the device is reset or after an interruption of the voltage supply, you save the configuration. To save your current configuration, you proceed as follows:

- Enter `enable` to switch to the Privileged Exec mode.
- Enter the following command:
`save [profile]`
- Execute the command by pressing the Enter key.

```
(EES)>enable
```

```
!*(EES)#s?
```

```
save          Save configuration.
script        CLI Script File.
serviceshell Enter system mode.
show          Display device options and settings.
```

```
!*(EES)#save?
```

```
[profile]     Save configuration to profile.
<cr>         Press Enter to execute the command.
```

D.2 Syntax of the „radius server auth add“ command

Use this command to add a RADIUS authentication server.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
 [name]: RADIUS authentication server name.
 [port]: RADIUS authentication server port (default: 1813).

Parameter	Meaning	Possible values
<1..8>	RADIUS server index.	1..8
<a.b.c.d>	RADIUS accounting server IP address.	IP address
<string>	Enter a user-defined text, max. 32 characters.	
<1..65535>	Enter port number between 1 and 65535.	1..65535

Mode and Privilege Level:

- ▶ You need to be in Global Config mode to be able to execute the command (see chapter [“Mode-based command hierarchy”](#)).
- ▶ You need to have Administrator Privilege Level to be able to execute the command.

Syntax of commands and parameters:

See table [\(see table 2\)](#)

Examples for executable commands:

- ▶ `radius server auth add 1 ip 10.115.30.40`
- ▶ `radius server auth add 2 ip 10.115.40.50 name radius-server2`
- ▶ `radius server auth add 3 ip 10.115.50.60 port 1813`
- ▶ `radius server auth add 4 ip 10.115.60.70 name radius-server4 port 1814`

E Maintenance

Hirschmann are continually working on improving and developing their software. Check regularly whether there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet (<http://www.hirschmann.com>).

E.1 Service Shell

A service technician uses the Service Shell function for maintenance of your functioning device. If you need service support, this function allows the service technician to access internal functions of your device from an external location.

Note: The Service Shell function is for service purposes exclusively. This function allows the access on internal functions of the device. In no case, execute internal functions without service technician instructions. Executing internal functions such as deleting the content of the NVM (non-volatile memory) possibly leads to inoperability of your device.

Note: When the Service Shell function is active, the CLI timeout function will be inactive.

Note: To prevent configuration inconsistencies, log out from the Service Shell function before any other user starts uploading a new configuration to the device.

- To switch from the User Exec mode to the Privileged Exec mode, enter `enable` or `en` and a space, and press the enter key.
- To get a list of the commands available in this mode, enter a question mark `?`.
- To start the Shell Service function, enter `serviceshell` or `ser` in the privileged exec mode and a space and then press the enter key.
- To end the Shell Service function, enter `exit` and then press the enter key.

```
!(EES) >enable

!(EES) #?
clear          Clear several items.
configure     Enter into global config mode.
copy          Copy different kinds of items.
debug         Service functions to find configuration errors.
exit          Exit from current mode.
help          Display help for various special keys.
history       Show a list of previously run commands.
login         Set login parameters.
logout        Exit this session.
network       Modify network parameters.
ping          Send ICMP echo packets to a specified
              IP address.

profile       Activate or delete configuration profiles.
reboot        Reset the device (cold start).
save          Save configuration.
serviceshell Enter system mode.
set           Set device parameters.
show          Display device options and settings.
traceroute    Trace route to a specified host.

!(EES) #serviceshell

-> exit
Au revoir!

!*(EES) #
```

■ Permanently disabling the Service Shell

If you do not need the Service Shell, the device allows you to disable the function. In this case you still have the option to configure the device. Though, the service technician has no possibilities to access internal functions of your device to call up additional required information.

Note:

Disabling the Service Shell function produces a permanent effect. To reactivate the Service Shell function, send the device back to the manufacturer.

- To display the Service Shell function, enter `serviceshell` or `ser` and a space, and then a question mark `?` .
- To permanently deactivate the Shell Service function, enter `deactivate` or `d` and a space, and press the enter key. This process is irreversible.

```
!(EES) >enable

!(EES) #serviceshell?
[deactivate]          Disable the service shell access permanently
                       (Cannot be undone).
<cr>                  Press Enter to execute the command.

!(EES) #serviceshell deactivate
```

Command reference

1 Address Conflict Detection (ACD)

1.1 address-conflict

Configure the address conflict settings.

1.1.1 address-conflict operation

Enable or disable the address conflict component.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict operation

■ no address-conflict operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no address-conflict operation

1.1.2 address-conflict detection-mode

Configure the detection mode.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict detection-mode <P-1>

Parameter	Value	Meaning
P-1	active-and-passive	Configure active and passive detection. During ip address configuration 'active' is sending ARP or NDP probes into the network and 'passive' is listening continuously on the network.
	active-only	Configure only active detection. During ip address configuration 'active' is sending once ARP or NDP probes into the network.
	passive-only	Configure passive detection. The device listens passively on the network if another device with an already locally configured ip address appears.

1.1.3 address-conflict detection-ongoing

Enable or disable the ongoing detection. If enabled, the device sends periodic ARP or NDP probes.

- ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: address-conflict detection-ongoing
-
- no address-conflict detection-ongoing
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no address-conflict detection-ongoing

1.1.4 address-conflict delay

The maximum detection delay time in milliseconds. Time gap between ARP or NDP probes.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict delay <P-1>

Parameter	Value	Meaning
P-1	20..500	Time gap between ARP or NDP probes ([ms], default 200).

1.1.5 address-conflict release-delay

Delay in seconds to the next ARP or NDP probe cycle after an ip address conflict was detected.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict release-delay <P-1>

Parameter	Value	Meaning
P-1	3..3600	Delay between probe cycles after conflict detection ([sec], default 15).

1.1.6 address-conflict max-protection

Maximum number of frequent address protections.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict max-protection <P-1>

Parameter	Value	Meaning
P-1	0..100	Maximum number of frequent address protections (default 3).

1.1.7 address-conflict protect-interval

Delay in milliseconds between two protections.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict protect-interval <P-1>

Parameter	Value	Meaning
P-1	20..5000	Delay between two protections ([ms], default 200).

1.1.8 address-conflict trap-status

If enabled this trap reports an address conflict.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict trap-status

■ no address-conflict trap-status

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no address-conflict trap-status

1.2 show

Display device options and settings.

1.2.1 show address-conflict global

Displays the component mode.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show address-conflict global

1.2.2 show address-conflict detected

Displays the last detected address conflict.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show address-conflict detected

1.2.3 show address-conflict fault-state

Displays the current conflict status.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show address-conflict fault-state

2 Application Lists

2.1 appllists

Configure an application list.

2.1.1 appllists set-authlist

Set an authentication list reference that shall be used by given application.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `appllists set-authlist <P-1> <P-2>`

Parameter	Value	Meaning
P-1	string	<application> Name of an application list.
P-2	string	<authlist_name> Name of referenced authentication list.

2.1.2 appllists enable

Activate a login application list.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `appllists enable <P-1>`

Parameter	Value	Meaning
P-1	string	<application> Name of an application list.

2.1.3 appllists disable

Deactivate a login application list.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** appllists disable <P-1>

Parameter	Value	Meaning
P-1	string	<application> Name of an application list.

2.2 show

Display device options and settings.

2.2.1 show appllists

Display ordered methods for application lists.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show appllists

3 Authentication Lists

3.1 authlists

Configure an authentication list.

3.1.1 authlists add

Create a new login authentication list.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `authlists add <P-1>`

Parameter	Value	Meaning
P-1	string	<authlist_name> Name of an authentication list.

3.1.2 authlists delete

Delete an existing login authentication list.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `authlists delete <P-1>`

Parameter	Value	Meaning
P-1	string	<authlist_name> Name of an authentication list.

3.1.3 authlists set-policy

Set the policies of a login authentication list.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `authlists set-policy <P-1> <P-2> [<P-3>] [<P-4>] [<P-5>] [<P-6>]`

Parameter	Value	Meaning
P-1	string	<authlist_name> Name of an authentication list.
P-2	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
P-3	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
P-4	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
P-5	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
P-6	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server

3.1.4 authlists enable

Activate a login authentication list.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `authlists enable <P-1>`

Parameter	Value	Meaning
P-1	string	<authlist_name> Name of an authentication list.

3.1.5 authlists disable

Deactivate a login authentication list.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: authlists disable <P-1>

Parameter	Value	Meaning
P-1	string	<authlist_name> Name of an authentication list.

3.2 show

Display device options and settings.

3.2.1 show authlists

Display ordered methods for authentication lists.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show authlists

4 Auto Disable

4.1 auto-disable

Configure the Auto Disable condition settings.

4.1.1 auto-disable reason

Enables/disables port Recovery by reason on this device.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: auto-disable reason <P-1>

Parameter	Value	Meaning
P-1	link-flap	Enable/disable link-flap
	crc-error	Enable/disable crc-error
	duplex-mismatch	Enable/disable duplex-mismatch
	bpdu-rate	Enable/disable bpdu-rate
	port-security	Enable/disable MAC based port security

- no auto-disable reason
 - Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no auto-disable reason

4.2 auto-disable

Configure the Auto Disable condition settings.

4.2.1 auto-disable timer

Timer value in seconds after a deactivated port is activated again. Possible values are: 30-4294967295. A value of 0 disables the timer.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: auto-disable timer <P-1>

Parameter	Value	Meaning
P-1	0..4294967295	Enter a number in the given range. Possible values are: 30-4294967295. A value of 0 disables the timer.

4.2.2 auto-disable reset

Reset the specific interface and reactivate the port

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: auto-disable reset

■ no auto-disable reset

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no auto-disable reset

4.3 show

Display device options and settings.

4.3.1 show auto-disable brief

Display Auto Disable summary by interface.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show auto-disable brief

4.3.2 show auto-disable reasons

Display summary of Auto Disable error reasons

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show auto-disable reasons

5 Class Of Service

5.1 classofservice

Class of service configuration.

5.1.1 classofservice ip-dscp-mapping

ip-dscp-mapping configuration

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `classofservice ip-dscp-mapping <P-1> <P-2> <P-3>`

Parameter	Value	Meaning
P-1	af11	
	af12	
	af13	
	af21	
	af22	
	af23	
	af31	
	af32	
	af33	
	af41	
	af42	
	af43	
	be	
	cs0	
	cs1	
	cs2	
	cs3	
	cs4	
	cs5	
	cs6	
	cs7	
	ef	
	0	
	1	
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		

Parameter	Value	Meaning
P-2	0..7	Enter the Traffic Class value.
P-3	0..3	Enter the Traffic Class value.

5.1.2 classofservice dot1p-mapping

Enter a VLAN priority and the traffic class it should be mapped to.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: classofservice dot1p-mapping <P-1> <P-2> <P-3>

Parameter	Value	Meaning
P-1	0..7	Enter the 802.1p priority.
P-2	0..7	Enter the Traffic Class value.
P-3	0..3	Enter a number in the given range.

5.2 classofservice

Interface classofservice configuration.

5.2.1 classofservice trust

trust configuration

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: classofservice trust <P-1>

Parameter	Value	Meaning
P-1	untrusted	Sets the class of service trust mode to untrusted
	dot1p	Sets the class of service trust mode to dot1p.
	ip-dscp	Sets the class of service trust mode to IP DSCP.

5.3 cos-queue

COS queue configuration

5.3.1 cos-queue strict

strict priority scheduler (default)

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `cos-queue strict <P-1> <P-2>`

Parameter	Value	Meaning
P-1	0..7	Enter a Queue Id from 0 to 7.
P-2	0..3	Enter a number in the given range.

5.3.2 cos-queue weighted

weighted scheduler

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `cos-queue weighted <P-1> <P-2>`

Parameter	Value	Meaning
P-1	0..7	Enter a Queue Id from 0 to 7.
P-2	0..3	Enter a number in the given range.

5.3.3 cos-queue min-bandwidth

Minimum/guaranteed bandwidth for the queues when in weighted mode

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `cos-queue min-bandwidth <P-1> <P-2> <P-3>`

Parameter	Value	Meaning
P-1	0..3	Enter a number in the given range.
P-2	0..7	Enter a Queue Id from 0 to 7.
P-3	0..100	Enter a number in the given range.

5.4 show

Display device options and settings.

5.4.1 show classofservice ip-dscp-mapping

Show ip-dscp-mapping configuration.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show classofservice ip-dscp-mapping

5.4.2 show classofservice dot1p-mapping

Display a table containing the vlan priority to traffic class mappings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show classofservice dot1p-mapping

5.4.3 show classofservice trust

Show a table containing the trust mode of all interfaces.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show classofservice trust

5.4.4 show cos-queue

Show cosqueue parameters

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show cos-queue

6 Command Line Interface (CLI)

6.1 cli

Set the CLI preferences.

6.1.1 cli serial-timeout

Set login timeout for serial line connection to CLI.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `cli serial-timeout <P-1>`

Parameter	Value	Meaning
P-1	0..160	Enter a number in the given range.

6.1.2 cli prompt

Change the system prompt. Following wildcards are allowed:

`%d` date, `%t` time, `%i` IP address, `%m` MAC address, `%p` productname

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `cli prompt <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters. Following wildcards are allowed: <code>\n %d</code> date, <code>%t</code> time, <code>%i</code> IP address, <code>%m</code> MAC address, <code>%p</code> productname

6.1.3 cli numlines

Set the number of lines for 'more'.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** cli numlines <P-1>

Parameter	Value	Meaning
P-1	0..250	Screen size for 'more' (23 = default, 0 = unlimited).

6.1.4 cli banner operation

Enable or disable the CLI login banner.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** cli banner operation

■ no cli banner operation

Disable the option

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no cli banner operation

6.1.5 cli banner text

Set the text for the CLI login banner (C printf format syntax allowed: \n \t).

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `cli banner text <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 1024 characters (allowed characters are from ASCII 32 to 127).

6.2 show

Display device options and settings.

6.2.1 show cli global

Display CLI preferences.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show cli global

6.2.2 show cli command-tree

Show a list of all commands.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show cli command-tree

6.3 logging

Logging configuration.

6.3.1 logging cli-command

Enable or disable the CLI command logging.

- ▶ **Mode:** Global Config Mode
 - ▶ **Privilege Level:** Administrator
 - ▶ **Format:** logging cli-command
-
- **no logging cli-command**
Disable the option
 - ▶ **Mode:** Global Config Mode
 - ▶ **Privilege Level:** Administrator
 - ▶ **Format:** no logging cli-command

6.4 show

Display device options and settings.

6.4.1 show logging cli-command

Show the CLI command logging preferences.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show logging cli-command

7 Clock

7.1 clock

Configure local and DST clock settings.

7.1.1 clock set

Edit current local time.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `clock set <P-1> <P-2>`

Parameter	Value	Meaning
P-1	YYYY-MM-DD	Local date (range: 2004-01-01 - 2037-12-31).
P-2	HH:MM:SS	Local time.

7.1.2 clock timezone offset

Local time offset (in minutes) with respect to UTC (positive values for locations east of Greenwich).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `clock timezone offset <P-1>`

Parameter	Value	Meaning
P-1	-780..840	Edit the timezone offset (in minutes).

7.1.3 clock timezone zone

Edit the timezone acronym (max. 4 characters).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock timezone zone <P-1>

Parameter	Value	Meaning
P-1	string	Edit the timezone acronym (max 4 characters).

7.1.4 clock summer-time mode

Configure summer-time mode parameters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock summer-time mode <P-1>

Parameter	Value	Meaning
P-1	disable	Disable recurring summer-time mode.
	recurring	Enable recurring summer-time mode.
	eu	Enable recurring summer-time used in most parts of the European Union.
	usa	Enable recurring summer-time used in most parts of the USA.

7.1.5 clock summer-time recurring start

Edit the starting date and time for daylight saving time.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock summer-time recurring start <P-1> <P-2> <P-3> <P-4>

Parameter	Value	Meaning
P-1	none	
	first	
	second	
	third	
	fourth	
	last	
P-2	none	
	sun	Sunday
	mon	Monday
	tue	Tuesday
	wed	Wednesday
	thu	Thursday
	fri	Friday
	sat	Saturday
P-3	none	
	jan	January
	feb	February
	mar	March
	apr	April
	may	May
	jun	June
	jul	July
	aug	August
	sep	September
	oct	October
	nov	November
dec	December	
P-4	string	<hh:mm> Present time in hh:mm format (00:00-23:59).

7.1.6 clock summer-time recurring end

Edit the ending date and time for daylight saving time.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock summer-time recurring end <P-1> <P-2> <P-3> <P-4>

Parameter	Value	Meaning
P-1	none	
	first	
	second	
	third	
	fourth	
	last	
P-2	none	
	sun	Sunday
	mon	Monday
	tue	Tuesday
	wed	Wednesday
	thu	Thursday
	fri	Friday
	sat	Saturday
P-3	none	
	jan	January
	feb	February
	mar	March
	apr	April
	may	May
	jun	June
	jul	July
	aug	August
	sep	September
	oct	October
	nov	November
	dec	December
P-4	string	<hh:mm> Present time in hh:mm format (00:00-23:59).

7.1.7 clock summer-time zone

Edit timezone acronym for summer-time (max. 4 characters).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock summer-time zone <P-1>

Parameter	Value	Meaning
P-1	string	Edit the timezone acronym (max 4 characters).

7.2 show

Display device options and settings.

7.2.1 show clock

Display the current time information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** `show clock [summer-time]`
`[summer-time]`: Display summer-time parameters.

8 Configuration

8.1 save

Save configuration.

8.1.1 save profile

Save configuration to profile.

- ▶ Mode: All Privileged Modes
- ▶ Privilege Level: Operator
- ▶ Format: save profile <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

8.2 config

Configure the Configuration Saving settings.

8.2.1 config watchdog admin-state

Enable or disable the Configuration Undo feature.

- ▶ **Mode:** Global Config Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** config watchdog admin-state
-
- **no config watchdog admin-state**
Disable the option
 - ▶ **Mode:** Global Config Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** no config watchdog admin-state

8.2.2 config watchdog timeout

Configure the Configuration Undo timeout (unit: seconds).

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** config watchdog timeout <P-1>

Parameter	Value	Meaning
P-1	30..600	Enter a number in the given range.

8.2.3 config encryption password set

Set the configuration file password.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: config encryption password set [<P-1>] [<P-2>]

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 64 characters.
P-2	string	Enter a user-defined text, max. 64 characters.

8.2.4 config encryption password clear

Clear the configuration file password.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: config encryption password clear [<P-1>]

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 64 characters.

8.2.5 config profile select

Select a configuration profile to be the active one.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: config profile select <P-1> <P-2>

Parameter	Value	Meaning
P-1	nvm	You can only select nvm for this command.
P-2	1..20	Index of the profile entry.

8.2.6 config profile delete

Delete configuration profile.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** config profile delete <P-1> num <P-2> profile <P-3>

num: Select the index of the profile to delete.

profile: Select the name of the profile to delete.

Parameter	Value	Meaning
P-1	nvm	non-volatile memory
P-2	1..20	Index of the profile entry.
P-3	string	Enter a user-defined text, max. 32 characters.

8.2.7 config fingerprint verify

Verify the fingerprint of the selected profile.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** config fingerprint verify <P-1> profile <P-2> <P-3> num <P-4> <P-5>

profile: Select name of profile to be verified.

num: Select index of profile to be verified.

Parameter	Value	Meaning
P-1	nvm	non-volatile memory
P-2	string	Enter a user-defined text, max. 32 characters.
P-3	string	Enter hash as 40 hexa-decimal characters.
P-4	1..20	Index of the profile entry.
P-5	string	Enter hash as 40 hexa-decimal characters.

8.3 copy

Copy different kinds of items.

8.3.1 copy firmware remote

Copy firmware image from server.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy firmware remote <P-1> system
system: Copy firmware from file server to system memory.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

8.3.2 copy firmware system remote

Copy firmware to file server.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: copy firmware system remote <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

8.3.3 copy config running-config nvm

Save running-config to nv memory.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** copy config running-config nvm [profile <P-1>]
[profile]: Save configuration to profile.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

8.3.4 copy config running-config remote

Save running-config to file server.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** copy config running-config remote <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

8.3.5 copy config nvm

Load configuration from NV memory.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** copy config nvm [profile <P-1>] running-config
remote <P-2>

[profile]: Load configuration from profile.

running-config: (Re)-load configuration from NV memory.

remote: Copy configuration from nvm to server.

Parameter	Value	Meaning
P-1	string	Filename.
P-2	string	Enter a user-defined text, max. 128 characters.

8.3.6 copy config remote

Copy configuration file from server.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `copy config remote <P-1> nvm [profile <P-2>] running-config`

`nvm`: Copy configuration file from server to NV memory.

`[profile]`: Copy configuration from server to named NV memory profile.

`running-config`: Copy configuration file from server to running-config.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 32 characters.

8.4 clear

Clear several items.

8.4.1 clear config

Clear running configuration.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clear config

8.4.2 clear factory

Set device back to factory settings (use with care).

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clear factory

8.5 show

Display device options and settings.

8.5.1 show running-config xml

Show the currently running configuration (XML file).

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show running-config xml

8.5.2 show running-config script

Show the currently running configuration (CLI script).

- ▶ **Mode:** Command is in all modes available.
 - ▶ **Privilege Level:** Administrator
 - ▶ **Format:** show running-config script [all]
- [all]: Show the currently running configuration (CLI script).

8.6 show

Display device options and settings.

8.6.1 show config watchdog

Show the Auto Configuration Undo settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show config watchdog

8.6.2 show config encryption

Show the settings for config encryption.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show config encryption

8.6.3 show config profiles

Show configuration profiles.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show config profiles <P-1> [<P-2>]

Parameter	Value	Meaning
P-1	nvm	non-volatile memory
P-2	1..20	Index of the profile entry.

8.6.4 show config status

Show sync Status of running-config with NVM and ACA.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show config status

9 Debugging

9.1 debug

Different tools to assist in debugging the device.

9.1.1 debug tcpdump help

Display help file for the tcpdump tool.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: debug tcpdump help

9.1.2 debug tcpdump start cpu

Start capture with default values.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: debug tcpdump start cpu [filter <P-1>] [parms <P-2>]

[filter]: Start capture with values from a filter file.

[parms]: Start capture with the tcpdump parameters (for details see tcpdump help).

Parameter	Value	Meaning
P-1	string	<filename> Enter a valid filename.
P-2	string	Enter a user-defined text, max. 255 characters.

9.1.3 debug tcpdump stop

Abort capture of network traffic.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: debug tcpdump stop

9.1.4 debug tcpdump filter show

Display a known filter file.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: debug tcpdump filter show <P-1>

Parameter	Value	Meaning
P-1	string	<filename> Enter a valid filename.

9.1.5 debug tcpdump filter list

Display all available filter files.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: debug tcpdump filter list

9.1.6 debug tcpdump filter delete

Delete a known filter file.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: debug tcpdump filter delete <P-1>

Parameter	Value	Meaning
P-1	string	<filename> Enter a valid filename.

9.2 copy

Copy different kinds of items.

9.2.1 copy tcpdumpcap nvm remote

Copy internal capture file from device to the server.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `copy tcpdumpcap nvm remote <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

9.2.2 copy tcpdumpfilter remote

Copy filter file from one memory location to another.

- ▶ Mode: Privileged Exec Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: `copy tcpdumpfilter remote <P-1> nvm <P-2>`
- nvm: Copy filter file from server to non-volatile memory.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	<filename> Enter a valid filename.

9.2.3 copy tcpdumpfilter nvm

Copy capture filter from non-volatile memory.

▶ **Mode:** Privileged Exec Mode

▶ **Privilege Level:** Operator

▶ **Format:** copy tcpdumpfilter nvm <P-1> remote <P-2>

remote: Copy capture file from non-volatile memory to the server.

Parameter	Value	Meaning
P-1	string	Filename.
P-2	string	Enter a user-defined text, max. 128 characters.

10 Device Monitoring

10.1 device-status

Configure various device conditions to be monitored.

10.1.1 device-status monitor link-failure

Enable or disable monitor state of network connection(s).

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** device-status monitor link-failure

■ no device-status monitor link-failure

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no device-status monitor link-failure

10.1.2 device-status monitor ring-redundancy

Enable or disable monitoring if ring-redundancy is present.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** device-status monitor ring-redundancy

■ no device-status monitor ring-redundancy

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no device-status monitor ring-redundancy

10.1.3 device-status trap

Configure the device to send a trap when the device status\nchanges.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** device-status trap

■ no device-status trap

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no device-status trap

10.2 device-status

Configure various device conditions to be monitored.

10.2.1 device-status link-alarm

Configure the monitor settings of the port link.

- ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Administrator
 - ▶ **Format:** device-status link-alarm
-
- **no device-status link-alarm**
Disable the option
 - ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Administrator
 - ▶ **Format:** no device-status link-alarm

10.3 show

Display device options and settings.

10.3.1 show device-status monitor

Display the device monitoring configurations.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show device-status monitor

10.3.2 show device-status state

Display the current state of the device.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show device-status state

10.3.3 show device-status trap

Display the device trap information and configurations.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show device-status trap

10.3.4 show device-status events

Display occurred device status events.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show device-status events

10.3.5 show device-status link-alarm

Display the monitor configurations of the network ports.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show device-status link-alarm

10.3.6 show device-status all

Display the configurable device status settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show device-status all

11 Device Security

11.1 security-status

Configure the security status settings.

11.1.1 security-status monitor pwd-change

Sets the monitoring of default password change for\n'n'user' and 'admin'.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor pwd-change

■ no security-status monitor pwd-change

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor pwd-change

11.1.2 security-status monitor pwd-min-length

Sets the monitoring of minimum length of the password\n(smaller 8).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor pwd-min-length

■ no security-status monitor pwd-min-length

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status monitor pwd-min-length

11.1.3 security-status monitor pwd-policy-config

Sets the monitoring whether the minimum password policy is configured. The device changes the security status to the value "error" if the value for at least one of the following password rules is 0:\n"minimum upper cases", "minimum lower cases", "minimum numbers", "minimum special characters".

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** security-status monitor pwd-policy-config

■ no security-status monitor pwd-policy-config

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status monitor pwd-policy-config

11.1.4 security-status monitor pwd-policy-inactive

Sets the monitoring whether at least one user is configured with inactive policy check. The device changes the security status to the value "error" if the function "policy check" is inactive for at least 1 user account.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** security-status monitor pwd-policy-inactive

■ no security-status monitor pwd-policy-inactive

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status monitor pwd-policy-inactive

11.1.5 security-status monitor telnet-enabled

Sets the monitoring of the activation of telnet on the switch.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** security-status monitor telnet-enabled

■ no security-status monitor telnet-enabled

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status monitor telnet-enabled

11.1.6 security-status monitor http-enabled

Sets the monitoring of the activation of http on the switch.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** security-status monitor http-enabled

■ no security-status monitor http-enabled

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status monitor http-enabled

11.1.7 security-status monitor snmp-unsecure

Sets the monitoring of SNMP security (SNMP v1/v2 is enabled or v3 encryption is disabled).

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** security-status monitor snmp-unsecure

■ no security-status monitor snmp-unsecure

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status monitor snmp-unsecure

11.1.8 security-status monitor sysmon-enabled

Sets the monitoring of the activation of System Monitor 1 on the switch.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** security-status monitor sysmon-enabled

■ no security-status monitor sysmon-enabled

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status monitor sysmon-enabled

11.1.9 security-status monitor no-link-enabled

Sets the monitoring of no link detection.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** security-status monitor no-link-enabled

■ no security-status monitor no-link-enabled

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status monitor no-link-enabled

11.1.10 security-status monitor hidisc-write-enabled

Sets the monitoring of HiDiscovery write enabled.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** security-status monitor hidisc-write-enabled

■ no security-status monitor hidisc-write-enabled

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status monitor hidisc-write-enabled

11.1.11 security-status monitor iec61850-mms-enabled

Sets the monitoring of the activation of IEC 61850 MMS on the switch.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** security-status monitor iec61850-mms-enabled

■ no security-status monitor iec61850-mms-enabled

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status monitor iec61850-mms-enabled

11.1.12 security-status monitor https-certificate

Sets the monitoring whether auto generated self-signed HTTPS certificate is in use.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** security-status monitor https-certificate

■ no security-status monitor https-certificate

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status monitor https-certificate

11.1.13 security-status trap

Configure if a trap is sent when the security status changes.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** security-status trap

■ no security-status trap

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no security-status trap

11.2 security-status

Configure the security status interface settings.

11.2.1 security-status no-link

Configure the monitoring of the specific ports.

- ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Administrator
 - ▶ **Format:** security-status no-link
-
- **no security-status no-link**
Disable the option
 - ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Administrator
 - ▶ **Format:** no security-status no-link

11.3 show

Display device options and settings.

11.3.1 show security-status monitor

Display the security status monitoring settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show security-status monitor

11.3.2 show security-status state

Display the current security status.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show security-status state

11.3.3 show security-status no-link

Display the settings of the monitoring of the specific\nnetwork ports.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show security-status no-link

11.3.4 show security-status trap

Display the security status trap information and settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show security-status trap

11.3.5 show security-status events

Display occurred security status events.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show security-status events

11.3.6 show security-status all

Display all security status settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show security-status all

12 Differentiated Services (DiffServ)

12.1 diffserv

Enable or disable DiffServ.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** diffserv

12.2 class-map

Manage DiffServ classes.

12.2.1 class-map name

Configure a Diffserv class.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** class-map name <P-1> match any ethertype <P-2> cos <P-3> secondary-cos <P-4> destination-address <P-5> <P-6> <P-7> source-address <P-8> <P-9> <P-10> dstip <P-11> <P-12> srcip <P-13> <P-14> dstl4port <P-15> srcl4port <P-16> ip dscp <P-17> precedence <P-18> tos <P-19> <P-20> protocol <P-21> vlan <P-22> secondary-vlan <P-23> class-map <P-24> <P-25>

match: Add a match rule for the class.

any: Match any packet.

ethertype: Add a match condition based on the ethertype value.

cos: Add a match condition based on the COS value.

secondary-cos: Add a match condition based on the secondary COS value.

destination-address: Add a match condition based on the destination mac address.

source-address: Add a match condition based on the source mac address.

dstip: Add a match condition based on the destination IPv4 address.

srcip: Add a match condition based on the source IP address.

dstl4port: Add a match condition based on the layer 4 destination port.

srcl4port: Add a match condition based on the layer 4 source port.

ip: Add a match condition based on IP DSCP, precedence or TOS fields.

dscp: Add a match condition based on the IP DSCP field.

precedence: Add a match condition based on the IP precedence field.

tos: Add a match condition based on the IP TOS field.

protocol: Add a match condition based on the IP protocol field.

vlan: Add a match condition based on the VLAN field.

secondary-vlan: Add a match condition based on the secondary VLAN field.

class-map: Add/remove a set of match condition defined for another class.

Parameter	Value	Meaning
P-1	string	Enter the DiffServ class name, max. 31 characters.
P-2	0x0600-0xffff	ethertype
	appletalk	appletalk
	arp	arp
	ibmsna	ibmsna
	ipv4	ipv4
	ipv6	ipv6
	ipx	ipx
	mplsmcast	mplsmcast
	mplsucast	mplsucast
	netbios	netbios
	novell	novell
	pppoe	pppoe
	rarp	rarp
P-3	0..7	COS value.
P-4	0..7	COS value.
P-5	mac	mac.
P-6	aa:bb:cc:dd:ee:ff	MAC address.
P-7	mac	MAC mask.
P-8	mac	mac.
P-9	aa:bb:cc:dd:ee:ff	MAC address.
P-10	mac	MAC mask.
P-11	A.B.C.D	IP address.
P-12	<a.b.c.d>	IP subnet mask.
P-13	A.B.C.D	IP address.
P-14	<a.b.c.d>	IP subnet mask.
P-15	domain	domain
	echo	echo
	ftp	ftp
	ftpdata	ftpdata
	http	http
	smtp	smtp
	snmp	snmp
	telnet	telnet
	tftp	tftp
	www	www
	0-65535	Port number

Parameter	Value	Meaning
P-16	domain	domain
	echo	echo
	ftp	ftp
	ftpdata	ftpdata
	http	http
	smtp	smtp
	snmp	snmp
	telnet	telnet
	tftp	tftp
	www	www
	0-65535	Port number
P-17	0-63	Decimal value
	af11	af11
	af12	af12
	af13	af13
	af21	af21
	af22	af22
	af23	af23
	af31	af31
	af32	af32
	af33	af33
	af41	af41
	af42	af42
	af43	af43
	be	be
	cs0	cs0
	cs1	cs1
	cs2	cs2
	cs3	cs3
	cs4	cs4
	cs5	cs5
	cs6	cs6
	cs7	cs7
	ef	ef
	P-18	0..7
P-19	string	<00-ff> Tos bits/mask.
P-20	string	<00-ff> Tos bits/mask.
P-21	icmp	icmp
	igmp	igmp
	ip	ip
	tcp	tcp
	udp	udp
	0-255	Protocol number

Parameter	Value	Meaning
P-22	1..4042	Enter the VLAN ID.
P-23	1..4042	Enter the VLAN ID.
P-24	string	Enter the DiffServ class name, max. 31 characters.
P-25	enable	Enable the option.
	disable	Disable the option.

12.2.2 class-map rename

Rename an existing class.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `class-map rename <P-1> <P-2>`

Parameter	Value	Meaning
P-1	string	Enter the DiffServ class name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.

12.2.3 class-map match-all

Create a new match-all class.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `class-map match-all <P-1>`

Parameter	Value	Meaning
P-1	string	Enter the DiffServ class name, max. 31 characters.

12.2.4 class-map remove

Remove a Diffserv class.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** class-map remove <P-1>

Parameter	Value	Meaning
P-1	string	Enter the DiffServ class name, max. 31 characters.

12.3 policy-map

Manage DiffServ policies.

12.3.1 policy-map create

Create a DiffServ policy.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `policy-map create <P-1> { in | out }`

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	in	Traffic direction in.
P-2	out	Traffic direction out.

12.3.2 policy-map name class add

Configure a Diffserv policy.

- ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: `policy-map name <string> class add <string>`
- class: Manage DiffServ policy-class instances.
add: Add a policy-class instance.

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.

12.3.3 policy-map name class name assign-queue

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** policy-map name <string> class name <string>
assign-queue <0..7>

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

assign-queue: Modify the queue id to which the associated traffic stream is assigned.

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	0..7	Assign queue id.

12.3.4 policy-map name class name conform-color

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** policy-map name <string> class name <string>
conform-color <string>

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

conform-color: Enable color-aware traffic policing and define the conform-color class.

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	string	Enter the DiffServ class name, max. 31 characters.

12.3.5 policy-map name class name drop

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** policy-map name <string> class name <string>
drop

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

drop: All packets for the associated traffic stream are dropped at ingress.

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.

12.3.6 policy-map name class name mark

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** policy-map name <string> class name <string>

```
mark {cos <0..7> |
      cos-as-sec-cos |
      ip-dscp <af11|af12|af13|af21|af22|
              af23|af31|af32|af33|af41|
              af42|af43|be|cs0|cs1|cs2|
              cs3|cs4|cs5|cs6|cs7|ef> |
      ip-precedence <0..7>}
```

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

mark: Add a mark attribute.

cos: Marks all packets with the specified COS value.

cos-as-sec-cos: Use secondary COS as COS.

ip-dscp: Marks all packets with the specified IP DSCP value.

ip-precedence: Marks all packets with the specified IP precedence value.

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	0..7	COS value.

Parameter	Value	Meaning
P-4	af11	af11
	af12	af12
	af13	af13
	af21	af21
	af22	af22
	af23	af23
	af31	af31
	af32	af32
	af33	af33
	af41	af41
	af42	af42
	af43	af43
	be	be
	cs0	cs0
	cs1	cs1
	cs2	cs2
	cs3	cs3
	cs4	cs4
	cs5	cs5
	cs6	cs6
cs7	cs7	
ef	ef	
P-5	0..7	Ip precedence value.

12.3.7 policy-map name class name mirror

Configure a Diffserv policy.

► Mode: Global Config Mode

► Privilege Level: Operator

► Format: `policy-map name <string> class name <string>`

```
mirror < 1/1 | 1/2 | 1/3 | 1/4 | 2/1 |
          2/2 | 2/3 | 2/4 | 3/1 | 3/2 |
          3/3 | 3/4 | 4/1 | 4/2 | 4/3 |
          4/4 | 5/1 | 5/2 | 5/3 | 5/4 >
```

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

mirror: All incoming packets for the associated traffic stream are copied to a specific egress interface.

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	1/1	slot 1 / port 1
	1/2	slot 1 / port 2
	1/3	slot 1 / port 3
	1/4	slot 1 / port 4
	2/1	slot 2 / port 1
	2/2	slot 2 / port 2
	2/3	slot 2 / port 3
	2/4	slot 2 / port 4
	3/1	slot 3 / port 1
	3/2	slot 3 / port 2
	3/3	slot 3 / port 3
	3/4	slot 3 / port 4
	4/1	slot 4 / port 1
	4/2	slot 4 / port 2
	4/3	slot 4 / port 3
	4/4	slot 4 / port 4
	5/1	slot 5 / port 1
	5/2	slot 5 / port 2
	5/3	slot 5 / port 3
	5/4	slot 5 / port 4
	lag/1	lag instance 1
	lag/2	lag instance 2

12.3.8 policy-map name class name police-simple conform action drop violate-action

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:**

```

policy-map name <string> class name <string>
  police-simple
    < 1..4294967295> <1..128> conform-action
      drop violate-action
        {drop |
          set-cos-as-sec-cos |
          set-cos-transmit <0..7> |
          set-dscp-transmit
            <af11|af12|af13|af21|af22|
              af23|af31|af32|af33|af41|
                af42|af43|be|cs0|cs1|cs2|
                  cs3|cs4|cs5|cs6|cs7|ef> |
          set-prec-transmit <0..7> |
          set-sec-cos-transmit <0..7> |
          transmit}

```

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

police-simple: Establish the traffic policing style for the specified class.

conform-action: Conform action.

violate-action: Violate action.

drop: Drop.

set-cos-as-sec-cos: set-cos-as-sec-cos

set-cos-transmit: set-cos-transmit

set-sec-cos-transmit: set-sec-cos-transmit

set-prec-transmit: set-prec-transmit

set-dscp-transmit: set-dscp-transmit

transmit: transmit

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	1..4294967295	Data rate (Kbps).
P-4	1..128	Burst size (KB).

Parameter	Value	Meaning
P-5	0..7	COS value.
P-6	af11	af11
	af12	af12
	af13	af13
	af21	af21
	af22	af22
	af23	af23
	af31	af31
	af32	af32
	af33	af33
	af41	af41
	af42	af42
	af43	af43
	be	be
	cs0	cs0
	cs1	cs1
	cs2	cs2
	cs3	cs3
	cs4	cs4
	cs5	cs5
	cs6	cs6
cs7	cs7	
ef	ef	
P-7	0..7	Ip precedence value.
P-8	0..7	COS value.

12.3.9 policy-map name class name police-simple conform action set-cos-as-sec-cos violate-action

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:**

```

policy-map name <string> class name <string>
  police-simple <1..4294967295> <1..128>
    conform-action set-cos-as-sec-cos
    violate-action
      {drop |
        set-cos-as-sec-cos |
        set-cos-transmit <0..7> |
        set-dscp-transmit
          <af11|af12|af13|af21|af22|
            af23|af31|af32|af33|af41|
              af42|af43|be|cs0|cs1|cs2|
                cs3|cs4|cs5|cs6|cs7|ef> |
        set-prec-transmit <0..7> |
        set-sec-cos-transmit <0..7> |
        transmit}

```

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

police-simple: Establish the traffic policing style for the specified class.

conform-action: Conform action.

violate-action: Violate action.

drop: Drop.

set-cos-as-sec-cos: set-cos-as-sec-cos

set-cos-transmit: set-cos-transmit

set-sec-cos-transmit: set-sec-cos-transmit

set-prec-transmit: set-prec-transmit

set-dscp-transmit: set-dscp-transmit

transmit: transmit

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	1..4294967295	Data rate (Kbps).

Parameter	Value	Meaning
P-4	1..128	Burst size (KB).
P-5	0..7	COS value.
P-6	af11	af11
	af12	af12
	af13	af13
	af21	af21
	af22	af22
	af23	af23
	af31	af31
	af32	af32
	af33	af33
	af41	af41
	af42	af42
	af43	af43
	be	be
	cs0	cs0
	cs1	cs1
	cs2	cs2
	cs3	cs3
	cs4	cs4
	cs5	cs5
	cs6	cs6
cs7	cs7	
ef	ef	
P-7	0..7	Ip precedence value.
P-8	0..7	COS value.

12.3.10 policy-map name class name police-simple conform action set-cos-transmit violate-action

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:**

```

policy-map name <string> class name <string>
  police-simple <1..4294967295> <1..128>
    conform-action set-cos-transmit <0..7>
    violate-action
      {drop |
        set-cos-as-sec-cos |
        set-cos-transmit <0..7> |
        set-dscp-transmit
          <af11|af12|af13|af21|af22|
          af23|af31|af32|af33|af41|
          af42|af43|be|cs0|cs1|cs2|
          cs3|cs4|cs5|cs6|cs7|ef> |
        set-prec-transmit <0..7> |
        set-sec-cos-transmit <0..7> |
        transmit}

```

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

police-simple: Establish the traffic policing style for the specified class.

conform-action: Conform action.

violate-action: Violate action.

drop: Drop.

set-cos-as-sec-cos: set-cos-as-sec-cos

set-cos-transmit: set-cos-transmit

set-sec-cos-transmit: set-sec-cos-transmit

set-prec-transmit: set-prec-transmit

set-dscp-transmit: set-dscp-transmit

transmit: transmit

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	1..4294967295	Data rate (Kbps).

Parameter	Value	Meaning
P-4	1..128	Burst size (KB).
P-5	0..7	COS value.
P-6	0..7	COS value.
P-7	af11	af11
	af12	af12
	af13	af13
	af21	af21
	af22	af22
	af23	af23
	af31	af31
	af32	af32
	af33	af33
	af41	af41
	af42	af42
	af43	af43
	be	be
	cs0	cs0
	cs1	cs1
	cs2	cs2
	cs3	cs3
	cs4	cs4
	cs5	cs5
	cs6	cs6
cs7	cs7	
ef	ef	
P-8	0..7	Ip precedence value.
P-9	0..7	COS value.

12.3.11 policy-map name class name police-simple conform action set-dscp-transmit violate-action

Configure a Diffserv policy.

► **Mode:** Global Config Mode

► **Privilege Level:** Operator

► **Format:** policy-map name <string> class name <string>

```

police-simple <1..4294967295> <1..128>
  conform-action set-dscp-transmit
    <af11|af12|af13|af21|af22|
      af23|af31|af32|af33|af41|
      af42|af43|be|cs0|cs1|cs2|
      cs3|cs4|cs5|cs6|cs7|ef>
  violate-action
    {drop |
      set-cos-as-sec-cos |
      set-cos-transmit <0..7> |
      set-dscp-transmit
        <af11|af12|af13|af21|af22|
          af23|af31|af32|af33|af41|
          af42|af43|be|cs0|cs1|cs2|
          cs3|cs4|cs5|cs6|cs7|ef> |
      set-prec-transmit <0..7> |
      set-sec-cos-transmit <0..7> |
      transmit}

```

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

police-simple: Establish the traffic policing style for the specified class.

conform-action: Conform action.

violate-action: Violate action.

drop: Drop.

set-cos-as-sec-cos: set-cos-as-sec-cos

set-cos-transmit: set-cos-transmit

set-sec-cos-transmit: set-sec-cos-transmit

set-prec-transmit: set-prec-transmit

set-dscp-transmit: set-dscp-transmit

transmit: transmit

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	1..4294967295	Data rate (Kbps).
P-4	1..128	Burst size (KB).
P-5	af11	af11
	af12	af12
	af13	af13
	af21	af21
	af22	af22
	af23	af23
	af31	af31
	af32	af32
	af33	af33
	af41	af41
	af42	af42
	af43	af43
	be	be
	cs0	cs0
	cs1	cs1
	cs2	cs2
	cs3	cs3
	cs4	cs4
	cs5	cs5
	cs6	cs6
cs7	cs7	
ef	ef	
P-6	0..7	COS value.

Parameter	Value	Meaning
P-7	af11	af11
	af12	af12
	af13	af13
	af21	af21
	af22	af22
	af23	af23
	af31	af31
	af32	af32
	af33	af33
	af41	af41
	af42	af42
	af43	af43
	be	be
	cs0	cs0
	cs1	cs1
	cs2	cs2
	cs3	cs3
	cs4	cs4
	cs5	cs5
	cs6	cs6
cs7	cs7	
ef	ef	
P-8	0..7	Ip precedence value.
P-9	0..7	COS value.

12.3.12 policy-map name class name police-simple conform action set-prec-transmit violate-action

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:**

```

policy-map name <string> class name <string>
  police-simple <1..4294967295> <1..128>
    conform-action set-prec-transmit <0..7>
    violate-action
      {drop |
        set-cos-as-sec-cos |
        set-cos-transmit <0..7> |
        set-dscp-transmit
          <af11|af12|af13|af21|af22|
          af23|af31|af32|af33|af41|
          af42|af43|be|cs0|cs1|cs2|
          cs3|cs4|cs5|cs6|cs7|ef> |
        set-prec-transmit <0..7> |
        set-sec-cos-transmit <0..7> |
        transmit}

```

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

police-simple: Establish the traffic policing style for the specified class.

conform-action: Conform action.

violate-action: Violate action.

drop: Drop.

set-cos-as-sec-cos: set-cos-as-sec-cos

set-cos-transmit: set-cos-transmit

set-sec-cos-transmit: set-sec-cos-transmit

set-prec-transmit: set-prec-transmit

set-dscp-transmit: set-dscp-transmit

transmit: transmit

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	1..4294967295	Data rate (Kbps).

Parameter	Value	Meaning
P-4	1..128	Burst size (KB).
P-5	0..7	Ip precedence value..
P-6	0..7	COS value.
P-7	af11	af11
	af12	af12
	af13	af13
	af21	af21
	af22	af22
	af23	af23
	af31	af31
	af32	af32
	af33	af33
	af41	af41
	af42	af42
	af43	af43
	be	be
	cs0	cs0
	cs1	cs1
	cs2	cs2
	cs3	cs3
	cs4	cs4
	cs5	cs5
	cs6	cs6
cs7	cs7	
ef	ef	
P-8	0..7	Ip precedence value.
P-9	0..7	COS value.

12.3.13 policy-map name class name police-simple conform action set-sec-cos-transmit violate-action

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:**

```

policy-map name <string> class name <string>
  police-simple <1..4294967295> <1..128>
    conform-action set-sec-cos-transmit <0..7>
    violate-action
      {drop |
        set-cos-as-sec-cos |
        set-cos-transmit <0..7> |
        set-dscp-transmit
          <af11|af12|af13|af21|af22|
          af23|af31|af32|af33|af41|
          af42|af43|be|cs0|cs1|cs2|
          cs3|cs4|cs5|cs6|cs7|ef> |
        set-prec-transmit <0..7> |
        set-sec-cos-transmit <0..7> |
        transmit}

```

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

police-simple: Establish the traffic policing style for the specified class.

conform-action: Conform action.

vioilate-action: Violate action.

drop: Drop.

set-cos-as-sec-cos: set-cos-as-sec-cos

set-cos-transmit: set-cos-transmit

set-sec-cos-transmit: set-sec-cos-transmit

set-prec-transmit: set-prec-transmit

set-dscp-transmit: set-dscp-transmit

transmit: transmit

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	1..4294967295	Data rate (Kbps).

Parameter	Value	Meaning
P-4	1..128	Burst size (KB).
P-5	0..7	COS value.
P-6	0..7	COS value.
P-7	af11	af11
	af12	af12
	af13	af13
	af21	af21
	af22	af22
	af23	af23
	af31	af31
	af32	af32
	af33	af33
	af41	af41
	af42	af42
	af43	af43
	be	be
	cs0	cs0
	cs1	cs1
	cs2	cs2
	cs3	cs3
cs4	cs4	
cs5	cs5	
cs6	cs6	
cs7	cs7	
ef	ef	
P-8	0..7	Ip precedence value.
P-9	0..7	COS value.

12.3.14 policy-map name class name police-simple conform action transmit violate-action

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:**

```

policy-map name <string> class name <string>
  police-simple <1..4294967295> <1..128>
    conform-action transmit violate-action
      {drop |
        set-cos-as-sec-cos |
        set-cos-transmit <0..7> |
        set-dscp-transmit
          <af11|af12|af13|af21|af22|
            af23|af31|af32|af33|af41|
              af42|af43|be|cs0|cs1|cs2|
                cs3|cs4|cs5|cs6|cs7|ef> |
        set-prec-transmit <0..7> |
        set-sec-cos-transmit <0..7> |
        transmit}

```

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

police-simple: Establish the traffic policing style for the specified class.

conform-action: Conform action.

violate-action: Violate action.

drop: Drop.

set-cos-as-sec-cos: set-cos-as-sec-cos

set-cos-transmit: set-cos-transmit

set-sec-cos-transmit: set-sec-cos-transmit

set-prec-transmit: set-prec-transmit

set-dscp-transmit: set-dscp-transmit

transmit: transmit

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	1..4294967295	Data rate (Kbps).
P-4	1..128	Burst size (KB).
P-5	0..7	COS value.

Parameter	Value	Meaning
P-6	af11	af11
	af12	af12
	af13	af13
	af21	af21
	af22	af22
	af23	af23
	af31	af31
	af32	af32
	af33	af33
	af41	af41
	af42	af42
	af43	af43
	be	be
	cs0	cs0
	cs1	cs1
	cs2	cs2
	cs3	cs3
	cs4	cs4
	cs5	cs5
	cs6	cs6
	cs7	cs7
ef	ef	
P-7	0..7	Ip precedence value.
P-8	0..7	COS value.

12.3.15 policy-map name class name police-two-rate conform-action ... exceed-action ... violate-action ...

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:**

```

policy-map name <string> class name <string>
  police-two-rate <1..4294967295> <1..128>
    conform-action *)
    exceed-action *)
    violate-action *)
  *){drop |
    set-cos-as-sec-cos |
    set-cos-transmit <0..7> |
    set-dscp-transmit
      <af11|af12|af13|af21|af22|
      af23|af31|af32|af33|af41|
      af42|af43|be|cs0|cs1|cs2|
      cs3|cs4|cs5|cs6|cs7|ef> |
    set-prec-transmit <0..7> |
    set-sec-cos-transmit <0..7> |
    transmit}

```

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

police-two-rate: Establish the two-rate traffic policing style for the specified class.

conform-action: Conform action.

exceed-action: Exceed action.

violate-action: Violate action.

drop: Drop.

set-cos-as-sec-cos: set-cos-as-sec-cos

set-cos-transmit: set-cos-transmit

set-sec-cos-transmit: set-sec-cos-transmit

set-prec-transmit: set-prec-transmit

set-dscp-transmit: set-dscp-transmit

transmit: transmit

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.
P-3	1..4294967295	Data rate (Kbps).
P-4	1..128	Burst size (KB).
P-5	1..4294967295	Data rate (Kbps).
P-6	1..128	Burst size (KB).
P-7	0..7	COS value.
P-8	af11	af11
	af12	af12
	af13	af13
	af21	af21
	af22	af22
	af23	af23
	af31	af31
	af32	af32
	af33	af33
	af41	af41
	af42	af42
	af43	af43
	be	be
	cs0	cs0
	cs1	cs1
	cs2	cs2
	cs3	cs3
	cs4	cs4
	cs5	cs5
	cs6	cs6
cs7	cs7	
ef	ef	
P-9	0..7	Ip precedence value.
P-10	0..7	COS value.

12.3.16 policy-map name class name redirect

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** policy-map name <string> class name <string>


```

      redirect < 1/1 | 1/2 | 1/3 | 1/4 | 2/1 |
                  2/2 | 2/3 | 2/4 | 3/1 | 3/2 |
                  3/3 | 3/4 | 4/1 | 4/2 | 4/3 |
                  4/4 | 5/1 | 5/2 | 5/3 | 5/4 |
                                lag/1 | lag/2 >
```

class: Manage DiffServ policy-class instances.

name: Configure a policy-class instance.

remove: Remove a policy-class instance.

redirect: All incoming packets for the associated traffic stream are redirected to a specific egress interface.

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.

Parameter	Value	Meaning
P-3	1/1	slot 1 / port 1
	1/2	slot 1 / port 2
	1/3	slot 1 / port 3
	1/4	slot 1 / port 4
	2/1	slot 2 / port 1
	2/2	slot 2 / port 2
	2/3	slot 2 / port 3
	2/4	slot 2 / port 4
	3/1	slot 3 / port 1
	3/2	slot 3 / port 2
	3/3	slot 3 / port 3
	3/4	slot 3 / port 4
	4/1	slot 4 / port 1
	4/2	slot 4 / port 2
	4/3	slot 4 / port 3
	4/4	slot 4 / port 4
	5/1	slot 5 / port 1
	5/2	slot 5 / port 2
	5/3	slot 5 / port 3
	5/4	slot 5 / port 4
	lag/1	lag instance 1
	lag/1	lag instance 1

12.3.17 policy-map name class remove

Configure a Diffserv policy.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `policy-map name <string> class remove <string>`
class: Manage DiffServ policy-class instances.
remove: Remove a policy-class instance.

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ class name, max. 31 characters.

12.3.18 policy-map rename

Rename an existing DiffServ policy.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `policy-map rename <string> <string>`

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.
P-2	string	Enter the DiffServ policy name, max. 31 characters.

12.3.19 policy-map remove

Remove a Diffserv policy.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `policy-map remove <string>`

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.

12.4 service-policy

Assign/detach a DiffServ traffic conditioning policy to/from all interfaces.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `service-policy`

12.5 service-policy

Assign/detach a DiffServ traffic conditioning policy to/from an interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `service-policy`

12.6 show

Display device options and settings.

12.6.1 show diffserv global

Show DiffServ global information.

- ▶ Mode: Command is in all modes available..
- ▶ Privilege Level: Guest
- ▶ Format: show diffserv global

12.6.2 show diffserv service brief

Display DiffServ policy summary information.

- ▶ Mode: Command is in all modes available..
- ▶ Privilege Level: Guest
- ▶ Format: show diffserv service brief

12.6.3 show diffserv service interface

Display policy service information for the specified interface and direction.

- ▶ **Mode:** Command is in all modes available..
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show diffserv service interface <P-1> <P-2>

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	in	Traffic direction in

12.6.4 show class-map

Show existing DiffServ classes or display information for a specified class.

- ▶ **Mode:** Command is in all modes available..
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show class-map [<P-1>]

Parameter	Value	Meaning
P-1	string	Enter the DiffServ class name, max. 31 characters.

12.6.5 show policy-map all

Show all Diffserv policies.

- ▶ **Mode:** Command is in all modes available..
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show policy-map all

12.6.6 show policy-map interface

Show the policies attached to the specified interface.

- ▶ Mode: Command is in all modes available..
- ▶ Privilege Level: Guest
- ▶ Format: show policy-map interface <P-1> <P-2>

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	in	Traffic direction in

12.6.7 show policy-map name

Show information for the specified policy.

- ▶ Mode: Command is in all modes available..
- ▶ Privilege Level: Guest
- ▶ Format: show policy-map name <P-1>

Parameter	Value	Meaning
P-1	string	Enter the DiffServ policy name, max. 31 characters.

12.6.8 show service-policy

Display a summary of policy-oriented statistics information for all interfaces in the specified direction.

- ▶ Mode: Command is in all modes available..
- ▶ Privilege Level: Guest
- ▶ Format: show service-policy <P-1>

Parameter	Value	Meaning
P-1	in	Traffic direction in

13 DoS Mitigation

13.1 dos

Manage DoS Mitigation

13.1.1 dos tcp-null

Enables TCP Null scan protection - all TCP flags and TCP sequence number zero.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-null

■ no dos tcp-null

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dos tcp-null

13.1.2 dos tcp-xmas

Enables TCP XMAS scan protection - TCP FIN, URG, PSH equal 1 and SEQ equals 0.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-xmas

- no dos tcp-xmas
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no dos tcp-xmas

13.1.3 dos tcp-syn-fin

Enables TCP SYN/FIN scan protection - TCP with SYN and FIN flags set.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-syn-fin

- no dos tcp-syn-fin
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no dos tcp-syn-fin

13.1.4 dos tcp-min-header

Enables TCP minimal header size check.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-min-header

- no dos tcp-min-header
 - Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no dos tcp-min-header

13.1.5 dos icmp-fragmented

Enables fragmented ICMP protection.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos icmp-fragmented

- no dos icmp-fragmented
 - Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no dos icmp-fragmented

13.1.6 dos icmp payload-check

Enables ICMP max payload size protection for IPv4 and IPv6.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos icmp payload-check

- no dos icmp payload-check
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no dos icmp payload-check

13.1.7 dos icmp payload-size

Configures maximum ICMP payload size (default: 512).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos icmp payload-size <P-1>

Parameter	Value	Meaning
P-1	0..1472	Max. ICMP payload size (default: 512)

13.1.8 dos ip-land

Enables LAND attack protection - source IP equals destination IP.

- ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: dos ip-land
-
- no dos ip-land
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no dos ip-land

13.1.9 dos tcp-offset

Enables TCP offset check - ingress TCP packets with fragment offset 1 are dropped.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-offset

■ no dos tcp-offset

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dos tcp-offset

13.1.10dos tcp-syn

Enables TCP source port smaller than 1024 protection.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-syn

■ no dos tcp-syn

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dos tcp-syn

13.1.11 dos l4-port

Enables UDP or TCP source port equals destination port check.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** dos l4-port

■ no dos l4-port

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no dos l4-port

13.2 show

Display device options and settings.

13.2.1 show dos

Show DoS Mitigation parameters

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show dos

14 IEEE 802.1x (Dot1x)

14.1 dot1x

Configure 802.1X parameters.

14.1.1 dot1x dynamic-vlan

Creates VLANs dynamically when a RADIUS-assigned VLAN does not exist.

- ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: dot1x dynamic-vlan
-
- no dot1x dynamic-vlan
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no dot1x dynamic-vlan

14.1.2 dot1x system-auth-control

Enable or disable 802.1X authentication support on the switch.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x system-auth-control

- no dot1x system-auth-control
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no dot1x system-auth-control

14.1.3 dot1x monitor

Enable or disable 802.1X monitor mode.

- ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: dot1x monitor
-
- no dot1x monitor
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no dot1x monitor

14.2 dot1x

Configure 802.1X interface parameters.

14.2.1 dot1x guest-vlan

Configure a VLAN as 802.1X guest VLAN.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x guest-vlan <P-1>

Parameter	Value	Meaning
P-1	0..4042	Enter the VLAN ID. Entering of ID 0 disables the feature.

14.2.2 dot1x max-req

Configure the maximum number of requests to be sent.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x max-req <P-1>

Parameter	Value	Meaning
P-1	1..10	Maximum number of requests (default: 2).

14.2.3 dot1x port-control

Set the authentication mode on the specified port.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** dot1x port-control <P-1>

Parameter	Value	Meaning
P-1	auto	Port is actually controlled by protocol.
	force-authorized	Port is authorized unconditionally (default).
	force-unauthorized	Port is unauthorized unconditionally.

14.2.4 dot1x re-authentication

Enable or disable re-authentication for the given interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** dot1x re-authentication

■ no dot1x re-authentication

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no dot1x re-authentication

14.2.5 dot1x unauthenticated-vlan

Configure a VLAN as 802.1X unauthenticated VLAN.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x unauthenticated-vlan <P-1>

Parameter	Value	Meaning
P-1	0..4042	Enter the VLAN ID. Entering of ID 0 disables the feature.

14.2.6 dot1x timeout guest-vlan-period

Configure the guest-vlan period value.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x timeout guest-vlan-period <P-1>

Parameter	Value	Meaning
P-1	1..300	Guest-vlan timeout in seconds (default: 90).

14.2.7 dot1x timeout reauth-period

Configure the re-authentication period.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x timeout reauth-period <P-1>

Parameter	Value	Meaning
P-1	1..65535	Timeout in seconds.

14.2.8 dot1x timeout quiet-period

Configure the quiet period value.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x timeout quiet-period <P-1>

Parameter	Value	Meaning
P-1	0..65535	Quiet period in seconds (default: 60).

14.2.9 dot1x timeout tx-period

Configure the transmit timeout period.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x timeout tx-period <P-1>

Parameter	Value	Meaning
P-1	1..65535	Timeout in seconds.

14.2.10 dot1x timeout supp-timeout

Configure the supplicant timeout period.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x timeout supp-timeout <P-1>

Parameter	Value	Meaning
P-1	1..65535	Timeout in seconds.

14.2.11 dot1x timeout server-timeout

Configure the server timeout period.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** dot1x timeout server-timeout <P-1>

Parameter	Value	Meaning
P-1	1..65535	Timeout in seconds.

14.2.12 dot1x initialize

Begins the initialization sequence on the specified port (port-control mode must be 'auto').

- ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** dot1x initialize
-
- **no dot1x initialize**
Disable the option
 - ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** no dot1x initialize

14.2.13dot1x re-authenticate

Begins the re-authentication sequence on the specified port (port-control mode must be 'auto').

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** dot1x re-authenticate

■ no dot1x re-authenticate

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no dot1x re-authenticate

14.3 show

Display device options and settings.

14.3.1 show dot1x global

Display global 802.1X configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show dot1x global

14.3.2 show dot1x auth-history

Display 802.1X authentication events and information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show dot1x auth-history [<P-1>] [<P-2>]

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	1..4294967294	802.1X history log entry index. This can be specified only if interface is provided. Parameter Usage: [<slot/port> [index]]

14.3.3 show dot1x detail

Display the detailed 802.1X configuration for the specified port.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show dot1x detail <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

14.3.4 show dot1x summary

Display summary information of the 802.1X configuration for a specified port or all ports.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show dot1x summary [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

14.3.5 show dot1x clients

Display 802.1X client information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show dot1x clients [<P-1>]

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.

14.3.6 show dot1x statistics

Display the 802.1X statistics for the specified port.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show dot1x statistics <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

14.4 clear

Clear several items.

14.4.1 clear dot1x statistics port

Resets the 802.1X statistics for specified port.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear dot1x statistics port <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

14.4.2 clear dot1x statistics all

Resets the 802.1X statistics for all ports.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear dot1x statistics all

14.4.3 clear dot1x auth-history port

Clears the 802.1X authentication history for specified port.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear dot1x auth-history port <P-1>`

Parameter	Value	Meaning
P-1	slot no./port no.	

14.4.4 clear dot1x auth-history all

Clears the 802.1X authentication history for all ports.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear dot1x auth-history all`

15 IEEE 802.3ad (Dot3ad)

15.1 link-aggregation

Configure 802.3ad link aggregation parameters to increase bandwidth and provide redundancy by combining connections.

15.1.1 link-aggregation add

Create a new Link Aggregation Group to increase bandwidth and provide link redundancy. If desired, enter a name up to 15 alphanumeric characters in length.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** link-aggregation add <P-1>

Parameter	Value	Meaning
P-1	lag/<lagport>	lag/<lagport> Enter a lag interface in lag/lagport format.

15.1.2 link-aggregation modify

Modify the parameters for the specified Link Aggregation Group.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** link-aggregation modify <P-1> name <P-2> addport <P-3> deleteport <P-4> adminmode linktrap static min-links <P-5>

name: Modify the name of the specified Link Aggregation Group.

addport: Add the specified port to the Link Aggregation Group.

deleteport: Delete the specified port from the Link Aggregation Group.

adminmode: Modify the administration mode of the specified Link Aggregation Group. To activate the group, enable the administration mode.

linktrap: Enable/Disable link trap notifications for the specified Link Aggregation Group

static: Enable or disable static capability for the specified Link Aggregation Group on a device. When enabled, LACP automatically helps prevent loops and allows non-link aggregation partners to support LACP.

min-links: Set the minimum links for the specified Link Aggregation Group.

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	string	Enter a user-defined text, max. 15 characters.
P-3	slot no./port no.	
P-4	slot no./port no.	
P-5	slot no./port no.	

■ no link-aggregation modify

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no link-aggregation modify

15.1.3 link-aggregation delete

Delete the Link Aggregation Group to divide the group into individual connections.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: link-aggregation delete <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

15.2 lacp

Configure lacp parameters.

15.2.1 lacp admin-key

Configure the administrative value of the key on this LAG.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp admin-key <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

15.2.2 lacp collector-max-delay

Configure the collector max delay on this LAG (default is 0).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp collector-max-delay <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

15.2.3 lacp lacpmode

Activate/deactivate LACP on an interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** lacp lacpmode

■ no lacp lacpmode

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no lacp lacpmode

15.2.4 lacp actor admin key

Configure the value of the LACP actor admin key on this port(default 0).

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** lacp actor admin key <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

15.2.5 lacp actor admin state lacp-activity

Enable/disable the LACP activity on the actor admin state.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** lacp actor admin state lacp-activity

■ no lacp actor admin state lacp-activity

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lacp actor admin state lacp-activity

15.2.6 lacp actor admin state lacp-timeout

Enable/disable the LACP timeout on the actor admin state.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp actor admin state lacp-timeout

■ no lacp actor admin state lacp-timeout

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lacp actor admin state lacp-timeout

15.2.7 lacp actor admin state aggregation

Enable/disable the aggregation on the actor admin state.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp actor admin state aggregation

■ no lacp actor admin state aggregation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lacp actor admin state aggregation

15.2.8 lacp actor admin port priority

Set LACP actor port priority value (default 128).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp actor admin port priority <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

15.2.9 lacp partner admin key

Configure the administrative value of the LACP key for the protocol partner on this LAG (default 0).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp partner admin key <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

15.2.10 lacp partner admin state lacp-activity

Enable/disable the LACP activity on the partner admin state.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** lacp partner admin state lacp-activity

■ no lacp partner admin state lacp-activity

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no lacp partner admin state lacp-activity

15.2.11 lacp partner admin state lacp-timeout

Enable/disable the LACP timeout on the partner admin state.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** lacp partner admin state lacp-timeout

■ no lacp partner admin state lacp-timeout

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no lacp partner admin state lacp-timeout

15.2.12 lacp partner admin state aggregation

Enable/disable the state aggregation on the partner admin state.

- ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** lacp partner admin state aggregation
- no lacp partner admin state aggregation
Disable the option
- ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** no lacp partner admin state aggregation

15.2.13 lacp partner admin port priority

Set LACP partner port priority value (default 128).

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** lacp partner admin port priority <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

15.2.14 lacp partner admin port id

Set LACP partner port value (default 0).

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** lacp partner admin port id <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

15.2.15lacp partner admin system-priority

Configure the partener system priority.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp partner admin system-priority <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

15.2.16lacp partner admin system-id

Configure the MAC address representing the administrative value of the LAG ports protocol partner system ID default (00:00:00:00:00:00).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp partner admin system-id <P-1>

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.

15.3 show

Display device options and settings.

15.3.1 show link-aggregation port

Show LAG configuration of a single port.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show link-aggregation port [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

15.3.2 show link-aggregation statistics

Show ports LAG statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show link-aggregation statistics [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

15.3.3 show link-aggregation members

Show the member ports for specified LAG.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show link-aggregation members <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

15.3.4 show lacp interface

Show LAG interfaces attributes.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show lacp interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

15.3.5 show lacp mode

Show lacp mode.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show lacp mode [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

15.3.6 show lacp actor

Show Link Aggregation Control protocol actor attributes.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show lacp actor [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

15.3.7 show lacp partner operational

Show Operational partner attributes.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show lacp partner operational [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

15.3.8 show lacp partner admin

Show administrative partner attributes.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show lacp partner admin [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

16 Filtering Database (FDB)

16.1 mac-filter

16.1.1 mac-filter

Static MAC filter configuration.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mac-filter <P-1> <P-2>

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	Enter the VLAN ID.

16.2 bridge

Bridge configuration.

16.2.1 bridge aging-time

Aging time configuration.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: bridge aging-time <P-1>

Parameter	Value	Meaning
P-1	10..500000	Enter a number in the given range.

16.3 show

Display device options and settings.

16.3.1 show mac-filter-table static

Displays the MAC address filter table.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mac-filter-table static

16.4 show

Display device options and settings.

16.4.1 show bridge aging-time

Address aging time.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show bridge aging-time

16.5 show

Display device options and settings.

16.5.1 show mac-addr-table

Displays the MAC address table.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mac-addr-table [<P-1>]

Parameter	Value	Meaning
P-1	a:b:c:d:e:f	Enter a MAC address.
	1..4042	Enter a VLAN ID.

16.6 clear

Clear several items.

16.6.1 clear mac-addr-table

Clears the MAC address table.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear mac-addr-table`

17 HiDiscovery

17.1 network

Configure the inband connectivity.

17.1.1 network hidiscovery operation

Enable/disable the HiDiscovery protocol on this device.

- ▶ Mode: Privileged Exec Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: network hidiscovery operation
-
- no network hidiscovery operation
Disable the option
 - ▶ Mode: Privileged Exec Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no network hidiscovery operation

17.1.2 network hidiscovery mode

Set the access level for HiDiscovery.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network hidiscovery mode <P-1>

Parameter	Value	Meaning
P-1	read-write	Allow detection and configuration.
	read-only	Allow only detection, no configuration.

17.1.3 network hidiscovery blinking

Enable/disable the HiDiscovery blinking sequence on this device. This preference is not saved in configuration

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network hidiscovery blinking

■ no network hidiscovery blinking

Disable the option

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: no network hidiscovery blinking

17.2 show

Display device options and settings.

17.2.1 show network hidiscovery

Show the HiDiscovery settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show network hidiscovery

18 Hypertext Transfer Protocol (HTTP)

18.1 http

Set HTTP parameters.

18.1.1 http port

Set the HTTP port number.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: http port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of the HTTP server (default: 80).

18.1.2 http server

Enable or disable the HTTP server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: http server

■ no http server

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no http server

18.2 show

Display device options and settings.

18.2.1 show http

Show HTTP server information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show http

19 HTTP Secure (HTTPS)

19.1 https

Set HTTPS parameters.

19.1.1 https server

Enable or disable the HTTPS server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: https server

■ no https server

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no https server

19.1.2 https port

Set the HTTPS port number.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: https port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of the web server (default: 443).

19.1.3 https certificate

Generate/Delete HTTPS X509/PEM certificate.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: https certificate <P-1>

Parameter	Value	Meaning
P-1	generate	Generates the item
	delete	Deletes the item

19.2 copy

Copy different kinds of items.

19.2.1 copy httpscert remote

Copy X509/PEM certificate from server.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `copy httpscert remote <P-1> nvm`

`nvm`: Copy HTTPS certificate (PEM) from the remote server to the NV memory.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

19.3 show

Display device options and settings.

19.3.1 show https

Show HTTPS server information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show https

20 Integrated Authentication Server (IAS)

20.1 ias-users

Manage IAS Users and User Accounts.

20.1.1 ias-users add

Add a new IAS user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ias-users add <P-1>`

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

20.1.2 ias-users delete

Delete an existing IAS user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ias-users delete <P-1>`

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

20.1.3 ias-users enable

Enable IAS user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ias-users enable <P-1>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

20.1.4 ias-users disable

Disable IAS user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ias-users disable <P-1>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

20.1.5 ias-users password

Change IAS user password.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ias-users password <P-1> [<P-2>]

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	string	Enter a user-defined text, max. 64 characters.

20.2 show

Display device options and settings.

20.2.1 show ias-users

Display IAS users and user accounts information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Administrator
- ▶ Format: show ias-users

21 IEC 61850 MMS Server

21.1 iec61850-mms

Configure the IEC61850 MMS Server settings.

21.1.1 iec61850-mms operation

Enable or disable the IEC61850 MMS Server. The MMS server facilitates real-time distribution of data and supervisory control functions for substations.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** iec61850-mms operation

■ no iec61850-mms operation

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no iec61850-mms operation

21.1.2 iec61850-mms write-access

Enable or disable the Write-Access on IEC61850 bridge objects via MMS. Write services allow the MMS client to access application content. - Possible security risk, as MMS communication is not authenticated -

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: iec61850-mms write-access

■ no iec61850-mms write-access

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no iec61850-mms write-access

21.1.3 iec61850-mms port

Defines the port number of the IEC61850 MMS server (default: 102).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: iec61850-mms port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of the IEC61850 MMS server (default: 102).

21.1.4 iec61850-mms max-sessions

Defines the maximum number of concurrent IEC61850 MMS sessions (default: 5).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: iec61850-mms max-sessions <P-1>

Parameter	Value	Meaning
P-1	1..15	Maximum number of concurrent IEC61850 MMS sessions (default: 5).

21.1.5 iec61850-mms technical-key

Defines the IEC61850 MMS Technical Key (default: KEY).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: iec61850-mms technical-key <P-1>

Parameter	Value	Meaning
P-1	string	Enter a IEC61850-7-2 Ed. VisibleString, max. 32 characters. The following characters are allowed: VisibleString (FROM ('A' 'a' 'B' 'b' 'C' 'c' 'D' 'd' 'E' 'e' 'F' 'f' 'G' 'g' 'H' 'h' 'I' 'i' 'J' 'j' 'K' 'k' 'L' 'l' 'M' 'm' 'N' 'n' 'O' 'o' 'P' 'p' 'Q' 'q' 'R' 'r' 'S' 's' 'T' 't' 'U' 'u' 'V' 'v' 'W' 'w' 'X' 'x' 'Y' 'y' 'Z' 'z' '_' '0' '1' '2' '3' '4' '5' '6' '7' '8' '9')

21.2 show

Display device options and settings.

21.2.1 show iec61850-mms

Show the IEC61850 MMS Server settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show iec61850-mms

22 IGMP Snooping

22.1 igmp-snooping

Configure IGMP snooping.

22.1.1 igmp-snooping mode

Enable or disable IGMP snooping.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping mode

■ no igmp-snooping mode

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no igmp-snooping mode

22.1.2 igmp-snooping querier mode

Enable or disable IGMP snooping querier on the system.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping querier mode

■ no igmp-snooping querier mode

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no igmp-snooping querier mode

22.1.3 igmp-snooping querier query-interval

Sets the IGMP querier query interval time (1-1800) in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping querier query-interval <P-1>

Parameter	Value	Meaning
P-1	1..1800	Enter a number in the given range.

22.1.4 igmp-snooping querier timer-expiry

Sets the IGMP querier timer expiration period (60-300) in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping querier timer-expiry <P-1>

Parameter	Value	Meaning
P-1	60..300	Enter a number in the given range.

22.1.5 igmp-snooping querier version

Sets the IGMP version (1-3) of the query.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `igmp-snooping querier version <P-1>`

Parameter	Value	Meaning
P-1	1..3	IGMP snooping querier's protocol version(1 to 3,default: 2).

22.1.6 igmp-snooping forward-unknown

Configure if and how unknown multicasts are forwarded.The setting can be discard, flood or query-ports.The default is flood.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `igmp-snooping forward-unknown <P-1>`

Parameter	Value	Meaning
P-1	discard	Unknown multicast frames will be discarded.
	flood	Unknown multicast frames will be flooded.
	query-ports	Unknown multicast frames will be forwarded only to query ports.

22.2 igmp-snooping

Configure IGMP snooping.

22.2.1 igmp-snooping vlan-id

Configure the VLAN parameters.

- ▶ **Mode:** VLAN Database Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `igmp-snooping vlan-id <P-1> mode fast-leave groupmembership-interval <P-2> maxresponse <P-3> mcrtrexpiretime <P-4> querier mode address <P-5> forward-known <P-6> forward-all <P-7> static-query-port <P-8> automatic-mode <P-9>`

`mode`: Enable or disable IGMP snooping per VLAN.

`fast-leave`: Enable or disable IGMP snooping fast-leave per VLAN.

`groupmembership-interval`: Set IGMP group membership interval time (2-3600) in seconds per VLAN.

`maxresponse`: Set the igmp maximum response time (1-25) in seconds per VLAN.

`mcrtrexpiretime`: Sets the multicast router present expiration time (0-3600) in seconds per VLAN.

`querier`: Set IGMP snooping querier on the system.

`mode`: Enable or disable IGMP snooping querier per VLAN.

`address`: Set IGMP snooping querier address on the system using a VLAN.

`forward-known`: Sets the mode how known multicast packets will be treated. The default value is registered-ports-only(2).

`forward-all`: Enable or disable IGMP snooping forward-all.

`static-query-port`: Enable or disable IGMP snooping static-query-port.

`automatic-mode`: Enable or disable IGMP snooping automatic-mode.

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.
P-2	2..3600	Enter a number in the given range.
P-3	1..25	Enter a number in the given range.

Parameter	Value	Meaning
P-4	0..3600	Enter a number in the given range.
P-5	a.b.c.d	IP address.
P-6	query-and-registered-ports	Addition of query ports to multicast filter portmasks.
	registered-ports-only	No addition of query ports to multicast filter portmasks.
P-7	slot no./port no.	
P-8	slot no./port no.	
P-9	slot no./port no.	

■ no igmp-snooping vlan-id

Disable the option

- ▶ Mode: VLAN Database Mode
- ▶ Privilege Level: Operator
- ▶ Format: no igmp-snooping vlan-id

22.3 igmp-snooping

Configure IGMP snooping.

22.3.1 igmp-snooping mode

Enable or disable IGMP snooping per interface.

- ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** igmp-snooping mode
-
- **no igmp-snooping mode**
Disable the option
 - ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** no igmp-snooping mode

22.3.2 igmp-snooping fast-leave

Enable or disable IGMP snooping fast-leave per interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** igmp-snooping fast-leave

■ no igmp-snooping fast-leave

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no igmp-snooping fast-leave

22.3.3 igmp-snooping groupmembership-interval

Set IGMP group membership interval time (2-3600) in seconds per interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping groupmembership-interval <P-1>

Parameter	Value	Meaning
P-1	2..3600	Enter a number in the given range.

22.3.4 igmp-snooping maxresponse

Set the igmp maximum response time (1-25) in seconds per interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping maxresponse <P-1>

Parameter	Value	Meaning
P-1	1..25	Enter a number in the given range.

22.3.5 igmp-snooping mcrtrexpiretime

Sets the multicast router present expiration time (0-3600) in seconds per interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `igmp-snooping mcrtrexpiretime <P-1>`

Parameter	Value	Meaning
P-1	0..3600	Enter a number in the given range.

22.3.6 igmp-snooping static-query-port

Configures the interface as a static query interface in all VLANs.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `igmp-snooping static-query-port`

■ no igmp-snooping static-query-port

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `no igmp-snooping static-query-port`

22.4 show

Display device options and settings.

22.4.1 show igmp-snooping global

Show IGMP snooping global information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping global

22.4.2 show igmp-snooping interface

Show IGMP snooping interface information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

22.4.3 show igmp-snooping vlan

Show IGMP snooping VLAN information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping vlan [<P-1>]

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

22.4.4 show igmp-snooping querier global

Show IGMP snooping querier information per VLAN.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping querier global

22.4.5 show igmp-snooping querier vlan

Show IGMP snooping querier VLAN information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping querier vlan [<P-1>]

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

22.4.6 show igmp-snooping enhancements vlan

Show IGMP snooping VLAN information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping enhancements vlan [<P-1>]

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

22.4.7 show igmp-snooping enhancements unknown-filtering

Show unknown multicast filtering information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping enhancements unknown-filtering

22.4.8 show igmp-snooping statistics global

Show number of control packets processed by CPU.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping statistics global

22.4.9 show igmp-snooping statistics interface

Show number of control packets processed by CPU per interface.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show igmp-snooping statistics interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

22.5 show

Display device options and settings.

22.5.1 show mac-filter-table igmp-snooping

Display IGMP snooping entries in the MFDB table.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mac-filter-table igmp-snooping

22.6 clear

Clear several items.

22.6.1 clear igmp-snooping

Clear all IGMP snooping entries.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear igmp-snooping`

23 Interface

23.1 shutdown

23.1.1 shutdown

Enable or disable the interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** shutdown

■ no shutdown

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no shutdown

23.2 auto-negotiate

23.2.1 auto-negotiate

Enable or disable automatic negotiation on the interface. The cable crossing settings have no effect if auto-negotiation is enabled. In this case cable crossing is always set to auto. Cable crossing is set to the value chosen by the user if auto-negotiation is disabled.

- ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** auto-negotiate
-
- **no auto-negotiate**
Disable the option
 - ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** no auto-negotiate

23.3 auto-power-down

23.3.1 auto-power-down

Set the auto-power-down mode on the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: auto-power-down <P-1>

Parameter	Value	Meaning
P-1	auto-power-save	The port goes in a low power mode.
	no-power-save	The port does not use the automatic power save mode.

23.4 cable-crossing

23.4.1 cable-crossing

Cable crossing settings on the interface. The cable crossing settings have no effect if auto-negotiation is enabled. In this case cable crossing is always set to auto. Cable crossing is set to the value chosen by the user if auto-negotiation is disabled.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `cable-crossing <P-1>`

Parameter	Value	Meaning
P-1	<code>mdi</code>	The port does not use the crossover mode.
	<code>mdix</code>	The port uses the crossover mode.
	<code>auto-mdix</code>	The port uses the auto crossover mode.

23.5 linktraps

23.5.1 linktraps

Enable/disable link up/down traps on the interface.

- ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** linktraps
-
- **no linktraps**
Disable the option
 - ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** no linktraps

23.6 speed

23.6.1 speed

Sets the speed and duplex setting for the interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** speed <P-1> [**<P-2>**]

Parameter	Value	Meaning
P-1	10	10 MBit/s.
	100	100 MBit/s.
	1000	1000 MBit/s.
P-2	full	full duplex.
	half	half duplex.

23.7 name

23.7.1 name

Set or remove a descriptive name for the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: name <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 64 characters.

23.8 power-state

23.8.1 power-state

Enable or disable the power state on the interface. The interface power state settings have no effect if the interface admin state is enabled.

- ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** power-state
-
- **no power-state**
Disable the option
 - ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** no power-state

23.9 mac-filter

23.9.1 mac-filter

static mac filter configuration

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: mac-filter <P-1> <P-2>

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	Enter the VLAN ID.

23.10 led-signaling

Enable or disable Port LED signaling.

23.10.1 led-signaling operation

Enable or disable Port LED signaling.

- ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** led-signaling operation
-
- **no led-signaling operation**
Disable the option
 - ▶ **Mode:** Interface Range Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** no led-signaling operation

23.11show

Display device options and settings.

23.11.1show port all

Show Table with interface parameters.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port all

23.12show

Display device options and settings.

23.12.1show led-signaling operation

Show Port LED signaling operation.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show led-signaling operation

24 Interface Statistics

24.1 utilization

Configure the interface utilization parameters.

24.1.1 utilization control-interval

Add interval time to monitor the bandwidth utilization of the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: utilization control-interval <P-1>

Parameter	Value	Meaning
P-1	1..3600	Add interval time to monitor the bandwidth utilization.

24.1.2 utilization alarm-threshold lower

Lower threshold value

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: utilization alarm-threshold lower <P-1>

Parameter	Value	Meaning
P-1	0..10000	Add alarm threshold lower value for monitoring bandwidth utilization in hundredths of a percent.

24.1.3 utilization alarm-threshold upper

Upper threshold value

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** utilization alarm-threshold upper <P-1>

Parameter	Value	Meaning
P-1	0..10000	Add alarm threshold upper value for monitoring bandwidth utilization in hundredths of a percent.

24.2 clear

Clear several items.

24.2.1 clear port-statistics

Clear all statistics counter.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear port-statistics`

24.3 show

Display device options and settings.

24.3.1 show interface counters

Show Table with interface counters.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show interface counters

24.3.2 show interface utilization

Show interface utilization.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show interface utilization [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

24.3.3 show interface statistics

Show summary interface statistics.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show interface statistics [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

24.3.4 show interface ether-stats

Show detailed interface statistics.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show interface ether-stats [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

25 Intern

25.1 help

Display help for various special keys.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** help

25.2 logout

Exit this session.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** logout

25.3 history

Show a list of previously run commands.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** history

25.4 vlan-mode

25.4.1 vlan-mode

Enter VLAN Configuration Mode.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `vlan-mode <P-1>`

Parameter	Value	Meaning
P-1	all	Select all VLAN configured.
	vlan	Enter single VLAN.
	vlan range	Enter VLAN range seperated by hyphen e.g 1-4.
	vlan list	Enter VLAN list seperated by comma e.g 2,4,6,... .
	complex range	Enter VLAN range and several VLAN seperated by comma for a list and hyphen for ranges e.g 2-4,6-9,11.

25.5 exit

Exit from vlan mode.

- ▶ Mode: VLAN Database Mode
- ▶ Privilege Level: Operator
- ▶ Format: exit

25.6 end

Exit to exec mode.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** end

25.7 serviceshell

Enter system mode.

25.7.1 serviceshell deactivate

Disable the service shell access permanently (Cannot be undone).

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: serviceshell deactivate

25.8 traceroute

Trace route to a specified host.

25.8.1 traceroute maxttl

Set max TTL value.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** traceroute <P-1> <P-2> maxttl <P-3> [initttl <P-4>] [interval <P-5>] [count <P-6>] [maxFail <P-7>] [size <P-8>] [port <P-9>]

[initttl]: Initial TTL value.

[interval]: Timeout until probe failure.

[count]: Number of probes for each TTL.

[maxFail]: Maximum number of consecutive probes that can fail.

[size]: Size of payload in bytes.

[port]: UDP destination port.

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.
P-2	string	Hostname or IP address.
P-3	1..255	Enter a number in the given range.
P-4	0..255	Enter a number in the given range.
P-5	1..60	Enter a number in the given range.
P-6	1..10	Enter a number in the given range.
P-7	0..255	Enter a number in the given range.
P-8	0..65507	Enter a number in the given range.
P-9	1..65535	Enter port number between 1 and 65535

25.9 reboot

Reset the device (cold start).

25.9.1 reboot after

Schedule reboot after specified time.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: reboot after <P-1>

Parameter	Value	Meaning
P-1	0..2147483	Enter Seconds Between 0 to 2147483. Setting 0 will clear scheduled Reboot if configurd.

25.10ping

25.10.1ping

Send ICMP echo packets to a specified IP address.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** ping <P-1> <P-2>

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.
P-2	string	Hostname or IP address.

25.11show

Display device options and settings.

25.11.1show reboot

Display Configured reboot in seconds

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show reboot

25.11.2show serviceshell

Display the service shell access.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show serviceshell

26 Internet Protocol Version 4 (IPv4)

26.1 network

Configure the inband connectivity.

26.1.1 network protocol

Select DHCP, BOOTP or none as the network configuration protocol.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network protocol <P-1>

Parameter	Value	Meaning
P-1	none	No network config protocol
	bootp	BOOTP
	dhcp	DHCP

26.1.2 network parms

Set network address, netmask and gateway

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network parms <P-1> <P-2> [<P-3>]

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.
P-2	A.B.C.D	IP address.
P-3	A.B.C.D	IP address.

26.2 clear

Clear several items.

26.2.1 clear arp-table-switch

Clear the agent's ARP table (cache).

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear arp-table-switch`

26.3 show

Display device options and settings.

26.3.1 show network parms

Show network settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show network parms

26.4 show

Display device options and settings.

26.4.1 show arp

Show ARP table.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show arp

27 Link Backup

27.1 link-backup

Configure Link Backup parameters.

27.1.1 link-backup operation

Enable or disable Link Backup.

- ▶ **Mode:** Global Config Mode
 - ▶ **Privilege Level:** Administrator
 - ▶ **Format:** link-backup operation
-
- **no link-backup operation**
 - Disable the option**
 - ▶ **Mode:** Global Config Mode
 - ▶ **Privilege Level:** Administrator
 - ▶ **Format:** no link-backup operation

27.2 link-backup

Configure Link Backup parameters.

27.2.1 link-backup add

Add a Link Backup interface pair.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** link-backup add <P-1> [failback-time <P-2>]
[description <P-3>]

[failback-time]: FailBack time in seconds for the interface pair.

[description]: Description for the interface pair.

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	0..3600	FailBack time interval.(default: 30)
P-3	string	Enter a user-defined text, max. 256 characters.

27.2.2 link-backup delete

Delete the associated backup interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** link-backup delete <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

27.2.3 link-backup modify

Modify a Link Backup interface pair.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** link-backup modify <P-1> [failback-status <P-2>] [failback-time <P-3>] [description <P-4>] [status <P-5>]

[failback-status]: Modify failback status.(default: enabled)

[failback-time]: Modify failback time.(default: 30)

[description]: Description for the interface pair.

[status]: Enable or disable a Link Backup interface pair entry.

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	enable	Enable the option.
	disable	Disable the option.
P-3	0..3600	FailBack time interval.(default: 30)
P-4	string	Enter a user-defined text, max. 256 characters.
P-5	enable	Enable the option.
	disable	Disable the option.

27.3 show

Display device options and settings.

27.3.1 show link-backup operation

Display Link Backup global information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show link-backup operation

27.3.2 show link-backup pairs

Display Link Backup interface pairs.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show link-backup pairs [<P-1>] [<P-2>]

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	slot no./port no.	

28 Link Layer Discovery Protocol (LLDP)

28.1 lldp

Configure of Link Layer Discovery Protocol.

28.1.1 lldp operation

Enable or disable the LLDP operational state.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp operation

■ no lldp operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp operation

28.1.2 lldp config chassis admin-state

Enable or disable the LLDP operational state.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp config chassis admin-state <P-1>

Parameter	Value	Meaning
P-1	enable	Enable the option.
	disable	Disable the option.

28.1.3 Ildp config chassis notification-interval

Enter the LLDP notification interval in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `lldp config chassis notification-interval <P-1>`

Parameter	Value	Meaning
P-1	5..3600	Enter a number in the given range.

28.1.4 Ildp config chassis re-init-delay

Enter the LLDP re-initialization delay in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `lldp config chassis re-init-delay <P-1>`

Parameter	Value	Meaning
P-1	1..10	Enter a number in the given range.

28.1.5 lldp config chassis tx-delay

Enter the LLDP transmit delay in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `lldp config chassis tx-delay <P-1>`

Parameter	Value	Meaning
P-1	1..8192	Enter a number in the given range.

28.1.6 lldp config chassis tx-hold-multiplier

Enter the LLDP transmit hold multiplier.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `lldp config chassis tx-hold-multiplier <P-1>`

Parameter	Value	Meaning
P-1	2..10	Enter a number in the given range.

28.1.7 lldp config chassis tx-interval

Enter the LLDP transmit interval in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `lldp config chassis tx-interval <P-1>`

Parameter	Value	Meaning
P-1	5..32768	Enter a number in the given range.

28.2 show

Display device options and settings.

28.2.1 show lldp global

Display the LLDP global configurations.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lldp global

28.2.2 show lldp port

Display port specific LLDP configurations.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lldp port [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

28.2.3 show lldp remote-data

Remote information collected with LLDP.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show lldp remote-data [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

28.3 Ildp

Configure of Link Layer Discovery Protocol on a port.

28.3.1 Ildp admin-state

Configure how the interface processes LLDP frames.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `lldp admin-state <P-1>`

Parameter	Value	Meaning
P-1	tx-only	Interface will only transmit LLDP frames. Received frames are not processed.
	rx-only	Interface will only receive LLDP frames. Frames are not transmitted.
	tx-and-rx	Interface will transmit and receive LLDP frames. This is the default setting.
	disable	Interface will neither transmit nor process received LLDP frames.

28.3.2 Ildp fdb-mode

Configure the LLDP FDB mode for this interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `lldp fdb-mode <P-1>`

Parameter	Value	Meaning
P-1	lldp-only	Collected remote data will be based on received LLDP frames only.
	mac-only	Collected remote data will be based on the switch's FDB entries only.
	both	Collected remote data will be based on received LLDP frames as well as on the switch's FDB entries.
	auto-detect	As long as no LLDP frames are received, the collected remote data will be based on the switch's FDB entries only. After the first LLDP frame is received, the remote data will be based on received LLDP frames only. This is the default setting.

28.3.3 Ildp max-neighbors

Enter the LLDP max neighbors for interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `lldp max-neighbors <P-1>`

Parameter	Value	Meaning
P-1	1..50	Enter a number in the given range.

28.3.4 Ildp notification

Enable or disable the LLDP notification operation for interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `lldp notification`

- no Ildp notification
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp notification

28.3.5 Ildp tlv link-aggregation

Enable or disable link-aggregation TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv link-aggregation

- no Ildp tlv link-aggregation
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv link-aggregation

28.3.6 Ildp tlv mac-phy-config-state

Enable or disable mac-phy-config-state TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv mac-phy-config-state

- no lldp tlv mac-phy-config-state
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv mac-phy-config-state

28.3.7 Ildp tlv max-frame-size

Enable or disable max-frame-size TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv max-frame-size

- no lldp tlv max-frame-size
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv max-frame-size

28.3.8 Ildp tlv mgmt-addr

Enable or disable mgmt-addr TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv mgmt-addr

- no lldp tlv mgmt-addr
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv mgmt-addr

28.3.9 Ildp tlv port-desc

Enable or disable port description TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv port-desc

- no lldp tlv port-desc
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv port-desc

28.3.10 Ildp tlv port-vlan

Enable or disable port-vlan TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv port-vlan

- no lldp tlv port-vlan
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv port-vlan

28.3.11 lldp tlv protocol

Enable or disable protocol TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv protocol

- no lldp tlv protocol
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv protocol

28.3.12 lldp tlv sys-cap

Enable or disable system capabilities TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv sys-cap

- no lldp tlv sys-cap
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv sys-cap

28.3.13 lldp tlv sys-desc

Enable or disable system description TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv sys-desc

- no lldp tlv sys-desc
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv sys-desc

28.3.14 lldp tlv sys-name

Enable or disable system name TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv sys-name

- no lldp tlv sys-name
 - Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv sys-name

28.3.15 lldp tlv vlan-name

Enable or disable vlan name TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv vlan-name

- no lldp tlv vlan-name
 - Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv vlan-name

28.3.16 lldp tlv protocol-based-vlan

Enable or disable protocol-based vlan TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv protocol-based-vlan

- no lldp tlv protocol-based-vlan
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv protocol-based-vlan

28.3.17 lldp tlv igmp

Enable or disable igmp TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv igmp

- no lldp tlv igmp
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv igmp

28.3.18 lldp tlv portsec

Enable or disable portsec TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv portsec

- no lldp tlv portsec
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv portsec

28.3.19 lldp tlv ptp

Enable or disable PTP TLV transmission.

- ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: lldp tlv ptp
-
- no lldp tlv ptp
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no lldp tlv ptp

29 Logging

29.1 logging

Logging configuration.

29.1.1 logging audit-trail

Add a comment for the audit trail.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging audit-trail <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 80 characters.

29.1.2 logging buffered severity

Configure the minimum severity level to be logged to the high priority buffer.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging buffered severity <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
6	Same as informational	
7	Same as debug	

29.1.3 logging host add

Add a new logging host.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging host add <P-1> addr <P-2> <P-3> [port <P-4>] [severity <P-5>] [type <P-6>]

addr: Enter the IP address of the server.

[port]: Enter the UDP port used for syslog server transmission.

[severity]: Configure the minimum severity level to be sent to this syslog server.

[type]: Configure the type of log messages to be sent to the syslog server.

Parameter	Value	Meaning
P-1	1..8	Syslog server entry index
P-2	string	Hostname or IP address.
P-3	a.b.c.d	IP address.
P-4	1..65535	UDP port number to be used
P-5	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
5	Same as notice	
6	Same as informational	
7	Same as debug	
P-6	systemlog	the system event log entries
	audittrail	the audit trail log entries

29.1.4 logging host delete

Delete a logging host.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging host delete <P-1>

Parameter	Value	Meaning
P-1	1..8	Syslog server entry index

29.1.5 logging host enable

Enable a logging host.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging host enable <P-1>

Parameter	Value	Meaning
P-1	1..8	Syslog server entry index

29.1.6 logging host disable

Disable a logging host.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging host disable <P-1>

Parameter	Value	Meaning
P-1	1..8	Syslog server entry index

29.1.7 logging host modify

Modify an existing logging host.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging host modify <P-1> [addr <P-2> <P-3>]
[port <P-4>] [severity <P-5>] [type <P-6>]

[addr]: Enter the IP address of the server.

[port]: Enter the UDP port used for syslog server transmission.

[severity]: Configure the minimum severity level to be sent to this syslog server.

[type]: Configure the type of log messages to be sent to the syslog server.

Parameter	Value	Meaning
P-1	1..8	Syslog server entry index
P-2	string	Hostname or IP address.
P-3	a.b.c.d	IP address.
P-4	1..65535	UDP port number to be used
P-5	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
5	Same as notice	
6	Same as informational	
7	Same as debug	
P-6	systemlog	the system event log entries
	audittrail	the audit trail log entries

29.1.8 logging syslog operation

Enable or disable the syslog client.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging syslog operation

- no logging syslog operation
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: no logging syslog operation

29.1.9 logging current-console operation

Enable or disable logging messages to the current remote console.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging current-console operation

- no logging current-console operation
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: no logging current-console operation

29.1.10 logging current-console severity

Configure the minimum severity level to be sent to the current remote console.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging current-console severity <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
6	Same as informational	
7	Same as debug	

29.1.11 logging console operation

Enable or disable logging to the local V.24 console.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging console operation

■ no logging console operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no logging console operation

29.1.12 logging console severity

Configure the minimum severity level to be logged to the V.24 console.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging console severity <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug

29.2 show

Display device options and settings.

29.2.1 show logging buffered

Display buffered (in-memory) log entries.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show logging buffered [<P-1>]

Parameter	Value	Meaning
P-1	string	<filter> Enter a comma separated list of severity ranges, numbers or enum strings are allowed. Example: 0-1,informational-debug

29.2.2 show logging traplogs

Display trap log entries.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show logging traplogs

29.2.3 show logging console

Display console logging configurations.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show logging console

29.2.4 show logging syslog

Display current syslog operational setting.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show logging syslog

29.2.5 show logging host

Display a list of logging hosts currently configured.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show logging host

29.3 copy

Copy different kinds of items.

29.3.1 copy eventlog buffered remote

Copy buffered log to file server.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: copy eventlog buffered remote <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

29.3.2 copy traplog system remote

Copy traplog to file server

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: copy traplog system remote <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

29.3.3 copy audittrail system remote

Copy audit trail to file server.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Auditor
- ▶ Format: copy audittrail system remote <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

29.4 clear

Clear several items.

29.4.1 clear logging buffered

Clear buffered log from memory.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clear logging buffered

29.4.2 clear eventlog

Clear the event log entries from memory.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clear eventlog

30 Management Access

30.1 network

Configure the inband connectivity.

30.1.1 network management access web timeout

Set the web interface idle timeout.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** network management access web timeout <P-1>

Parameter	Value	Meaning
P-1	0..160	Idle timeout of a session in minutes (default: 5).

30.1.2 network management access add

Add a new entry with index.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** network management access add <P-1> [ip <P-2>] [mask <P-3>] [http <P-4>] [https <P-5>] [snmp <P-6>] [telnet <P-7>] [iec61850-mms <P-8>] [ssh <P-9>]

[ip]: Configure IP address which should have access to management.

[mask]: Configure network mask to allow a subnet for management access.

[http]: Configure if HTTP is allowed to have management access.

[https]: Configure if HTTPS is allowed to have management access.

[snmp]: Configure if SNMP is allowed to have management access.

[telnet]: Configure if telnet is allowed to have management access.

[iec61850-mms]: Configure if IEC61850-Mms is allowed to have management access.

[ssh]: Configure if SSH is allowed to have management access.

Parameter	Value	Meaning
P-1	1..16	Pool entry index.
P-2	a.b.c.d	IP address.
P-3	0..32	Prefix length netmask.
P-4	enable	Enable the option.
	disable	Disable the option.
P-5	enable	Enable the option.
	disable	Disable the option.
P-6	enable	Enable the option.
	disable	Disable the option.
P-7	enable	Enable the option.
	disable	Disable the option.
P-8	enable	Enable the option.
	disable	Disable the option.
P-9	enable	Enable the option.
	disable	Disable the option.

30.1.3 network management access delete

Delete an entry with index.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: network management access delete <P-1>

Parameter	Value	Meaning
P-1	1..16	Pool entry index.

30.1.4 network management access modify

Modify an entry with index.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** network management access modify <P-1> ip <P-2> mask <P-3> http <P-4> https <P-5> snmp <P-6> telnet <P-7> iec61850-mms <P-8> ssh <P-9>

ip: Configure ip-address which should have access to management.

mask: Configure network mask to allow a subnet for management access.

http: Configure if HTTP is allowed to have management access.

https: Configure if HTTPS is allowed to have management access.

snmp: Configure if SNMP is allowed to have management access.

telnet: Configure if telnet is allowed to have management access.

iec61850-mms: Configure if IEC61850-Mms is allowed to have management access.

ssh: Configure if ssh is allowed to have management access.

Parameter	Value	Meaning
P-1	1..16	Pool entry index.
P-2	a.b.c.d	IP address.
P-3	0..32	Prefix length netmask.
P-4	enable	Enable the option.
	disable	Disable the option.
P-5	enable	Enable the option.
	disable	Disable the option.
P-6	enable	Enable the option.
	disable	Disable the option.
P-7	enable	Enable the option.
	disable	Disable the option.
P-8	enable	Enable the option.
	disable	Disable the option.
P-9	enable	Enable the option.
	disable	Disable the option.

30.1.5 network management access operation

Enable/Disable operation for RMA.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** network management access operation

■ no network management access operation

Disable the option

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no network management access operation

30.1.6 network management access status

Activate/Deactivate an entry.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** network management access status <P-1>

Parameter	Value	Meaning
P-1	1..16	Pool entry index.

■ no network management access status

Disable the option

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no network management access status

30.2 show

Display device options and settings.

30.2.1 show network management access global

Show global restricted management access preferences.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show network management access global

30.2.2 show network management access rules

Show restricted management access rules.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show network management access rules [<P-1>]

Parameter	Value	Meaning
P-1	1..16	Pool entry index.

31 Management Address

31.1 network

Configure the inband connectivity.

31.1.1 network management mac

Configure the locally administered MAC address.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network management mac [local-address <P-1>]
[local-address]: Enter the local admin MAC address (xx:xx:xx:xx:xx:xx). If the local address is nonzero, the device starts with this MAC address at the next boot. If the MAC address is changed, they must be stored by the configuration manager. A MAC address with a set multicast bit will not be accepted

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.

31.1.2 network management port

Configure management access per port. Setting to 'all' will allowed access from all ports.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network management port <P-1>

Parameter	Value	Meaning
P-1	all or slot no./port no.	

31.2 show

Display device options and settings.

31.2.1 show network management mac

Displays the MAC address settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show network management mac

31.2.2 show network management port

Show the management access port.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show network management port

32 Media Redundancy Protocol (MRP)

32.1 mrp

Configure the MRP settings.

32.1.1 mrp domain modify advanced-mode

Configure the MRM Advanced Mode.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify advanced-mode <P-1>

Parameter	Value	Meaning
P-1	enable	Enable the option.
	disable	Disable the option.

32.1.2 mrp domain modify manager-priority

Configure the MRM priority.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify manager-priority <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter the MRM priority (default: 32768).

32.1.3 mrp domain modify mode

Configure the role of the MRP device.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify mode <P-1>

Parameter	Value	Meaning
P-1	client	The device will be in the role of a ring client (MRC).
	manager	The device will be in the role of a ring manager (MRM).

32.1.4 mrp domain modify name

Configure the logical name of the MRP domain.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify name <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 255 characters.

32.1.5 mrp domain modify operation

Enable or disable the MRP function.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify operation <P-1>

Parameter	Value	Meaning
P-1	enable	Enable the option.
	disable	Disable the option.

32.1.6 mrp domain modify port primary

Configure the primary ringport.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify port primary <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

32.1.7 mrp domain modify port secondary

Configure the secondary ringport.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify port secondary <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

32.1.8 mrp domain modify recovery-delay

Configure the MRM Recovery Delay.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify recovery-delay <P-1>

Parameter	Value	Meaning
P-1	500ms	Maximum recovery delay of 500ms in the MRP domain.
	200ms	Maximum recovery delay of 200ms in the MRP domain.
	30ms	Maximum recovery delay of 30ms in the MRP domain.
	10ms	Maximum recovery delay of 10ms in the MRP domain.

32.1.9 mrp domain modify round-trip-delay

Configure the round-trip-delay counters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify round-trip-delay <P-1>

Parameter	Value	Meaning
P-1	reset	Reset the round-trip-delay counters.

32.1.10mrp domain modify vlan

Configure the VLAN identifier of the MRP domain.\n(VLAN ID 0 means that no VLAN is used).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify vlan <P-1>

Parameter	Value	Meaning
P-1	0..4042	VLAN identifier of the MRP domain.\n(VLAN ID 0 means that no VLAN is used).

32.1.11 mrp domain add default-domain

Default MRP domain ID.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain add default-domain

32.1.12 mrp domain add domain-id

MRP domain ID. Format: 16 bytes in decimal notation.\n(Example: 1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain add domain-id <P-1>

Parameter	Value	Meaning
P-1	string	<domain id> MRP domain ID. Format: 16 bytes in decimal notation.\n(Example: 1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16).

32.1.13 mrp domain delete

Delete the current MRP domain.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain delete

32.1.14mrp operation

Enable or disable MRP.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp operation

■ no mrp operation

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no mrp operation

32.2 show

Display device options and settings.

32.2.1 show mrp

Show MRP settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp

33 MRP IEEE

33.1 mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

33.1.1 mrp-ieee global join-time

Set the IEEE multiple registration protocol join time-interval. The join timer controls the interval between join message transmissions sent to applicant state machines. An instance of this timer is required on a per-Port, per-MRP participant basis.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee global join-time <P-1>

Parameter	Value	Meaning
P-1	10..100	Join time-interval in centi-seconds.

33.1.2 mrp-ieee global leave-time

Set the IEEE multiple registration protocol leave time-interval. The leave timer controls the period of time that the registrar state machine waits in the leave state before transiting to the empty state. An instance of the timer is required for each state machine in the leave state.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee global leave-time <P-1>

Parameter	Value	Meaning
P-1	20..600	Leave time-interval in centi-seconds.

33.1.3 mrp-ieee global leave-all-time

Set the IEEE multiple registration protocol leave-all time-interval. The leave all timer controls the frequency with which the leaveall state machine generates leaveall PDUs. The timer is required on a per-Port, per-MRP Participant basis.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee global leave-all-time <P-1>

Parameter	Value	Meaning
P-1	200..6000	Leave-All time-interval in centi-seconds.

33.2 show

Display device options and settings.

33.2.1 show mrp-ieee global interface

Show the global configuration of IEEE multiple registration protocol per interface.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mrp-ieee global interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

34 MRP IEEE MMRP

34.1 mrp-ieee

Configure IEEE MRP protocols.

34.1.1 mrp-ieee mmrp vlan-id

Configure the VLAN parameters.

- ▶ **Mode:** VLAN Database Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `mrp-ieee mmrp vlan-id <P-1> forward-all <P-2> forbidden-servicereq <P-3>`

`forward-all`: Enable or disable 'Forward All Groups' in a given Vlan for a given interface.

`forbidden-servicereq`: Enable or disable the mmrp feature 'Forbidden Service Requirement' in a given Vlan for a given interface.

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.
P-2	slot no./port no.	
P-3	slot no./port no.	

■ no mrp-ieee mmrp vlan-id

Disable the option

- ▶ **Mode:** VLAN Database Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `no mrp-ieee mmrp vlan-id`

34.2 show

Display device options and settings.

34.2.1 show mrp-ieee mmrp global

Display the IEEE MMRP global configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mmrp global

34.2.2 show mrp-ieee mmrp interface

Display the IEEE MMRP interface configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mmrp interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

34.2.3 show mrp-ieee mmrp statistics global

Display the IEEE MMRP global statistics.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mrp-ieee mmrp statistics global

34.2.4 show mrp-ieee mmrp statistics interface

Display the IEEE MMRP interface statistics.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mrp-ieee mmrp statistics interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

34.2.5 show mrp-ieee mmrp service-requirement forward-all vlan

Show Forward-All setting for port in given VLAN.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mrp-ieee mmrp service-requirement forward-all vlan [<P-1>]

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

34.2.6 show mrp-ieee mmrp service-requirement forbidden vlan

Show Forward-All setting for port in given VLAN.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mrp-ieee mmrp service-requirement forbidden vlan [<P-1>]

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

34.3 mrp-ieee

Configure IEEE MRP protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration.

34.3.1 mrp-ieee mmrp operation

Enable or disable MMRP globally. Devices use MMRP information for dynamic registration of group membership and individual MAC addresses with end devices and switches that support extended filtering services, within the connected LAN.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee mmrp operation

■ no mrp-ieee mmrp operation

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no mrp-ieee mmrp operation

34.3.2 mrp-ieee mmrp periodic-machine

Enable or disable MMRP periodic state machine globally. When enabled, the periodic state machine sends extra MMRP messages when the periodic timer expires.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee mmrp periodic-machine

■ no mrp-ieee mmrp periodic-machine

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no mrp-ieee mmrp periodic-machine

34.4 clear

Clear several items.

34.4.1 clear mrp-ieee mmrp

Clear the IEEE MMRP global and port statistic tables.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear mrp-ieee mmrp`

34.5 mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

34.5.1 mrp-ieee mmrp operation

Enable or disable MMRP on the interface, with MMRP enabled globally and on this interface, the device sends and receives MMRP messages on this port.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee mmrp operation

■ no mrp-ieee mmrp operation

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no mrp-ieee mmrp operation

34.5.2 mrp-ieee mmrp restrict-register

Enable or disable restriction of dynamic mac address registration using IEEE MMRP on the port. When enabled, the dynamic registration of mac address attributes is allowed only if the attribute has already been statically registered on the device.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee mmrp restrict-register

■ no mrp-ieee mmrp restrict-register

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no mrp-ieee mmrp restrict-register

34.6 show

Display device options and settings.

34.6.1 show mac-filter-table mmrp

Display MMRP entries in the MFDB table.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mac-filter-table mmrp

35 MRP IEEE MVRP

35.1 mrp-ieee

Configure IEEE MRP protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration.

35.1.1 mrp-ieee mvrp operation

Enable or disable IEEE MVRP globally. When enabled, the device distributes VLAN membership information on MVRP enable active ports. MVRP-aware devices use the information to dynamically create VLAN members and update the local VLAN member database.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee mvrp operation

■ no mrp-ieee mvrp operation

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no mrp-ieee mvrp operation

35.1.2 mrp-ieee mvrp periodic-machine

Enable or disable IEEE MVRP periodic state machine globally. When enabled, the device sends MVRP messages to the connected MVRP-aware devices when the periodic timer expires.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee mvrp periodic-machine

■ no mrp-ieee mvrp periodic-machine

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no mrp-ieee mvrp periodic-machine

35.2 mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

35.2.1 mrp-ieee mvrp operation

Enable or disable IEEE MVRP on the port. When enabled, globally and on this port, the device distributes VLAN membership information to MVRP aware devices connected to this port.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee mvrp operation

■ no mrp-ieee mvrp operation

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no mrp-ieee mvrp operation

35.2.2 mrp-ieee mvrp restrict-register

Enable or disable restriction of dynamic VLAN registration using IEEE MVRP on the port. When enabled, the dynamic registration of VLAN attributes is allowed only if the attribute has already been statically registered on the device.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee mvrp restrict-register

■ no mrp-ieee mvrp restrict-register

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no mrp-ieee mvrp restrict-register

35.3 show

Display device options and settings.

35.3.1 show mrp-ieee mvrp global

Display the IEEE MVRP global configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mvrp global

35.3.2 show mrp-ieee mvrp interface

Display the IEEE MVRP interface configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mvrp interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

35.3.3 show mrp-ieee mvrp statistics global

Display the IEEE MVRP global statistics.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mrp-ieee mvrp statistics global

35.3.4 show mrp-ieee mvrp statistics interface

Display the IEEE MVRP interface statistics.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mrp-ieee mvrp statistics interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

35.4 clear

Clear several items.

35.4.1 clear mrp-ieee mvrp

Clear the IEEE MVRP global and port statistic tables.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear mrp-ieee mvrp`

36 Port Monitor

36.1 port-monitor

Configure the Port Monitor condition settings.

36.1.1 port-monitor operation

Enable or disable the port monitor

- ▶ **Mode:** Global Config Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** port-monitor operation
-
- no port-monitor operation
 - Disable the option**
 - ▶ **Mode:** Global Config Mode
 - ▶ **Privilege Level:** Operator
 - ▶ **Format:** no port-monitor operation

36.2 port-monitor

Configure the Port Monitor condition settings.

36.2.1 port-monitor condition crc-fragments interval

Configure the measure interval in seconds (5-180s) for CRC-Fragment detection. Default 10.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition crc-fragments interval <P-1>

Parameter	Value	Meaning
P-1	5..180	Enter a number in the given range.

36.2.2 port-monitor condition crc-fragments count

Configure the CRC-Fragment counter in parts per million (1-1000000 [ppm]). Default 1000 [ppm].

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition crc-fragments count <P-1>

Parameter	Value	Meaning
P-1	1..1000000	Enter a number in the given range.

36.2.3 port-monitor condition crc-fragments mode

Enable or disable CRC-Fragments condition to trigger an action

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-monitor condition crc-fragments mode

■ no port-monitor condition crc-fragments mode

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no port-monitor condition crc-fragments mode

36.2.4 port-monitor condition link-flap interval

Configure the measure interval in seconds (1-180s) for Link Flap detection.
Default 10.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-monitor condition link-flap interval <P-1>

Parameter	Value	Meaning
P-1	1..180	Enter a number in the given range.

36.2.5 port-monitor condition link-flap count

Configure the Link Flap counter (1-100). Default 5.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-monitor condition link-flap count <P-1>

Parameter	Value	Meaning
P-1	1..100	Enter a number in the given range.

36.2.6 port-monitor condition link-flap mode

Enable or disable link-flap condition to trigger an action

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-monitor condition link-flap mode

■ no port-monitor condition link-flap mode

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no port-monitor condition link-flap mode

36.2.7 port-monitor condition duplex-mismatch mode

Enable or disable duplex mismatch detection condition to trigger an action

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-monitor condition duplex-mismatch mode

■ no port-monitor condition duplex-mismatch mode

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no port-monitor condition duplex-mismatch mode

36.2.8 port-monitor action

Enable or disable interface on port condition.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-monitor action <P-1>

Parameter	Value	Meaning
P-1	port-disable	Enable or disable interface on port condition
	trap-only	Send only a trap.

36.2.9 port-monitor reset

reset the port monitor.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-monitor reset

■ no port-monitor reset

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no port-monitor reset

36.3 show

Display device options and settings.

36.3.1 show port-monitor operation

Display the Port Monitor operation.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-monitor operation

36.3.2 show port-monitor brief

Display the Port Monitor summary.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-monitor brief

36.3.3 show port-monitor port

Display the Port Monitor interface details.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-monitor port <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

36.3.4 show port-monitor link-flap

Display the link-flaps counts for a specific interface.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-monitor link-flap <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

36.3.5 show port-monitor crc-fragments

Display CRC-Fragments counts for a specific interface

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-monitor crc-fragments <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

37 Port Security

37.1 port-security

Port MAC locking/security

37.1.1 port-security operation

Enable/Disable Port MAC locking/security

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-security operation

■ no port-security operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no port-security operation

37.2 port-security

Port MAC locking/security

37.2.1 port-security operation

Enable/Disable Port MAC locking/security for the interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-security operation

- no port-security operation

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no port-security operation

37.2.2 port-security max-dynamic

Set dynamic limit for the interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-security max-dynamic <P-1>

Parameter	Value	Meaning
P-1	0..600	maximum number of dynamically locked MAC addresses allowed

37.2.3 port-security max-static

Set Static Limit for the interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-security max-static <P-1>

Parameter	Value	Meaning
P-1	0..64	maximum number of statically locked MAC addresses allowed

37.2.4 port-security mac-address add

Add Static MAC address to the interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-security mac-address add <P-1> <P-2>

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	VLAN ID

37.2.5 port-security mac-address move

Make dynamic MAC addresses static for the interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-security mac-address move

37.2.6 port-security mac-address delete

Remove Static MAC address from the interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-security mac-address delete <P-1> <P-2>

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	VLAN ID

37.2.7 port-security violation-traps

SNMP violation traps for the interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-security violation-traps operation
[frequency <P-1>]

operation: Enable/Disable SNMP violation traps for the interface.

[frequency]: The minimum seconds between two successive violation traps on this port.

Parameter	Value	Meaning
P-1	0..3600	time in seconds

■ no port-security violation-traps

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no port-security violation-traps

37.3 show

Display device options and settings.

37.3.1 show port-security global

Port Security global status

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-security global

37.3.2 show port-security interface

Display port-security (port MAC locking) information for system.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-security interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

37.3.3 show port-security dynamic

Display dynamically learned MAC addresses

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-security dynamic <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

37.3.4 show port-security static

Display statically locked MAC addresses

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-security static <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

37.3.5 show port-security violation

Display port security violation information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-security violation <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

38 Precision Time Protocol (PTP)

38.1 ptp

Enable or disable the Precision Time Protocol (IEEE 1588-2008).

38.1.1 ptp operation

Enable or disable the Precision Time Protocol (IEEE 1588-2008).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp operation

■ no ptp operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ptp operation

38.1.2 ptp clock-mode

Configure PTPv2 (IEEE1588-2008) clock mode. \nIf the clock mode is changed, PTP will be initialized.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp clock-mode <P-1>

Parameter	Value	Meaning
P-1	v2-boundary-clock v2-transparent-clock	

38.1.3 ptp sync-lower-bound

Configure the lower bound for the PTP clock synchronization status \n(unit: nanoseconds). If the absolute value of the offset \ninto the master clock is smaller than the lower bound, \nthe clock's status is set to synchronized (true).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ptp sync-lower-bound <P-1>`

Parameter	Value	Meaning
P-1	1..999999999	

38.1.4 ptp sync-upper-bound

Configure the upper bound for the PTP clock synchronization status \n(unit: nanoseconds). If the absolute value of the offset \ninto the master clock is bigger than the upper bound, \nthe clock's status is set to unsynchronized (false).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ptp sync-upper-bound <P-1>`

Parameter	Value	Meaning
P-1	31..1000000000	

38.1.5 ptp management

Enable or disable PTP management via PTP management messages.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** ptp management

■ no ptp management

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no ptp management

38.1.6 ptp v2-transparent-clock syntonization

Enable or disable the syntonization (frequency synchronization) of the transparent-clock.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** ptp v2-transparent-clock syntonization

■ no ptp v2-transparent-clock syntonization

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no ptp v2-transparent-clock syntonization

38.1.7 ptp v2-transparent-clock network-protocol

Configure the network-protocol of the transparent-clock.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** ptp v2-transparent-clock network-protocol <P-1>

Parameter	Value	Meaning
P-1	ieee802.3	
	udp-ipv4	

38.1.8 ptp v2-transparent-clock multi-domain

Enable or disable the transparent-clock to process only the primary-domain or all domain numbers.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** ptp v2-transparent-clock multi-domain

■ no ptp v2-transparent-clock multi-domain

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no ptp v2-transparent-clock multi-domain

38.1.9 ptp v2-transparent-clock sync-local-clock

Enable or disable synchronization of the local clock (also enables synchronization).

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** ptp v2-transparent-clock sync-local-clock

■ no ptp v2-transparent-clock sync-local-clock

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no ptp v2-transparent-clock sync-local-clock

38.1.10 ptp v2-transparent-clock delay-mechanism

Configure the delay mechanism of the transparent-clock.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** ptp v2-transparent-clock delay-mechanism <P-1>

Parameter	Value	Meaning
P-1	e2e	
	p2p	
	e2e-optimized	
	disable	

38.1.11 ptp v2-transparent-clock primary-domain

Configure the primary-domain (for syntonization) of the transparent-clock.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ptp v2-transparent-clock primary-domain <P-1>`

Parameter	Value	Meaning
P-1	0..255	Enter a number in the given range.

38.1.12 ptp v2-transparent-clock vlan

VLAN in which PTP packets are send. With a value of none all packets are send untagged.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ptp v2-transparent-clock vlan <P-1>`

Parameter	Value	Meaning
P-1	vlanId	Send ptp to vlanId Use 0 for priority only tagged frames
	none	Send all ptp packets untagged

38.1.13 ptp v2-transparent-clock vlan-priority

VLAN priority of tagged ptp packets.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ptp v2-transparent-clock vlan-priority <P-1>`

Parameter	Value	Meaning
P-1	0..7	

38.1.14ptp v2-boundary-clock domain

Configure the PTP domain number (0..255)

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock domain <P-1>

Parameter	Value	Meaning
P-1	0..255	Enter a number in the given range.

38.1.15ptp v2-boundary-clock priority1

Configure the priority1 value (0..255) for the BMCA

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock priority1 <P-1>

Parameter	Value	Meaning
P-1	0..255	Enter a number in the given range.

38.1.16ptp v2-boundary-clock priority2

Configure the priority2 value (0..255) for the BMCA

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock priority2 <P-1>

Parameter	Value	Meaning
P-1	0..255	Enter a number in the given range.

38.1.17 ptp v2-boundary-clock utc-offset

Configure the current UTC offset (TAI - UTC) in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock utc-offset <P-1>

Parameter	Value	Meaning
P-1	-32768..32767	

38.1.18 ptp v2-boundary-clock utc-offset-valid

Configure the UTC offset valid flag

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock utc-offset-valid

■ no ptp v2-boundary-clock utc-offset-valid

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ptp v2-boundary-clock utc-offset-valid

38.2 ptp

Enable or disable the Precision Time Protocol (IEEE 1588-2008) on a port.

38.2.1 ptp v2-transparent-clock operation

Enable or disable the sending and receiving / processing of PTP synchronization messages.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `ptp v2-transparent-clock operation`

■ no ptp v2-transparent-clock operation

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `no ptp v2-transparent-clock operation`

38.2.2 ptp v2-transparent-clock asymmetry

Set the asymmetry of the link connected to this interface

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `ptp v2-transparent-clock asymmetry <P-1>`

Parameter	Value	Meaning
P-1	- 2000000000..200000 0000	

38.2.3 ptp v2-transparent-clock pdelay-interval

Configure the Peer Delay Interval in seconds {1|2|4|8|16|32}. \nThis interval is used if delay-mechanism is set to p2p

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock pdelay-interval <P-1>

Parameter	Value	Meaning
P-1	1	
	2	
	4	
	8	
	16	
	32	

38.2.4 ptp v2-boundary-clock operation

Enable or disable the sending and receiving/processing of PTP synchronization messages.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock operation

■ no ptp v2-boundary-clock operation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ptp v2-boundary-clock operation

38.2.5 ptp v2-boundary-clock pdelay-interval

Configure the Peer Delay Interval in seconds {1|2|4|8|16|32}. \nThis interval is used if delay-mechanism is set to p2p

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock pdelay-interval <P-1>

Parameter	Value	Meaning
P-1	1	
	2	
	4	
	8	
	16	
	32	

38.2.6 ptp v2-boundary-clock announce-interval

Configure the Announce Interval in seconds {1|2|4|8|16}.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock announce-interval <P-1>

Parameter	Value	Meaning
P-1	1	
	2	
	4	
	8	
	16	

38.2.7 ptp v2-boundary-clock sync-interval

Configure the Sync Interval in seconds {0.25|0.5|1|2}.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ptp v2-boundary-clock sync-interval <P-1>`

Parameter	Value	Meaning
P-1	0.25	
	0.5	
	1	
	2	

38.2.8 ptp v2-boundary-clock announce-timeout

Configure the Announce Receipt Timeout (2..10).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ptp v2-boundary-clock announce-timeout <P-1>`

Parameter	Value	Meaning
P-1	2..10	

38.2.9 ptp v2-boundary-clock asymmetry

Set the asymmetry of the link connected to this interface

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `ptp v2-boundary-clock asymmetry <P-1>`

Parameter	Value	Meaning
P-1	- 20000000000..200000 0000	

38.2.10 ptp v2-boundary-clock v1-compatibility-mode

Set the PTPv1 Hardware compatibility mode {auto|on|off}.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `ptp v2-boundary-clock v1-compatibility-mode <P-1>`

Parameter	Value	Meaning
P-1	on	
	off	
	auto	

38.2.11 ptp v2-boundary-clock delay-mechanism

Configure the delay mechanism of the boundary-clock.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `ptp v2-boundary-clock delay-mechanism <P-1>`

Parameter	Value	Meaning
P-1	e2e	
	p2p	
	disable	

38.2.12 ptp v2-boundary-clock network-protocol

Configure the network-protocol

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock network-protocol <P-1>

Parameter	Value	Meaning
P-1	ieee802.3	
	udp-ipv4	

38.2.13 ptp v2-boundary-clock vlan-priority

VLAN priority of tagged ptp packets.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock vlan-priority <P-1>

Parameter	Value	Meaning
P-1	0..7	

38.2.14ptp v2-boundary-clock vlan

VLAN in which PTP packets are send. With a value of none all packets are send untagged.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** ptp v2-boundary-clock vlan <P-1>

Parameter	Value	Meaning
P-1	vlanId	Send ptp to vlanId Use 0 for priority only tagged frames
	none	Send all ptp packets untagged

38.3 show

Display device options and settings.

38.3.1 show ptp

Show PTP parameters and status

- ▶ **Mode:** Command is in all modes available.
 - ▶ **Privilege Level:** Guest
 - ▶ **Format:** show ptp [global] [v2-boundary-clock] [v2-transparent-clock] [port] [v2-transparent-clock] [v2-boundary-clock]
- [global]: Show PTP global status
[v2-boundary-clock]: Show PTP Boundary Clock status
[v2-transparent-clock]: Show PTP Transparent Clock status
[port]: Show PTP port values
[v2-transparent-clock]: Show the PTP Transparent Clock port values
[v2-boundary-clock]: Show the PTP Boundary Clock port values.

39 Password Management

39.1 passwords

Manage password policies and options.

39.1.1 passwords min-length

Set minimum password length for user passwords.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: passwords min-length <P-1>

Parameter	Value	Meaning
P-1	1..64	Enter a number in the given range.

39.1.2 passwords max-login-attempts

Set maximum login attempts for the users.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: passwords max-login-attempts <P-1>

Parameter	Value	Meaning
P-1	0..5	Enter a number in the given range.

39.1.3 passwords min-uppercase-chars

Set minimum upper case characters for user passwords.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `passwords min-uppercase-chars <P-1>`

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

39.1.4 passwords min-lowercase-chars

Set minimum lower case characters for user passwords.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `passwords min-lowercase-chars <P-1>`

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

39.1.5 passwords min-numeric-chars

Set minimum numeric characters for user passwords.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `passwords min-numeric-chars <P-1>`

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

39.1.6 passwords min-special-chars

Set minimum special characters for user passwords.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `passwords min-special-chars <P-1>`

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

39.2 show

Display device options and settings.

39.2.1 show passwords

Display password policies and options.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show passwords

40 Radius

40.1 authorization

Configure authorization parameters.

40.1.1 authorization network radius

Enable or disable the switch to accept VLAN assignment by the RADIUS server.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** authorization network radius

■ no authorization network radius

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no authorization network radius

40.2 radius

Configure RADIUS parameters.

40.2.1 radius accounting mode

Enable or disable RADIUS accounting function.

- ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: radius accounting mode
-
- no radius accounting mode
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: no radius accounting mode

40.2.2 radius server attribute 4

Specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: radius server attribute 4 <P-1>

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.

40.2.3 radius server acct add

Add a RADIUS accounting server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: radius server acct add <P-1> ip <P-2> [name <P-3>] [port <P-4>]

ip: RADIUS accounting server IP address.

[name]: RADIUS accounting server name.

[port]: RADIUS accounting server port (default: 1813).

Parameter	Value	Meaning
P-1	1..8	Next RADIUS server valid index (it can be seen with '#show radius global' command).
P-2	a.b.c.d	IP address.
P-3	string	Enter a user-defined text, max. 32 characters.
P-4	1..65535	Enter port number between 1 and 65535

40.2.4 radius server acct delete

Delete a RADIUS accounting server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: radius server acct delete <P-1>

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

40.2.5 radius server acct modify

Change a RADIUS accounting server parameters.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** radius server acct modify <P-1> [name <P-2>] [port <P-3>] [status <P-4>] [secret [<P-5>]] [encrypted <P-6>]

[name]: RADIUS accounting server name.

[port]: RADIUS accounting server port (default: 1813).

[status]: Enable or disable a RADIUS accounting server entry.

[secret]: Configure the shared secret for the RADIUS accounting server.

[encrypted]: Configure the encrypted shared secret.

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.
P-2	string	Enter a user-defined text, max. 32 characters.
P-3	1..65535	Enter port number between 1 and 65535
P-4	enable disable	Enable the option. Disable the option.
P-5	string	Enter a user-defined text, max. 128 characters.
P-6	string	Enter a user-defined text, max. 128 characters.

40.2.6 radius server auth add

Add a RADIUS authentication server.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** radius server auth add <P-1> ip <P-2> [name <P-3>] [port <P-4>]

ip: RADIUS authentication server IP address.

[name]: RADIUS authentication server name.

[port]: RADIUS authentication server port (default: 1812).

Parameter	Value	Meaning
P-1	1..8	Next RADIUS server valid index (it can be seen with '#show radius global' command).
P-2	a.b.c.d	IP address.
P-3	string	Enter a user-defined text, max. 32 characters.
P-4	1..65535	Enter port number between 1 and 65535

40.2.7 radius server auth delete

Delete a RADIUS authentication server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: radius server auth delete <P-1>

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

40.2.8 radius server auth modify

Change a RADIUS authentication server parameters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: radius server auth modify <P-1> [name <P-2>] [port <P-3>] [msgauth] [primary] [status <P-4>] [secret [<P-5>]] [encrypted <P-6>]

[name]: RADIUS authentication server name.

[port]: RADIUS authentication server port (default: 1812).

[msgauth]: Enable or disable the message authenticator attribute for this server.

[primary]: Configure the primary RADIUS server.

[status]: Enable or disable a RADIUS authentication server entry.

[secret]: Configure the shared secret for the RADIUS authentication server.

[encrypted]: Configure the encrypted shared secret.

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.
P-2	string	Enter a user-defined text, max. 32 characters.
P-3	1..65535	Enter port number between 1 and 65535
P-4	enable	Enable the option.
	disable	Disable the option.
P-5	string	Enter a user-defined text, max. 128 characters.
P-6	string	Enter a user-defined text, max. 128 characters.

■ no radius server auth modify

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no radius server auth modify

40.2.9 radius server retransmit

Configure the retransmit value for the RADIUS server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: radius server retransmit <P-1>

Parameter	Value	Meaning
P-1	1..15	Maximum number of retransmissions (default: 4).

40.2.10radius server timeout

Configure the RADIUS server timeout value.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: radius server timeout <P-1>

Parameter	Value	Meaning
P-1	1..30	Timeout in seconds (default: 5).

40.3 show

Display device options and settings.

40.3.1 show radius global

Display global RADIUS configuration.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show radius global

40.3.2 show radius auth servers

Display all configured RADIUS authentication servers.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show radius auth servers [<P-1>]

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

40.3.3 show radius auth statistics

Display RADIUS authentication server statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show radius auth statistics <P-1>

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

40.3.4 show radius acct statistics

Display RADIUS accounting server statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show radius acct statistics <P-1>

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

40.3.5 show radius acct servers

Display all configured RADIUS accounting servers.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show radius acct servers [<P-1>]

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

40.4 clear

Clear several items.

40.4.1 clear radius

Clear the RADIUS statistics.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clear radius <P-1>

Parameter	Value	Meaning
P-1	statistics	Clear the RADIUS statistics.

41 Remote Monitoring (RMON)

41.1 rmon-alarm

Create a RMON alarm action.

41.1.1 rmon-alarm add

Add RMON alarm.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `rmon-alarm add <P-1> [mib-variable <P-2>] [rising-threshold <P-3>] [falling-threshold <P-4>]`

[mib-variable]: **MIB variable**

[rising-threshold]: **Rising threshold**

[falling-threshold]: **Falling threshold**

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.
P-2	string	Enter an object identifier of the particular variable to be sampled, max. 32 characters.
P-3	1..2147483647	Enter the rising threshold for the sampled statistic.
P-4	1..2147483647	Enter the falling threshold for the sampled statistic.

41.1.2 rmon-alarm enable

Enable RMON alarm.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: rmon-alarm enable <P-1>

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.

41.1.3 rmon-alarm disable

Disable RMON alarm.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: rmon-alarm disable <P-1>

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.

41.1.4 rmon-alarm delete

Delete RMON alarm.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: rmon-alarm delete <P-1>

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.

41.1.5 rmon-alarm modify

Modify RMON alarm parameters.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `rmon-alarm modify <P-1> [mib-variable <P-2>] [rising-threshold <P-3>] [falling-threshold <P-4>] [interval <P-5>] [sample-type <P-6>] [startup-alarm <P-7>] [rising-event <P-8>] [falling-event <P-9>]`

[mib-variable]: Enter the alarm mib variable.

[rising-threshold]: Enter the alarm rising threshold.

[falling-threshold]: Enter the alarm falling-threshold.

[interval]: Enter the alarm interval in seconds over which the data is sampled.

[sample-type]: Enter the alarm method of sampling the selected variable.

[startup-alarm]: Enter the alarm type.

[rising-event]: Enter the alarm rising-event index.

[falling-event]: Enter the alarm falling-event index.

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.
P-2	string	Enter an object identifier of the particular variable to be sampled, max. 32 characters.
P-3	1..2147483647	Enter the rising threshold for the sampled statistic.
P-4	1..2147483647	Enter the falling threshold for the sampled statistic.
P-5	1..2147483647	Enter the interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
P-6	absoluteValue	Variable is compared directly with the thresholds.
	deltaValue	Variable is subtracted from the current value and the difference compared with the thresholds.
P-7	risingAlarm	Single rising alarm generated when the sample is greater than or equal to the rising threshold.
	fallingAlarm	Single falling alarm generated when the sample is less than or equal to the falling threshold.
	risingOrFallingAlarm	Single Rising alarm generated when the sample is greater than or equal to rising-Threshold and single falling alarm generated when the sample is less than or equal to fallingThreshold.

Parameter	Value	Meaning
P-8	1..65535	Enter the index of the eventEntry that is used when a rising threshold is crossed.
P-9	1..65535	Enter the index of the eventEntry that is used when a falling threshold is crossed.

41.2 show

Display device options and settings.

41.2.1 show rmon statistics

Show RMON statistics configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show rmon statistics [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

41.2.2 show rmon alarm

Display configuration on RMON alarms.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show rmon alarm

42 Script File

42.1 script

CLI Script File.

42.1.1 script apply

Executes the CLI Script File available in the system.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: script apply <P-1>

Parameter	Value	Meaning
P-1	string	Filename.

42.1.2 script validate

Only validates the CLI Script File available in the system.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: script validate <P-1>

Parameter	Value	Meaning
P-1	string	Filename.

42.1.3 script list system

list all the Script files available in the system memory.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: script list system

42.1.4 script delete

delete the CLI Script Files.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: script delete [<P-1>]

Parameter	Value	Meaning
P-1	string	Filename.

42.2 copy

Copy different kinds of items.

42.2.1 copy script remote

Copy Script file from server.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `copy script remote <P-1> running-config nvm <P-2>`

`running-config`: Copy Script file from file server to `running-config`.

`nvm`: Copy Script file to non-volatile memory.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 32 characters.

42.2.2 copy script nvm

Copy Script file from non-volatile system memory to destination.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** `copy script nvm <P-1> running-config remote <P-2>`

`running-config`: Copy Script file from non-volatile system memory to `running-config`.

remote: Copy Script file to file server.

Parameter	Value	Meaning
P-1	string	Filename.
P-2	string	Enter a user-defined text, max. 128 characters.

42.2.3 copy script running-config nvm

Copy running configuration to non-volatile memory.

- ▶ Mode: Privileged Exec Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: copy script running-config nvm <P-1> [all]
- [all]: Copy all running configuration to non-volatile memory.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

42.2.4 copy script running-config remote

Copy running configuration to file server.

- ▶ Mode: Privileged Exec Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: copy script running-config remote <P-1> [all]
- [all]: Copy all running configuration to file server.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

42.3 show

Display device options and settings.

42.3.1 show script system

Displays the content of the CLI Script File exist in the system.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show script system <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

43 Selftest

43.1 selftest

Configure the selftest settings.

43.1.1 selftest action

Configure the action that a selftest component should take.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: selftest action <P-1> <P-2>

Parameter	Value	Meaning
P-1	task	Configure the action for task errors.
	resource	Configure the action for lack of resources.
	software	Configure the action for broken software integrity.
	hardware	Configure the action for detected hardware errors.
P-2	log-only	Write a message to the logging file.
	send-trap	Send a trap to the management station.
	reboot	Reboot the device.

43.1.2 selftest ramtest

Enable or disable the RAM selftest on cold start of the device. When disabled the device booting time is reduced.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: selftest ramtest

- no selftest ramtest
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: no selftest ramtest

43.1.3 selftest system-monitor

Enable or disable the System Monitor 1 access during the boot phase.
Please note: If the System Monitor is disabled it is possible to lose access to the device permanently in case of losing administrator password or mis-configuration.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: selftest system-monitor

- no selftest system-monitor
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: no selftest system-monitor

43.1.4 selftest boot-default-on-error

Enable or disable loading of the default configuration in case there is any error loading the configuration during boot phase. If disabled the system will be halted.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** selftest boot-default-on-error

■ no selftest boot-default-on-error

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no selftest boot-default-on-error

43.2 show

Display device options and settings.

43.2.1 show selftest action

Displays the actions of the device takes if an error occurs.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show selftest action

43.2.2 show selftest settings

Displays the selftest settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show selftest settings

44 sFlow

44.1 show

Display device options and settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show

45 Switched Monitoring (SMON)

45.1 monitor

Configure port mirroring.

45.1.1 monitor session

Configure port mirroring.

► **Mode:** Global Config Mode

► **Privilege Level:** Operator

► **Format:** monitor session <P-1> destination interface <P-2> source add interface <P-3> [<P-4>] remove interface <P-5> mode

destination: Configure the probe interface.

interface: Configure interface.

source: Configure the source interface.

add: Add an interface

interface: Configure interface.

remove: Remove an interface

interface: Configure interface.

mode: Enable/Disable port mirroring session. Note: does not affect the source or destination interfaces.

Parameter	Value	Meaning
P-1	1	Monitor session index.
P-2	slot no./port no.	
P-3	slot no./port no.	
P-4	tx	Interface will only transmit frames. Received frames that are not processed.
	rx	Interface will only receive frames. Frames are not transmitted.
	txrx	Interface will receive and transmit frames.
P-5	slot no./port no.	

- no monitor session
 - Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no monitor session

45.2 show

Display device options and settings.

45.2.1 show monitor session

Display port monitor session settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show monitor session <P-1>

Parameter	Value	Meaning
P-1	1	Monitor session index.

45.3 clear

Clear several items.

45.3.1 clear monitor session

Delete configuration for this session.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear monitor session <P-1>

Parameter	Value	Meaning
P-1	1	Monitor session index.

46 Simple Network Management Protocol (SNMP)

46.1 snmp

Configure of SNMP versions and traps.

46.1.1 snmp access version v1

Enable or disable SNMP version V1.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp access version v1

■ no snmp access version v1

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no snmp access version v1

46.1.2 snmp access version v2

Enable or disable SNMP version V2.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp access version v2

- no snmp access version v2
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: no snmp access version v2

46.1.3 snmp access version v3

Enable or disable SNMP version V3.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp access version v3

- no snmp access version v3
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: no snmp access version v3

46.1.4 snmp access port

Configure the SNMP access port.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp access port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of the SNMP server (default: 161).

46.1.5 snmp access snmp-over-802

Configure SNMPover802.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** snmp access snmp-over-802

■ no snmp access snmp-over-802

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no snmp access snmp-over-802

46.2 show

Display device options and settings.

46.2.1 show snmp access

Show SNMP access configuration settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show snmp access

47 SNMP Community

47.1 snmp

Configure of SNMP versions and traps.

47.1.1 snmp community ro

SNMP v1/v2 read-only community.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp community ro

47.1.2 snmp community rw

SNMP v1/v2 read-write community.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp community rw

47.2 show

Display device options and settings.

47.2.1 show snmp community

Display SNMP v1/2 community.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show snmp community

48 SNMP Logging

48.1 logging

Logging configuration.

48.1.1 logging snmp-request get operation

Enable or disable logging of SNMP GET or SET requests.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging snmp-request get operation

■ no logging snmp-request get operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no logging snmp-request get operation

48.1.2 logging snmp-request get severity

Define severity level.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging snmp-request get severity <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
6	Same as informational	
7	Same as debug	

48.1.3 logging snmp-request set operation

Enable or disable logging of SNMP GET or SET requests.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging snmp-request set operation

■ no logging snmp-request set operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no logging snmp-request set operation

48.1.4 logging snmp-request set severity

Define severity level.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging snmp-request set severity <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug

48.2 show

Display device options and settings.

48.2.1 show logging snmp

Show the SNMP logging settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show logging snmp

49 Simple Network Time Protocol (SNTP)

49.1 sntp

Configure SNTP settings.

49.1.1 sntp client operation

Enable or disable the SNTP client

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client operation

■ no sntp client operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no sntp client operation

49.1.2 sntp client operating-mode

Set the operating mode of the SNTP client. \n\n unicast-mode, the client sends a request to the SNTP Server. \n\n broadcast-mode, the client waits for a broadcast message from the SNTP Server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client operating-mode <P-1>

Parameter	Value	Meaning
P-1	unicast	Set the operating mode to unicast.
	broadcast	Set the operating mode to broadcast.

49.1.3 sntp client request-interval

Set the SNTP client request interval in seconds. \n\nThe request-interval is only used in the operating-mode unicast.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client request-interval <P-1>

Parameter	Value	Meaning
P-1	5..3600	Enter a number in the given range.

49.1.4 sntp client broadcast-rcv-timeout

Set the SNTP client broadcast receive timeout in seconds. \n\nThe broadcast receive timeout is only used in the operating-mode broadcast.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client broadcast-rcv-timeout <P-1>

Parameter	Value	Meaning
P-1	128..2048	Enter a number in the given range.

49.1.5 sntp client disable-after-sync

If this option is activated, the SNTP client disables itself \nonce it is synchronized to a SNTP server.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** sntp client disable-after-sync

■ no sntp client disable-after-sync

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no sntp client disable-after-sync

49.1.6 sntp client server add

Add a SNTP client server connection

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** sntp client server add <P-1> <P-2> <P-3> [port <P-4>] [description <P-5>]

[port]: Set the port number of the external time server.

[description]: Description of the external time server

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.
P-2	string	Hostname or IP address.
P-3	a.b.c.d	IP address.
P-4	1..65535	Port number of SNTP Server (default 123).
P-5	string	Enter a user-defined text, max. 32 characters.

49.1.7 sntp client server delete

delete a SNTP client server connection

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client server delete <P-1>

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.

49.1.8 sntp client server mode

Enable or disable a SNTP client server connection

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client server mode <P-1>

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.

■ no sntp client server mode

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no sntp client server mode

49.1.9 sntp server operation

Enable or disable the SNTP server

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** sntp server operation

■ no sntp server operation

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no sntp server operation

49.1.10 sntp server port

Set the local socket port number used to listen for client requests.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** sntp server port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of SNTP Server (default 123).

49.1.11 sntp server only-if-synchronized

Set the disabling of the SNTP server function, \nif it is not synchronized to another external time reference

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** sntp server only-if-synchronized

■ no sntp server only-if-synchronized

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no sntp server only-if-synchronized

49.1.12 sntp server broadcast operation

Enable or disable the SNTP server broadcast mode

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** sntp server broadcast operation

■ no sntp server broadcast operation

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no sntp server broadcast operation

49.1.13 sntp server broadcast address

Set the SNTP server's broadcast or multicast IP address\n(default: 0.0.0.0 (none)).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server broadcast address <P-1>

Parameter	Value	Meaning
P-1	a.b.c.d	IP address.

49.1.14 sntp server broadcast port

Set the destination socket port number used to send\nbroadcast or multicast messages to the client.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server broadcast port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of SNTP Server (default 123).

49.1.15 sntp server broadcast interval

Set the SNTP server's interval in seconds for sending\nbroadcast or multi-cast messages.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server broadcast interval <P-1>

Parameter	Value	Meaning
P-1	64..1024	Enter a number in the given range.

49.1.16sntp server broadcast vlan

Set the SNTP server's broadcast VLAN ID used for sending broadcast or multicast messages.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server broadcast vlan <P-1>

Parameter	Value	Meaning
P-1	0..4042	Enter the VLAN ID. Entering of ID 0 uses the management VLAN ID.

49.2 show

Display device options and settings.

49.2.1 show sntp global

Show SNTP configuration parameters and information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show sntp global

49.2.2 show sntp client status

Show SNTP client status.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show sntp client status

49.2.3 show sntp client server

Show SNTP client server connections.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show sntp client server [<P-1>]

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.

49.2.4 show sntp server status

Show SNTP server configuration parameters and information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show sntp server status

49.2.5 show sntp server broadcast

Show SNTP server broadcast configuration parameters.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show sntp server broadcast

50 Spanning Tree

50.1 spanning-tree

Enable or disable the Spanning Tree protocol.

50.1.1 spanning-tree operation

Enable or disable.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** spanning-tree operation

■ no spanning-tree operation

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no spanning-tree operation

50.1.2 spanning-tree bpdu-filter

Enable or disable BPDU filter on edge ports.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** spanning-tree bpdu-filter

- no spanning-tree bpdu-filter
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no spanning-tree bpdu-filter

50.1.3 spanning-tree bpdu-guard

Enable or disable BPDU guard on edge ports.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree bpdu-guard

- no spanning-tree bpdu-guard
Disable the option
 - ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no spanning-tree bpdu-guard

50.1.4 spanning-tree bpdu-migration-check

Force the specified port to transmit RST or MST BPDUs.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree bpdu-migration-check <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

50.1.5 spanning-tree forceversion

Set the force protocol version parameter.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree forceversion <P-1>

Parameter	Value	Meaning
P-1	stp	Spanning Tree Protocol (STP).
	rstp	Rapid Spanning Tree Protocol (RSTP).

50.1.6 spanning-tree forward-time

Set the Bridge Forward Delay parameter [s].

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree forward-time <P-1>

Parameter	Value	Meaning
P-1	4..30	Enter the bridge forward delay as an integer.

50.1.7 spanning-tree hello-time

Set the Hello Time parameter [s].

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree hello-time <P-1>

Parameter	Value	Meaning
P-1	1..2	Set the Hello Time parameter (unit: seconds).

50.1.8 spanning-tree hold-count

Set bridge hold count parameter.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree hold-count <P-1>

Parameter	Value	Meaning
P-1	1..40	Set bridge hold count parameter.

50.1.9 spanning-tree max-age

Set the bridge Max Age parameter.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree max-age <P-1>

Parameter	Value	Meaning
P-1	6..40	Set the bridge Max Age parameter.

50.1.10 spanning-tree mst priority

Specify the bridge priority used by a MST instance.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree mst priority <P-1> <P-2>

Parameter	Value	Meaning
P-1	0	Enter the multiple spanning tree ID 0 (0 is for CIST and RSTP).
P-2	0..61440	Set the Mst Bridge priority.

50.2 spanning-tree

Enable or disable the Spanning Tree protocol on a port.

50.2.1 spanning-tree mode

Enable or disable.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree mode

■ no spanning-tree mode

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no spanning-tree mode

50.2.2 spanning-tree bpdu-flood

Enable or disable BPDU flood on a port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree bpdu-flood

- no spanning-tree bpdu-flood
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no spanning-tree bpdu-flood

50.2.3 spanning-tree edge-auto

Enable or disable the auto edge detection on a port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree edge-auto

- no spanning-tree edge-auto
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no spanning-tree edge-auto

50.2.4 spanning-tree edge-port

Enable or disable that port being an edge port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree edge-port

■ no spanning-tree edge-port

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no spanning-tree edge-port

50.2.5 spanning-tree guard-loop

Enable or disable the loop guard on a port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree guard-loop

■ no spanning-tree guard-loop

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no spanning-tree guard-loop

50.2.6 spanning-tree guard-root

Enable or disable the root guard on a port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree guard-root

- no spanning-tree guard-root
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no spanning-tree guard-root

50.2.7 spanning-tree guard-tcn

Enable or disable the TCN guard on that port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree guard-tcn

- no spanning-tree guard-tcn
Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no spanning-tree guard-tcn

50.2.8 spanning-tree cost

Specify the port path cost.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree cost <P-1>

Parameter	Value	Meaning
P-1	0..200000000	Specify the port path cost.

50.2.9 spanning-tree priority

Specify the port priority.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree priority <P-1>

Parameter	Value	Meaning
P-1	0..240	Specify the port priority.

50.3 show

Display device options and settings.

50.3.1 show spanning-tree global

Display the Common and Internal Spanning Tree information and settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show spanning-tree global

50.3.2 show spanning-tree mst

Display detailed information and settings for a MST instance. CIST instance is 0 same value for RSTP as instance.

- ▶ **Mode:** Command is in all modes available.
 - ▶ **Privilege Level:** Guest
 - ▶ **Format:** show spanning-tree mst <P-1> [port [<P-2>]]
- [port]: Display summarized information and settings for all ports in a MST instance.

Parameter	Value	Meaning
P-1	0	Enter the multiple spanning tree ID 0 (0 is for CIST and RSTP).
P-2	slot no./port no.	

50.3.3 show spanning-tree port

Spanning Tree information and settings for an interface.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show spanning-tree port <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

51 Secure Shell (SSH)

51.1 ssh

Set SSH parameters.

51.1.1 ssh server

Enable or disable the SSH server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh server

■ no ssh server

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ssh server

51.1.2 ssh timeout

Set the SSH connection idle timeout in minutes (default: 5).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh timeout <P-1>

Parameter	Value	Meaning
P-1	0..160	Idle timeout of a session in minutes (default: 5).

51.1.3 ssh port

Set the SSH port number (default: 22).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of the SSH server (default: 22).

51.1.4 ssh max-sessions

Set the maximum number of concurrent SSH sessions (default: 5).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh max-sessions <P-1>

Parameter	Value	Meaning
P-1	1..5	Maximum number of concurrent SSH sessions (default: 5).

51.1.5 ssh key rsa

Generate or delete RSA key

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh key rsa <P-1>

Parameter	Value	Meaning
P-1	generate	Generates the item
	delete	Deletes the item

51.1.6 ssh key dsa

Generate or delete DSA key

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh key dsa <P-1>

Parameter	Value	Meaning
P-1	generate	Generates the item
	delete	Deletes the item

51.2 copy

Copy different kinds of items.

51.2.1 copy sshkey remote

Copy SSH key from server.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** copy sshkey remote <P-1> nvm

nvm: Copy SSH key from server to NV memory.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

51.3 show

Display device options and settings.

51.3.1 show ssh

Show SSH server information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ssh

52 Storm Control

52.1 storm-control

Configure the global storm-control settings.

52.1.1 storm-control flow-control

Enable or disable flow control globally.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** storm-control flow-control

■ no storm-control flow-control

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no storm-control flow-control

52.2 traffic-shape

Traffic shape commands.

52.2.1 traffic-shape bw

Set threshold value

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: traffic-shape bw <P-1>

Parameter	Value	Meaning
P-1	0..100	Enter a number in the given range.

52.3 storm-control

Storm control commands

52.3.1 storm-control flow-control

Enable or disable flow control (802.3x) for this port.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** storm-control flow-control

■ no storm-control flow-control

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no storm-control flow-control

52.3.2 storm-control ingress unit

Set unit.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** storm-control ingress unit <P-1>

Parameter	Value	Meaning
P-1	percent	Metering unit expressed in percentage of bandwidth.
	pps	Metering unit expressed in packets per second.

52.3.3 storm-control ingress threshold

Set threshold value. The rate limiter function calculates the threshold based on data packets sized 512 bytes. When the unit is set to pps, the maximum value is 24414 for 100Mb/s and 244140 for 1000Mb/s.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: storm-control ingress threshold <P-1>

Parameter	Value	Meaning
P-1	0..1000000	Enter a number in the given range.

52.3.4 storm-control ingress unicast operation

Enable/disable ingress unicast storm control.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: storm-control ingress unicast operation

■ no storm-control ingress unicast operation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no storm-control ingress unicast operation

52.3.5 storm-control ingress multicast operation

enable/disable ingress multicast storm control.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** storm-control ingress multicast operation

■ no storm-control ingress multicast operation

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no storm-control ingress multicast operation

52.3.6 storm-control ingress broadcast operation

Enable/disable ingress broadcast storm control.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** storm-control ingress broadcast operation

■ no storm-control ingress broadcast operation

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no storm-control ingress broadcast operation

52.4 show

Display device options and settings.

52.4.1 show storm-control flow-control

Global flow control status.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show storm-control flow-control

52.4.2 show storm-control ingress

Show storm control ingress parameters.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show storm-control ingress [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

52.4.3 show traffic-shape

Show Traffic Shape Parameters.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show traffic-shape

53 System

53.1 system

Set system related values e.g. name of the device, location of the device, contact data for the person responsible for the device, and pre-login banner text.

53.1.1 system name

Edit the name of the device. The system name consists of an alphanumeric ASCII character string with 0..255 characters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: system name <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 255 characters.

53.1.2 system location

Edit the location of the device. The system location consists of an alphanumeric ASCII character string with 0..255 characters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: system location <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 255 characters.

53.1.3 system contact

Edit the contact information for the person responsible for the device. The contact data consists of an alphanumeric ASCII character string with 0..255 characters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: system contact <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 255 characters.

53.1.4 system pre-login-banner operation

Enable or disable the pre-login banner. You use the pre-login banner to display a greeting or information to users before they login to the device.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: system pre-login-banner operation

■ no system pre-login-banner operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no system pre-login-banner operation

53.1.5 system pre-login-banner text

Edit the text for the pre-login banner (C printf format syntax allowed: \\n\\t)
The device allows you to edit an alphanumeric ASCII character string with up to 512 characters.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** system pre-login-banner text <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 512 characters (allowed characters are from ASCII 32 to 127).

53.2 show

Display device options and settings.

53.2.1 show eventlog

Show event log notice and warning entries with time stamp.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show eventlog

53.2.2 show system info

Show system related information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show system info

53.2.3 show system pre-login-banner

Show pre-login banner status and text.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show system pre-login-banner

53.2.4 show system flash-status

Show the flash memory statistics of the device.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show system flash-status

Telnet

54 Telnet

54.1 telnet

Set Telnet parameters.

54.1.1 telnet server

Enable or disable the telnet server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: telnet server

■ no telnet server

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no telnet server

54.1.2 telnet timeout

Set the idle timeout for a telnet connection in minutes.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: telnet timeout <P-1>

Parameter	Value	Meaning
P-1	0..160	Idle timeout of a session in minutes (default: 5).

54.1.3 telnet port

Set the listening port for the telnet server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: telnet port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Set the listening port for the telnet server.

54.1.4 telnet max-sessions

Set the maximum number of sessions for the telnet server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: telnet max-sessions <P-1>

Parameter	Value	Meaning
P-1	1..5	Set the maximum number of connections for the telnet server.

54.2 show

Display device options and settings.

54.2.1 show telnet

Show telnet server information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show telnet

55 Traps

55.1 snmp

Configure of SNMP versions and traps.

55.1.1 snmp trap mode

Enable/disable SNMP trap.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp trap mode <P-1> disable enable

disable: deactivate a SNMP trap.

enable: activate a SNMP trap.

Parameter	Value	Meaning
P-1	string	<name> Trap name (1 to 32 characters)

55.1.2 snmp trap delete

Delete SNMP trap.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp trap delete <P-1>

Parameter	Value	Meaning
P-1	string	<name> Trap name (1 to 32 characters)

55.1.3 snmp trap add

Add SNMP trap.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** snmp trap add <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<name> Trap name (1 to 32 characters)
P-2	a.b.c.d	a.b.c.d Single IP address.
	a.b.c.d:n	a.b.c.d:n Address with port.

55.2 show

Display device options and settings.

55.2.1 show snmp traps

Display SNMP traps.

- ▶ Mode: Command is in all modes available..
- ▶ Privilege Level: Guest
- ▶ Format: show snmp traps

Users

56 Users

56.1 users

Manage Users and User Accounts.

56.1.1 users add

Add a new user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users add <P-1>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

56.1.2 users delete

Delete an existing user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users delete <P-1>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

56.1.3 users enable

Enable user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users enable <P-1>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

56.1.4 users disable

Disable user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users disable <P-1>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

56.1.5 users password

Change user password.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users password <P-1> [<P-2>]

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	string	Enter a user-defined text, max. 64 characters.

56.1.6 users snmpv3 authentication

Specify authentication setting for a user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users snmpv3 authentication <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	md5	MD5 as SNMPv3 user authentication mode.
	sha1	SHA1 as SNMPv3 user authentication mode.

56.1.7 users snmpv3 encryption

Specify encryption settings for a user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users snmpv3 encryption <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	none	SNMPv3 encryption method is none.
	des	DES as SNMPv3 encryption method.
	aescfb128	AES-128 as SNMPv3 encryption method.

56.1.8 users access-role

Specify snmpv3 access role for a user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users access-role <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	guest	Enable guest access.
	auditor	Enable auditor access.
	operator	Enable operator access.
	administrator	Enable administrator access.
	unauthorized	Set unauthorized access.

56.1.9 users lock-status

Set the lockout status of a specified user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users lock-status <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	lock	Lock specific user. User can't login anymore.
	unlock	Unlock specific user. User can login again.

56.1.10 users password-policy-check

Set password policy check option. The device checks the "minimum password length", regardless of the setting for this option.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users password-policy-check <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	enable	Enable the option.
	disable	Disable the option.

56.2 show

Display device options and settings.

56.2.1 show users

Display users and user accounts information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show users

57 Virtual LAN (VLAN)

57.1 name

57.1.1 name

Assign a name to a VLAN

- ▶ **Mode:** VLAN Database Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** name <P-1> <P-2>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.
P-2	string	Enter a user-defined text, max. 32 characters.

57.2 vlan-unaware-mode

57.2.1 vlan-unaware-mode

Enable or disable VLAN unaware mode.

- ▶ **Mode:** VLAN Database Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** vlan-unaware-mode

■ no vlan-unaware-mode

Disable the option

- ▶ **Mode:** VLAN Database Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no vlan-unaware-mode

57.3 vlan

Creation and configuration of VLANS.

57.3.1 vlan add

Create a VLAN

- ▶ Mode: VLAN Database Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan add <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

57.3.2 vlan delete

Delete a VLAN

- ▶ Mode: VLAN Database Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan delete <P-1>

Parameter	Value	Meaning
P-1	2..4042	Enter VLAN ID. VLAN ID 1 can not be deleted or created

57.4 vlan

Configure 802.1Q port parameters for VLANs.

57.4.1 vlan acceptframe

Configure how to handle tagged/untagged frames received.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** vlan acceptframe <P-1>

Parameter	Value	Meaning
P-1	all	Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.
	vlanonly	Only frames received with a VLAN tag will be forwarded. All other frames will be dropped.

57.4.2 vlan ingressfilter

Enable/Disable application of Ingress Filtering Rules.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** vlan ingressfilter

- no vlan ingressfilter
 - Disable the option
 - ▶ Mode: Interface Range Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: no vlan ingressfilter

57.4.3 vlan priority

Configure the priority for untagged frames.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan priority <P-1>

Parameter	Value	Meaning
P-1	0..7	Enter a number in the given range.

57.4.4 vlan pvid

Configure the VLAN id for a specific port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan pvid <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

57.4.5 vlan tagging

Enable or disable tagging for a specific VLAN port.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** vlan tagging <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

■ no vlan tagging

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no vlan tagging

57.4.6 vlan participation include

vlan participation to include

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** vlan participation include <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

57.4.7 vlan participation exclude

vlan participation to exclude

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** vlan participation exclude <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

57.4.8 vlan participation auto

vlan participation to auto

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** vlan participation auto <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

57.5 show

Display device options and settings.

57.5.1 show vlan id

Display configuration of a single specified VLAN.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show vlan id <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

57.5.2 show vlan brief

Show general VLAN parameters.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show vlan brief

57.5.3 show vlan port

Show VLAN configuration of a single port.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show vlan port [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

57.5.4 show vlan member current

Show membership of ports in static VLAN or dynamically created.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show vlan member current

57.5.5 show vlan member static

Show membership of ports in static VLAN.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show vlan member static

57.6 network

Configure the inband connectivity.

57.6.1 network management vlan

Configure the management VLAN ID of the switch.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network management vlan <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

57.6.2 network management priority dot1p

Configure the management VLAN priority of the switch.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network management priority dot1p <P-1>

Parameter	Value	Meaning
P-1	0..7	Enter a number in the given range.

57.6.3 network management priority ip-dscp

Configure the management VLAN ip-dscp priority of the switch.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network management priority ip-dscp <P-1>

Parameter	Value	Meaning
P-1	0..63	Enter a number in the given range.

F Further Support

■ Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at

<http://www.hirschmann.com>

Contact our support at

<https://hirschmann-support.belden.eu.com>

You can contact us

in the EMEA region at

▶ Tel.: +49 (0)1805 14-1538

▶ E-mail: hac.support@belden.com

in the America region at

▶ Tel.: +1 (717) 217-2270

▶ E-mail: inet-support.us@belden.com

in the Asia-Pacific region at

▶ Tel.: +65 6854 9860

▶ E-mail: inet-ap@belden.com

■ Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

▶ Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.

▶ Training offers you an introduction to the basics, product briefing and user training with certification.

The current technology and product training courses can be found at

<http://www.hicomcenter.com>

▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:

<http://www.hicomcenter.com>



HIRSCHMANN

A **BELDEN** BRAND